DEPARTMENT OF DEFENSE

HANDBOOK

FOR WRITING

SECURITY CLASSIFICATION GUIDANCE

November 1999

ASSISTANT SECRETARY OF DEFENSE FOR
COMMAND, CONTROL, COMMUNICATIONS, AND
INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

FOREWORD

This Handbook is issued under the authority of DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996. Its purpose is to assist in the development of the security classification guidance required under paragraph 2-500 of DoD 5200.1-R, for each system, plan, program, or project in which classified information is involved.

DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," March 18, 1986, is hereby canceled.

This Handbook is effective immediately.

Users of this Handbook are encouraged to direct comments to the Director, Security; Office of the Deputy Assistant Secretary of Defense (Security and Information Operations), 6000 Defense, The Pentagon, Washington, DC 20301-6000.

DoD Components may obtain copies of this Handbook through their own publications channels. Approved for public release; distribution unlimited. Authorized registered users may obtain copies of this Handbook from the Defense Technical Information Center, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218. Other Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161. This Handbook is also available on the web at: http://web7.whs.osd.mil under Publications.

for Christopher K. Mellon
Deputy Assistant Secretary of Defense
(Security and Information Operations)

TABLE OF CONTENTS

REFERENCES

(a) Executive Order 12958, "Classified National Security Information," April 20, 1995
(b) Information Security Oversight Office Directive No. 1., "Classified National Security Information," October 13, 1995
(c) DoD 5200.1-R, "Information Secuirty Program," January 1997
(d) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 1998
(e) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 1998
(f) DoD O-5200.1-I, "Index of Security Classification Guides," September 1996

C1. CHAPTER 1

INTRODUCTION

C1.1.1. Good security classification practice calls for the timely issuance of comprehensive guidance regarding security classification of information concerning any system, plan, program, or project; the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Precise classification guidance is prerequisite to effective and efficient information security and assures that security resources are expended to protect only that which truly warrants protection in the interests of national security. Executive Order 12958 (reference (a)) and its implementing Information Security Oversight Office Directive No. 1 (reference (b)), provide general requirements and standards concerning the issuance of security classification guides.

C1.1.2. Information is classified to assist in ensuring that it is provided an appropriate level of protection. Therefore, it is essential that a classification guide be concerned with identifying the specific items of information and the level of protection required, as well as the time period for which protection must be continued.

C1.1.3. A classification guide should be issued as early as practical in the life cycle of the classified system, plan, program or project. Any uncertainty in application of the policies and procedures contained in DoD 5200.1-R, "Information Security Program" (reference (c)), which implements the provisions of reference (a) and (b) within DoD, will result in a less than satisfactory security classification guide. Accordingly, the requirements of DoD 5200.1-R regarding classification, declassification, downgrading, marking, and security classification guides should be reviewed and understood before proceeding with the task of writing a security classification guide.

C1.1.4. DoD information that does not, individually or in compilation, require classification, must be reviewed in accordance with DoD 5400.7-R (reference (d)), prior to any contemplated release to the public. In addition, such information must also be reviewed for compliance with the provisions of Deputy Secretary of Defense Memorandum, dated December 7, 1998 (reference (e)), prior to its placement on any publicly accessible DoD web site. Information that does not require classification may nevertheless be exempt from release to the public for several reasons, such as, for example, privacy of individuals or restrictions on the export of defense articles and services. Some restrictions may apply to information released to other U.S. Government Agencies, even if it is not approved for public release.

C2. CHAPTER 2

CLASSIFICATION AND DECLASSIFICATION

C2.1. GENERAL

Since the primary purpose of this Handbook is to provide assistance to those who are responsible for the writing of a security classification guide, some discussion of classification and declassification principles is warranted.

C2.2. CLASSIFICATION DECISIONS

C2.2.1. Basically, information is classified either originally or derivatively. Original classification occurs when information is developed that intrinsically meets the criteria for classification under Executive Order 12958 (reference (a)). Such classification cannot reasonably be derived from a previous classification decision still in force involving in substance, the same or closely related information. A security classification guide is the written record of an original classification decision or series of decisions regarding a system, plan, program, or project. Derivative classification occurs when the information under review is already known to be classified.

C2.2.2. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. Information that has been officially released, or is otherwise in the public domain, may not be classified. Information may be considered for classification only if it concerns one of the categories specified in section 1.5a of reference (a):

C2.2.2.1. Military plans, weapon systems, or operations.

C2.2.2.2. Foreign government information.

C2.2.2.3. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

C2.2.2.4. Foreign relations or foreign activities of the United States, including confidential sources.

C2.2.2.5. Scientific, technological, or economic matters relating to the national security.

C2.2.2.6. United States Government programs for safeguarding nuclear materials or facilities; or

C2.2.2.7. Vulnerabilities or capabilities of systems, installations. projects or plans relating to the national security.

C2.2.3. An original classification authority is confronted with the need to decide whether certain information should be classified. To make this determination there are a number of steps to follow. These steps may be laid out as a series of questions.

C2.2.3.1. Is the information owned by, produced by or for, or under the control of the United States Government?

C2.2.3.2. Does the information fall within one or more of the several categories of information in subsections C2.2.1. through C2.2.2.7., above? If the answer to this question is "no," the information cannot be classified. If the answer is "yes," then the next question applies.

C2.2.3.3. Can the unauthorized disclosure of the information reasonably be expected to cause damage to the national security? If the answer is "no," the information cannot be classified. If the answer is "yes," then the fourth question applies.

C2.2.3.4. What is the level of damage ("damage," "serious damage," or "exceptionally grave damage") to the national security expected in the event of an unauthorized disclosure of the information? If the answer to this question is "damage" you have arrived at a decision to classify the information Confidential. If the answer is "serious damage," you have arrived at a decision to classify the information Secret. If the answer is "exceptionally grave damage," you have arrived at a decision to classify the information Top Secret.

C2.3. WHEN TO DECLASSIFY

The declassification decision determines duration of protection, and is as important as the original classification determination. At the time an item of information is classified, original classifiers shall:

C2.3.1. Assign a date within 10 years from the date of classification upon that the information can be automatically declassified.

C2.3.2. Determine a specific event, reasonably expected to occur within 10 years, that can be set as the signal for automatic declassification; or

C2.3.3. Designate the information as being automatically declassified 10 years from the date of its original classification.

C2.3.4. An original classifier may extend classification beyond 10 years only if:

C2.3.4.1. The unauthorized disclosure of the information could reasonably be expected to cause damage to the national security for a period in excess of 10 years; and

C2.3.4.2. Release of the information could reasonably be expected to:

C2.3.4.2.1. Reveal an intelligence source, method, or activity, or a cryptologic system or activity.

C2.3.4.2.2. Reveal information that would assist in the development or use of weapons of mass destruction.

C2.3.4.2.3. Reveal information that would impair the development or use of technology within a United States weapon system.

C2.3.4.2.4. Reveal United States military plans, or national security emergency preparedness plans.

C2.3.4.2.5. Reveal foreign government information.

C2.3.4.2.6. Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years.

C2.3.4.2.7. Impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services are authorized.

C2.3.4.2.8. Violate a statute, treaty, or international agreement.

C2.4. DOWNGRADING

Executive Order 12958 (reference (a)) does permit an original classifier to provide downgrading of classification to a lower level at predetermined points in time, or upon the occurrence of specified events. You are encouraged to specify in your guide, downgrading to a lower level of classification when the lower level will provide adequate protection.

C3. CHAPTER 3

PLAN OF ACTION FOR WRITING CLASSIFICATION GUIDES

C3.1. STEP 1. CONSIDER RELATED CURRENT GUIDANCE

C3.1.1. Before writing a security classification guide, it is necessary to find out what, if any, classification guidance exists applicable to items of information concerning the system, plan, program or project for which the classification guide is being constructed. Any existing guidance may affect your effort, and should be considered carefully. Uniformity and consistency in the exercise of classification authority, especially in the form of a security classification guide, are essential. Beware of conflicts between the guide you will be developing and any already approved guide.

C3.1.2. In some fields of interest, guides have been issued that apply to a broad spectrum of activities. Such guides often are issued as DoD Instructions through the DoD Directives System. DoD 5200.1-I (reference (f)) provides a listing of most guides issued within the Department of Defense. Many of the listed guides are available from the Defense Technical Information Center. Always check reference (f), but be aware that some classification guides are too sensitive to be identified in that document. In addition, there may be other classification guides issued along functional lines by activities outside the Department of Defense that could have a bearing on your effort. Seek the advice of those who have knowledge of classification in the subject area under consideration or in closely related fields. If your activity has an information security specialist, that individual may be a particularly valuable source of advice and assistance.

C3.2. STEP 2. DETERMINE STATE-OF-THE-ART STATUS

Reasonable classification determinations cannot be made in the scientific and technical field without analysis of what has been accomplished, what is being attempted and by whom. Make use of scientific and information services. Consult technical and intelligence specialists. Obtain assistance available from any proper source. Learn about the state-of-the-art, the state of development, attainment in the field of work, and what is known and openly published about it, including:

C3.2.1. The known or published status (foreign and domestic).

C3.2.2. The known but unpublished (probably classified) status in the United States.

C3.2.3. The known but unpublished status in friendly and unfriendly countries.

C3.2.4. The extent of foreign knowledge of the unpublished status in the United States.

C3.3. STEP 3. IDENTIFY NATIONAL ADVANTAGE

The subject matter of your guide must be looked at as a totality. Decide what it does or seeks to accomplish that will result in a net national advantage. Cover all the values, direct and indirect, accruing or expected to accrue to the United States. In the final analysis, the decision to classify will be related to one or more of the following factors, producing directly or indirectly, the actual or expected net national advantage:

C3.3.1. Fact of interest by the U.S. Government in the particular effort as a whole or in specific parts that are being considered or emphasized.

C3.3.2. Fact of possession by the United States.

C3.3.3. Capabilities of the resulting product in terms of quality, quantity, and location.

C3.3.4. Performance, including operational performance, as it relates to capabilities.

C3.3.5. Vulnerabilities, weaknesses, countermeasures, and counter-countermeasures.

C3.3.6. Uniqueness. Exclusive United States knowledge.

C3.3.7. Lead time, related to state-of-the-art.

C3.3.8. Surprise, related to possession and capability to use.

C3.3.9. Specifications. May be indicative of goals, aims, or achievements.

C3.3.10. Manufacturing technology.

C3.3.11. Associations with other data or activities.

C3.4. STEP 4. MAKE INITIAL CLASSIFICATION DETERMINATION

Making the analyses outlined in sections C3.2. and C3.3., above, will lead to conclusions on the ways the effort will result in net national advantage, and hence, what it is that requires classification to protect that advantage. Although at this stage of the guide's preparation you are concerned primarily with information relating to the overall effort, consideration must be given to some of the more particular information or data such as that covering performance capabilities, and possible vulnerabilities and weaknesses. Appendix 1 has been designed to help in that consideration.

C3.5. STEP 5. IDENTIFY SPECIFIC ITEMS OF INFORMATION THAT REQUIRE CLASSIFICATION

C3.5.1. The real heart of a classification guide is the identification and enunciation of the specific items or elements of information warranting security protection. Regardless of the size or complexity of the subject matter of the guide, or the level at which the classification guide is issued, there are certain identifiable features of the information that create or contribute to actual or expected national security advantage. There also may be certain items of information that need to be protected to prevent or make it more difficult for hostile forces to develop or apply timely and effective countermeasures. The problem is to identify and state those special features or critical items of information and to decide how and why they are related to the net national advantage. Several additional steps relating to this problem of identification of classifiable details are laid out in Appendices 2 and 3. The important thing is that the statements of classification in the guide are clear and specific so as to minimize the probability of error by those who will use the classification guide. (See Chapter 4 for a complete discussion on classifying hardware items.)

C3.5.2. It is equally important that you specify precisely and clearly the level of classification to be applied to each item of information identified in the guide. Broad guidance such as "U-S" meaning Unclassified to Secret does not provide sufficient instruction to users of the guide, unless you also delineate the exact circumstances under which each level of classification should be applied. The exact circumstances may be supplied in amplifying comments, for example, "Unclassified ("U") when X is not revealed;" "Confidential when X is revealed;" and "Secret when X and Y are

revealed." Failure to provide such guidance will result in users of the guide making their own interpretations that may, or may not, be consistent with your intent.

C3.5.3. Information that has been officially released to the public may not be classified. This does not include unauthorized releases such as "leaks."

C3.6. STEP 6. DETERMINE HOW LONG CLASSIFICATION MUST CONTINUE

C3.6.1. Equally important to a determination to classify is the decision on how long the classification should remain in effect. The following are factors that may influence this decision:

C3.6.1.1. At the conceptual stage of a new effort there may be good reason to classify more information about the effort than will be necessary in later phases. Typically, information loses its sensitivity and importance in terms of creating or contributing to the national advantage over time.

C3.6.1.2. At certain stages in production, or deployment, it may not be practical or possible to protect certain items of information from disclosure. It is also possible that design improvements may have eliminated exploitable vulnerabilities.

C3.6.1.3. Once a decision is made to release information to the public, it cannot remain classified.

C3.6.2. With these factors in mind, and considering the provisions of section C2.3., proceed with the determination of the appropriate declassification instructions for each item of classified information.

C3.6.3. Always look at the possibility of providing for automatic downgrading of the classification that is assigned. Future downgrading is an option that is always open when information is originally classified at "S" or "TS" levels. Consider it carefully in every instance, and provide for downgrading at fixed future points in time when the damage that is expected to result from an unauthorized disclosure will be reduced to a level prescribed for lower classification.

C3.7. STEP 7. WRITING THE GUIDE

C3.7.1. Determine exactly what warrants security classification. Set clear, precise language or statements describing which items of information require classification. It is also advisable to include items that are unclassified. This assures

users of the guide that this information is, in fact, unclassified and was not inadvertently omitted. While there is no mandatory DoD-wide format for security classification guides, first consider the guide illustrated in Appendix 4. (Also see Appendix 5 for some format variations.) Place significant words of the guide's title first, for example, "FA-5B Aircraft Security Classification Guide."

C3.7.2. There are a number of administrative requirements for security classification guides. Bear in mind that the security classification guide you are writing must:

C3.7.2.1. Precisely state the specific information elements to be protected.

C3.7.2.2. Identify the classification levels "TS," "S," or "C" and any additional control marking such as Restricted Data (RD), Formerly Restricted Data (FRD) or NO FOREIGN DISSEMINATION (NOFORN), that may apply to each element of information, or when it will serve a useful purpose, specify that the information is unclassified.

C3.7.2.3. Identify the reason for classification.

C3.7.2.4. Specify the duration of classification for each element of information (except RD and FRD). RD and FRD is subject to the provisions of the Atomic Energy Act, therefore, no declassification determination should be entered for this information.

C3.7.2.5. State any downgrading action that is to occur, and when such action is to take place.

C3.7.2.6. Identify the original classification authority who personally approved the guide in writing, and who has program or supervisory responsibility over the information addressed in the guide as well as the Office of Primary Responsibility that can be contacted for clarification or additional information.

C3.7.2.7. Include amplifying comments whenever appropriate to explain the exact application of classification.

C4. CHAPTER 4

CLASSIFYING HARDWARE ITEMS

C4.1. GENERAL

A piece of hardware may convey information that is as sensitive as the words printed upon a piece of paper.

C4.2. BASIC CONSIDERATIONS

Hardware items may be classified if they reveal information or information can be obtained from them. The following are some basic considerations:

C4.2.1. An item of hardware does not necessarily need to be classified simply because it is part of a classified product or effort.

C4.2.2. Unclassified off-the-shelf items, unless modified in some particular way to make them perform differently, can never be classified even though they constitute a critical element, become an integral part of a classified end product, or produce a properly classified effect. However, the association of otherwise unclassified hardware with a particular effort or product may reveal something classified about that effort or product. Common integrated circuits that control frequencies are notable examples. In such cases it is the association with the effort or product that reveals the classified information, not the circuits themselves. Decisions regarding what aspect of the system to classify may be difficult but are necessary to delineate for users of the guide, what information requires protection.

C4.2.3. Frequently, classified information pertaining to a hardware item can be restricted to the paper work associated with the item.

C4.2.4. Unusual, unique, or peculiar uses or modifications of ordinarily available unclassified materials or hardware may create a classifiable item of information. In another instance, just using a particular material in a particular effort might reveal a classifiable research or development interest. In such cases, it is especially important to accurately identify the classified information to determine whether it is the hardware or material that reveals classified information or the association of uses of the hardware with a particular effort that reveals such information.

C4.2.5. At some stage in a production effort, production and engineering plans are drawn. Usually a family-tree type diagram is prepared to assist in determining what components, parts, and materials will be required. This diagram supplies a good basis to determine where and when classified information will be involved in the production effort.

C4.2.6. Another usual step in production engineering is the development of drawings for all the individual elements that go into the final product. These drawings show design data, functions, and specifications, all of which are closely tied with items of information that may be classified. From these drawings it is possible to determine exactly which elements of the final product will reveal classified information. It is also possible to determine associations that may reveal classified information. This is a prime opportunity to identify and isolate classification requirements.

C4.3. USER CONSIDERATIONS

Know who will be using your classification guide.

C.4.3.1. Usually management and staff supervisory personnel need to have a fairly broad knowledge of classification requirements. Farther down the line however, foremen and workers usually need to know only which hardware items are classified the appropriate levels of classification and which items are unclassified. Therefore, as soon as possible in the production planning process, make a listing of all classified hardware items according to part number or other identifier, and when necessary for understanding, a listing of unclassified items. Such a listing will be valuable to procurement and logistics (shipping, handling, and storage) personnel. The listing should preferably be unclassified, but should be reviewed carefully to ensure that the listing itself does not reveal classified information.

C4.3.2. When planning a production line, careful attention is needed to delay as long as possible the insertion of classified hardware items.

C4.3.3. Test equipment rarely embodies classified information. When such equipment is used to test tolerances, specifications, performance, and other details that are classified, the equipment would still be unclassified unless it was calibrated or set in such a way as to reveal the classified information pertaining to the item being tested. This is one example of a situation where it may be possible to limit the classified information to the paper work involved and to the test operator's personal knowledge, precluding the necessity for classifying the test equipment itself.

C5. CHAPTER 5

CLASSIFYING MILITARY OPERATIONS INFORMATION

C5.1. GENERAL

The security classification of military operations information is subject to many of the considerations described in Chapter 3 and Appendix 3 of this Handbook. While there are no hard and fast rules for classification of military operations information, and while each Military Service and command may require a unique approach to operations security (OPSEC), there are basic concepts that can be applied.

C5.2. MILITARY OPERATIONS INFORMATION

For the purpose of this Handbook, military operations is defined as information pertaining to a strategic or tactical military action, including training, movement of troops and equipment, supplies, and other information vital to the success of any battle or campaign.

C5.3. MILITARY OPERATIONS CLASSIFICATION CONSIDERATIONS

C5.3.1. Successful battle operations depend largely upon our ability to assess correctly the capability and intention of enemy forces at each stage of the battle while concealing our own capabilities and intentions, and to communicate an effective battle doctrine throughout our forces. Classifiable information would include:

C5.3.1.1. The number, type, location, and strengths of opposing units.

C5.3.1.2. The capabilities and vulnerabilities of weapons in enemy hands, and how he normally applies the weapons.

C5.3.1.3. The morale and physical condition of the enemy force.

C5.3.2. In considering classification guidance for military operations, there may be good reason to classify more information about the operations in the beginning than will be necessary later. Certain elements of information such as troop movements may no longer require protection after a certain date or event. When this point is reached, downgrading or even declassification should be considered.

C5.3.3. The following are examples of information relating to military operations that may warrant classification:

TOPIC	CLASS	DECLASS	REMARKS
C5.3.3.1. Overall operational plans	"S"	Date, event, date within 10 years	
C5.3.3.2. System operational deployment or employment	"C"	After deployment or employment	
C5.3.3.3. Initial Operational Capability (IOC) date	"C"	After IOC Date	
C5.3.3.4. Planned location of operational units	"S"	After arrival on site	
C5.3.3.5. Equipage dates, readiness dates, operational employment dates	"S"	After these events	
C5.3.3.6. Total manpower or personnel requirements for total operational force	"C"	After operation	
C5.3.3.7. Coordinates of selected operational sites	"S"	"C" after site activation; "U" on termination of site	
C5.3.3.8. Specific operational performance data that relates to the effectiveness of the control of forces and data on specific vulnerabilities and weaknesses.	"S"	Date/event, date within 10 years	
C5.3.3.9. Existing OPSEC and COMSEC	"S"	Date/event,date within 10 years	
C5.3.3.10. Target characteristics	"S"	Date/Event, date within 10 years	

C6. CHAPTER 6

CLASSIFYING INTELLIGENCE INFORMATION

C6.1. CLASSIFICATION CONSIDERATIONS

Producers of intelligence must be wary of applying so much security that they are unable to provide a useful product to their consumers. Consequently, an intelligence product should be classified only when its disclosure could reasonably be expected to cause some degree of damage to national security. The following are some basic considerations, but are not necessarily all-inclusive:

C6.1.1. In general, resource information should not be classified unless it reveals some aspect of the intelligence mission, and its revelation would jeopardize the effectiveness of a particular function. An example of classifiable resource information is the intelligence contingency fund.

C6.1.2. Intelligence concerning foreign weapons systems may be classified based on what is generally known about a particular system or its components. Normally, the less that is publicly known about a particular system or component, the higher its level of classification.

C6.1.3. Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the particular source or method.

C6.1.4. Intelligence that does not identify or reveal a sensitive source or method is usually not classified unless the information contains other classified information such as intelligence activities including intelligence plans, policies, or operations.

C6.1.5. Intelligence that reveals the identity of a conventional source or method normally does not require classification. However, if the information is communicated to the Department of Defense by a foreign government, whether under a formal government-to-government agreement or, simply with the understanding that the information is provided in confidence, the information must be protected at the level and for the length of time agreed to by the United States and the transmitting government. If the information is obtained from a foreign government without any agreement or restrictions, the classification, if any, should be based solely on the content of the information provided.

C6.1.6. Intelligence that reveals the identification of all known and possible

enemy capabilities to collect and exploit information from a given or similar operation is classified. This threat would include enemy intelligence collection and analysis capabilities, efforts, and successes. An integral part of this data is an assessment of enemy human intelligence, signal intelligence, and reconnaissance satellite capabilities.

C6.1.7. Defense users must respect security classification assigned to intelligence received from non-Defense sources.

C6.1.8. An intelligence estimate is normally classified since it contains sensitive sources, methods, or raw or evaluated intelligence.

C6.1.9. An intelligence requirement is classified when it reveals what is not known, what is necessary to know, and why. Moreover, the requirement may recommend a sensitive source or method, other military intelligence required, or contain technical and operational characteristics of classified weapons systems.

C6.1.10. The classification of relationships with foreign intelligence organizations is related to the following considerations:

C6.1.10.1. Normally, the fact of broad, United States general intelligence cooperation with foreign countries or groups of countries that the United States maintains formal military alliances or agreements (e.g., NATO) is not classified.

C6.1.10.2. The fact of intelligence cooperation between the United States and a specific governmental component in an allied country or general description of the nature of intelligence cooperation between the United States and any allied country may be classified. The fact of intelligence cooperation between the United States and specifically named countries or their governmental components that the United States is NOT allied is always classified.

C6.1.10.3. Details of any intelligence exchange agreements are classified. In some instances, the mere existence of such an agreement may be classified.

C6.1.10.4. The identities of foreign governmental or military personnel who provide intelligence under such agreements or liaison relationships may be classified.

C6.1.11. Information that reveals counterintelligence activities, identities of undercover personnel or units or clandestine human agents, methods of operations and analytical techniques for the interpretation of intelligence data is classified.

C6.1.12. Cryptologic information (including cryptologic sources and methods) is classified.

C6.1.13. Information concerning electronics intelligence, telemetry intelligence, and electronic warfare is usually classified.

C6.1.14. The intelligence community normally considers the following categories of information to be classified:

C6.1.14.1. Cryptologic, cryptographic, signals intelligence, or imagery intelligence.

C6.1.14.2. Counterintelligence.

C6.1.14.3. Special access programs.

C6.1.14.4. Information that identifies clandestine organizations, agents, sources, or methods.

C6.1.14.5. Information on personnel under official or nonofficial cover, or revelation of a cover arrangement.

C6.1.14.6. Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.

C6.1.14.7. Methods or procedures used to acquire, produce, or support intelligence activities.

C6.1.14.8. Intelligence organizational structure, size, installations, security, objectives, and budget.

C6.1.14.9. Information that would divulge intelligence interests, value, or extent of knowledge on a subject.

C6.1.14.10. Training provided to or by an intelligence organization that would indicate its capability or identify personnel.

C6.1.14.11. Personnel recruiting, hiring, training, assignment, and evaluation policies.

C6.1.14.12. Information that could lead to foreign political, economic, or military action against the United States or its allies.

C6.1.14.13. Events leading to international tension that would affect U.S. foreign policy.

C6.1.14.14. Diplomatic or economic activities affecting national security or international security negotiations.

C6.1.14.15. Information affecting U.S. plans to meet diplomatic contingencies affecting national security.

C6.1.14.16. Nonattributable activities conducted abroad in support of U.S. foreign policy.

C6.1.14.17. U.S. surreptitious collection in a foreign nation that would affect relations with the country.

C6.1.14.18. Covert relationships with international organizations or foreign governments.

C6.1.14.19. Information related to political or economic instabilities in a foreign country threatening American lives and installation there.

C6.1.14.20. Information divulging U.S. intelligence and assessment capabilities.

C6.1.14.21. Defense plans and capabilities of the United States and its allies that could enable a foreign entity to develop countermeasures.

C6.1.14.22. Information disclosing U.S. systems and weapons capabilities or deployment.

C6.1.14.23. Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.

C6.1.14.24. Information on technical systems for collection and production of intelligence.

C6.1.14.25. U.S. nuclear programs and facilities.

C6.1.14.26. Foreign nuclear programs, facilities, and intentions.

C6.1.14.27. Contractual relationships that reveal the specific interest and expertise of an intelligence organization.

C6.1.14.28. Information that could place an individual in jeopardy.

C6.1.14.29. Information on secret writing when it relates to specific chemicals, reagents, developing, and microdots.

C6.1.14.30. U.S. military space programs.

C6.2. INTELLIGENCE DECLASSIFICATION CONSIDERATIONS

Normally intelligence will remain classified for a longer duration than other types of classified information, but still only as long as is necessary to protect a certain source or method. The outline in Chapter 3 of this Handbook on determining how long classification must continue is applicable to all information, including intelligence.

C6.3. CLASSIFICATION GUIDE ILLUSTRATIONS

The treatment of classifying details (Appendix 2) and recommended format for a security classification guide (Appendix 4) are applicable to the development of an intelligence security classification guide. In addition, the following is provided as an example of security classification guidance that might be applied to a Human Intelligence (HUMINT) effort:

TOPIC	CLASS	DECLASS	REMARKS
C6.3.1. Biographic information taken exclusively from open source, where no intelligence connection is shown.	"U"		
C6.3.2. Positive identification of an individual as potential source to a U.S. intelligence agency.	"S-TS"	Date/event within 10 years, or 10 years from origination.	"TS if identified as an actual source.
C6.3.3. Identity of a target installation or target personality when not linked to a specific collection operation.	"S"	Date/event within 10 years, or 10 years from origination.	"TS" when linked to an actual source or Specific collection operation.
C6.3.4. Interest in specific events for collection exploitation, including specific areas of technology.	"S"	Date/event within 10 years, or 10 years from origination.	
C6.3.5. Names of collection agency case officers in conjunction with a specific collection operation.	"C"	Date/event within 10 years, or 10 years from origination.	
C6.3.6. Information on collection agency HUMINT policy plans, plans, methods, or accomplishments.	"S"	Date/event within 10 years, or 10 years from origination.	

C7. CHAPTER 7

CLASSIFYING FOREIGN RELATIONS INFORMATION

C7.1. GENERAL

The Department of State (DoS) is the agency primarily responsible for the development and execution of the foreign policy of the United States, and thus is also the primary agency responsible for the security classification of foreign relations information. Most Defense classification determinations in the area of foreign relations will be derivative in nature. However, there will be instances where Defense projects and programs involve foreign relations information for which security classification guidance must be developed.

C7.2. FOREIGN RELATIONS CLASSIFICATION CONSIDERATIONS

The following are some of the types of information or material involving foreign relations that warrant classification consideration:

C7.2.1. All material that reveals or recommends U.S. Government positions or options in a negotiation with a foreign government or group of governments, or comments on the merits of foreign government positions in such negotiations.

C7.2.2. All material that comments on the quality, character, or attitude of a serving foreign government official, whether elected or appointed, and regardless of whether the comment is favorable or critical. Illustrations of the types of information covered in this category are records revealing:

C7.2.2.1. A foreign official speaking in a highly critical manner of his own government's policy.

C7.2.2.2. A foreign official suggesting how pressure might effectively be brought to bear on another part of his own government.

C7.2.2.3. A foreign official acting in unusually close concert with U.S. officials where public knowledge of this might be harmful to that foreign official.

C7.2.2.4. A foreign official whose professional advancement would be beneficial to U.S. interest, especially if any implication has been made of U.S. efforts to further his advancement, or if public knowledge of this might place the person or his career in jeopardy.

C7.2.3. All unpublished adverse comments by U.S. officials on the competence, character, attitudes, or activities of a serving foreign government official.

C7.2.4. All material that constitutes or reveals unpublished correspondence between heads of state or heads of government.

C7.2.5. Statements of U.S. intent to defend, or not defend, identifiable areas, in any foreign country or region.

C7.2.6. Statements of U.S. intent to militarily attack identifiable areas in any foreign country or region.

C7.2.7. Statements of U.S. policies or initiatives within collective security organizations, e.g., NATO.

C7.2.8. Agreements with foreign countries to use or have access to, military or naval facilities.

C7.2.9. Contingency plans as they involve other countries, the use of foreign bases, territory, or airspace; or the use of chemical, biological, or nuclear weapons.

C7.2.10. Defense surveys of foreign territories for purposes of basing or using in contingencies.

C7.2.11. Statements relating to any use of foreign bases not authorized under bilateral agreements.

C7.3. CLASSIFICATION GUIDE ILLUSTRATIONS

C7.3.1. The treatment of classifying details (Appendix 2) and recommended format for a security classification guide (Appendix 4) are applicable to the development of a foreign relations security classification guide. The following is provided as an example of the impact that foreign government information might have on the development of classification guidance:

C7.3.1.1. A DoD Component is involved in negotiating an arrangement with country "X." In the process of the negotiations, the foreign counterpart states that his country does not want discussion on the subject to become public knowledge. At the same time, the foreign official makes it clear that his country has announced publicly its intention to seek U.S. views on the subject of the discussions.

C7.3.1.2. The nature of business being discussed is such that the United States would not require protecting the discussions from public disclosure. Moreover, the subject matter is one that would not ordinarily be classified. The DoD Component, however, does classify the notes and transcripts pertaining to the discussion because of the expressed wishes of the foreign government. The information fits the description of foreign government information. Thus, a classification guide on the subject might contain the following topics:

TOPIC	CLASS	DECLASS	REMARKS
C7.3.1.2.1. Apple orchard negotiations with country "X."	"U"		Mere fact of negotiations only, and elaboration may be classified, see next topic.
C7.3.1.2.2. Transcripts of apple orchard negotiations and substantive notes pertaining to them.		"C"	Requires consultation with foreign government.

C7.3.1.3. The foregoing scenario illustrates a brief classification guide involving the foreign relations of the United States as well as foreign government information. The guide could not have been written until after the opening of the negotiations at which point the foreign official made known the two critical elements of information. In anticipation that the negotiations will involve a large number of personnel from several U.S. Agencies and will last several years, a classification guide such as this one, brief as it is, can serve a very useful purpose.

C7.3.1.4. To illustrate a scenario with military implications, let's presume that two countries in Europe have secretly granted the United States permission to fly over their territory, but only at high (50,000 feet) altitudes. One of the countries ("Y") indicated that serious damage would occur to our relations if the information became public while the other ("Z") indicated that it did not want the information to be in the public domain. Classification guide topics might read as follows:

TOPIC		CLASS	DECLASS	REMARKS
C7.3.1.4.1.	Fact of U.S overflights - Europe.			
C7.3.1.4.2.	(S) Country "Y"	"S"	Requires written	(S) Must be at least
C7.3.1.4.3.	(C) Country "Z"	"C"	approval of foreign	50,000 feet altitude;
C7.3.1.4.4.	(U) Other European	"U"	government involved.	lower flights not permitted in "Y" and "Z"

In this example, the guide itself would have to be classified "S" as it reveals the information that country "Y" has determined would result in serious damage.

AP1. APPENDIX 1

CLASSIFICATION FACTORS

The following questions, answers, and potential actions will assist in systematically determining whether certain broad aspects of an effort warrant security classification:

AP1.1. Is the effort a new generation, a development, or a modification of an existing unclassified system, program, project, or item?

Yes ⇨ Probably not classifiable unless effort represents a significant breakthrough.

NO ⇩ Determine whether the name or title, standing alone, reveals the information that would cause damage

AP1.2. Is it known publicly or reasonably presumed known that the United States is interested in this kind of effort?

YES ⇨ Probably not classifiable

NO ⇩

AP1.3. Is the exact extent of U.S. interest known publicly or reasonably surmised from openly available information?

YES ⇨ Probably not classifiable

NO ⇩ Determine what information would reveal the degree of attainment by the U.S. in the particular field, and how that would be of value to a foreign interest in planning actions detrimental to national security.

AP1.4. Is the REASON for U.S. interest known publicly or reasonably surmised from openly available information?

YES → Probably not classifiable

NO — Determine what information would reveal purpose, goal, or mission of the effort that would cause the actual damage.

AP1.5. Would unauthorized knowledge of U.S. interest in this effort cause or worsen foreign political, economic, or military activities.

YES → Classifiable. The level of classification would be based on the degree of damage to national security.

NO — Not classifiable.

AP1.6. Would unauthorized knowledge, magnitude, or mere fact of the overall effort have a detrimental effect on U.S. national security?

YES → Classifiable. The level of classification would be based on the degree of damage to the national security.

Not classifiable

AP1.7. Would the fact of U.S. interest or accomplishment in the area:

AP1.7.1. Spur foreign interests in a similar effort that would be detrimental to the United States?

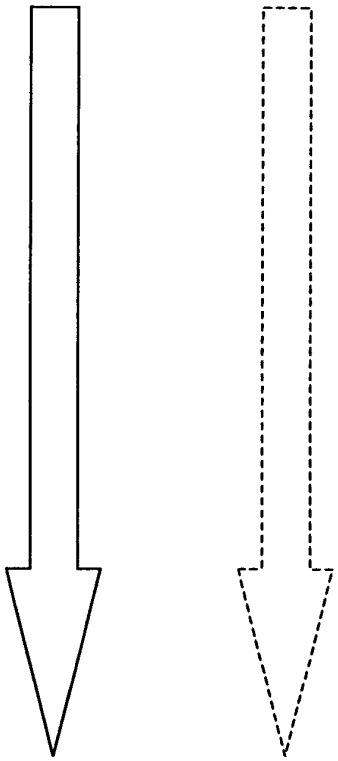
YES → Classifiable. The level of classification would be based on the degree of damage to national security.

AP1.7.2. Spur foreign interests to develop countermeasures which could diminish U.S.advantage? Spur foreign interests in military or political action against the United States or an ally?

AP.1.7.3. Provide foreign interests with propaganda capable of damaging U.S. national security.

AP 1.7.4 Eliminate or significantly diminish required lead time or a valuable element of surprise related to national security?

AP1.7.5. Indicate to foreign interests a lag or failure by the United States to pursue or attain a necessary or expected competence in a particular field related to national security?



NOW CONSIDER CLASSIFYING SPECIFIC DETAILS OF THE EFFORT (AP2. APPENDIX 2).

AP2. APPENDIX 2

CLASSIFYING DETAILS

Having considered the factors involved in making classification determinations concerning the overall effort, it is now necessary to take the second step and consider the classification of certain specific details of the effort. Providing answers to the following questions will assist in systematically reviewing the details of the effort to determine security classification. The questions are not presented in any order of priority. A listing of specific items of information to consider is contained in Appendix 3.

AP2.1. PERFORMANCE OR CAPABILITY

AP2.1.1. What will this do (actual or planned) that is better, faster, or cheaper (in terms of all kinds of resources) than anything like it?

AP2.1.2. How does this degree or kind of performance contribute to or create a national security advantage? How much of an advantage?

AP2.1.3. How long can this data be protected? What is the advantage?

AP2.1.4. How would knowledge of these performance details help an enemy, or damage the success of the effort?

AP2.1.5. Would statement of a particular degree of attained performance or capability be of value to hostile intelligence in assessing U.S. capabilities? Would such a statement spur a foreign nation to similar effort, or to develop or plan countermeasures?

AP2.2. UNIQUENESS

AP2.2.1. What information pertaining to this effort is know or believed to be the exclusive knowledge of the United States?

AP2.2.2. Is it known or reasonable to believe that other nations have achieved a comparable degree of success or attainment?

AP2.2.3. What information, if disclosed, would result in or assist other nations in developing a similar item or arriving at a similar level of achievement?

AP2.2.4. In what way or ways does the uniqueness of this item contribute to a national security advantage?

AP2.2.5. In what way or ways has the end product of this effort or any of its parts been modified, developed, or applied so at to be unique to this kind of effort? How unique is this?

AP2.2.6. Is the method of adaptation or application of the end product or any of its parts the source of the uniqueness and a national security advantage? In what way or ways? Is it in itself a unique adaptation of application in this kind of effort?

AP2.3. TECHNOLOGICAL LEAD TIME

AP2.3.1. How long did it take to reach this level of performance or achievement?

AP2.3.2. How much time and effort have been expended? Was this a special concerted effort or only a gradual developmental type of activity?

AP2.3.3. If all or some of the details involved in reaching this stage of development or achievement were known, how much sooner could this goal have been reached? Which details would contribute materially to a shortening of the time for reaching this goal? Can these details be protected? For how long?

AP2.3.4. Have other nations reached this level of development or achievement?

AP2.3.5. Do other nations know how far we have advanced in this kind of effort?

AP2.3.6. Would knowledge of this degree of development or achievement spur a foreign nation to accelerate its efforts to diminish our lead in this field? What details of knowledge would be likely to cause such acceleration?

AP2.3.7. How important, in terms of anticipated results, is the lead-time we think we have gained?

AP2.3.8. What national security advantage actually results from this lead-time?

AP2.3.9. How long is it practical to believe that this lead-time will represent an actual advantage?

AP2.3.10. How long is it practical to expect to be able to protect this lead-time?

AP2.4. SURPRISE

AP2.4.1. Do other nations know we have reached this level of development or achievement?

AP2.4.2. Will operational use of the end item of this effort give us an immediate advantage that would be less or lost if it were known that we have achieved this particular goal?

AP2.4.3. What is the nature of the advantage resulting from surprise use of this end item?

AP2.4.4. When will this element of surprise be lost?

AP2.5. VULNERABILITIES AND WEAKNESSES

AP2.5.1. What are the weak spots in this effort that make it vulnerable to failure? What is the rate or effect of this failure?

AP2.5.2. How will the failure of the effort in whole or in part affect the national security advantage expected upon completion of this effort, or use of the resulting end item?

AP2.5.3. What elements of this effort are subject to countermeasures?

AP2.5.4. How would knowledge of these vulnerable elements assist in planning or carrying out countermeasures?

AP2.5.5. Can information concerning these weak or vulnerable elements be protected from unauthorized disclosure – or are they inherent in the system?

AP2.5.6. Can these weaknesses or vulnerabilities be exploited to reduce or defeat the success o this effort? How could this be done?

AP2.5.7. What measures are planned or have been taken to offset these weaknesses or vulnerabilities?

AP2.5.8. Are the counter-countermeasures obvious, special, unique, unknown to outsiders or other nations?

AP2.5.9. How would knowledge of these counter-countermeasures assist in carrying out or planning new countering efforts?

AP2.5.10. Would knowledge of specific performance capabilities assist in developing or applying specific countermeasures? How? What would be the effect on the expected national security advantage?

AP2.6. SPECIFICATIONS

AP2.6.1. What would details of specification reveal:

AP2.6.1.1. A special or unusual interest that contributes to the resulting or expected national security advantage?

AP2.6.1.2. Special or unique compositions that contribute to the resulting or expected national security advantage?

AP2.6.1.3. Special or unique levels of performance that are indicative of a classifiable level of achievement or goal?

AP2.6.1.4. Special, or unique use of certain materials that reveals or suggests the source of a national security advantage?

AP2.6.1.5. Special or unique size, weight, or shape that contributes to the resulting or expected national security advantage?

AP2.6.2. Are any specification details contributory to the resulting or expected national security advantage? How?

AP2.6.3. Can details of specifications be protected? For how long?

AP2.7. CRITICAL ELEMENTS

AP2.7.1. What are the things that really make this effort work?

AP2.7.2. Which of these critical elements contribute to the resulting of expected national security advantage? How? To what extent?

AP2.7.3. Are these critical elements the source of weakness or vulnerability to countermeasures?

AP2.7.4. What details of information pertaining to these critical elements disclose or reveal the national security advantage, weakness or vulnerability?

AP2.7.5. Can details of information pertaining to these critical elements be protected by classification? For how long?

AP2.8. MANUFACTURING TECHNOLOGY

AP2.8.1. What manufacturing methods, techniques, or modes of operation were developed to meet the requirements of this effort?

AP2.8.2. Which of these manufacturing innovations are unique to this effort or this product? Are they generally known or suspected?

AP2.8.3. Are these manufacturing innovations essential to successful production of the product?

AP2.8.4. What kind of lead-time results from these innovations?

AP2.9. ASSOCIATIONS

AP2.9.1. Are there any associations between this effort and others that raise classification questions?

AP2.9.2. Are there associations between information in this effort, and already publicly available information (unclassified), that raise classification problems?

AP2.9.3. Is it necessary or possible to classify items of information in this effort because of their association with other unclassified or classified information would diminish or result in the loss of a national security advantage?

AP2.10. PROTECTABILITY

AP2.10.1. Can the information effectively be protected from unauthorized disclosure by classification? For how long?

AP2.10.2. If not, what alternative means can be used to ensure protection?

AP3. APPENDIX 3

ITEMS OF INFORMATION

The following are some items of information that may disclose present or future strategic or tactical capabilities and vulnerabilities and that should be considered when preparing classification guidance:

AP3.1. PERFORMANCE AND CAPABILITIES

- Accuracy
- Alert time
- Altitude
  - Maximum
  - Optimum
- Ballistics
  - Initial
  - Terminal
- Control
- Countermeasures (proven, unproven)
  - Counter-countermeasures
  - Decoys
  - Electronic
  - Penetration aids
  - Shield materials
- Depth/height (also of burst)
  - Maximum
  - Optimum
- Duration (flight)
- Effectiveness
- Frequencies (bands, specific, command, operating, infrared, microwave, radio, comsec)
- Payload
- Penetration
- Range (range scales)
- Rate of fire
- Reaction time
- Reliability/failure rate data
- Resolution
- Response time
- Sensitivity
- Sequence of events
- Signature Characteristics
  - Acceptance
  - Analysis
  - Distinguishment
  - Identification
- Speed/velocity
  - Acceleration/deceleration
  - Cruise
  - Intercept
  - Landing
  - Maximum
  - Minimum
  - Optimum

Heating
Impulse
Intercept
Lethality/critical effects
Lift
Limitations
Maneuverability
Military strength
  Actual
  Planned, predicted, anticipated
Miss distance
Noise figure
Operational readiness time cycle
Stability
Target data
  Details
  Identification
  Illumination
  Impact predicted
  Preliminary
  Priority
  Range determination
Thresholds
Thrust
Toxicity

AP3.2. SPECIFICATIONS

(Detailed, Basic, Subsidiary)

Balance
Burn rate
Capacity (system)
Center of gravity
Codes
Composition
Configuration/contour
Consumption
Energy requirements
  Specific
  Total
Filler
Fineness
Grain configuration
Hardness, degree
Input data
Loading/loads
Mass factor (propellant)
Moment of inertia
On-station time
Output data
Payload
Power requirements
Purity
Size, weight, shape
Stability (static, dynamic)
Strength of members, frames
Stresses
Thickness
Tolerance
Type

AP3.3. VULNERABILITY

- Countermeasures/counter Countermeasures
- Dynamic pressure (supersonic)
- EMP (radiation)
- Ground or air shock
- Jamming
- Signature characteristics
  - Acoustic
  - Electrical
  - Infrared
  - Magnetic
  - Pressure
  - Radar
  - Static overpressure

AP3.4. PROCUREMENT AND PRODUCTION

- Completion date or dates
- Numbers
  - Dispersion (numbers per unit of force)
  - On-hand stockpile
  - Planned or programmed (totals scheduled)
  - Rate of delivery or production
  - Requirements
  - Spares
- Progress/schedules (milestones)
- Stock density
- Supply plans and status
- Tactical deployment

AP3.5. OPERATIONS

- Countdown time
- Deployment data
- Environment
- Location
- Numbers available
- Objectives
  - Mission or program
  - Specific or general
  - Test, broad or detailed
- Plans
  - Command and control
- Results
  - Analysis, conclusions, reports
- Sequence of events
- Staging techniques
- Statement/concept
- Tactical
  - Build-up, units per force activation dates, personnel

AP4. APPENDIX 4

RECOMMENDED FORMAT FOR A SECURITY CLASSIFICATION GUIDE

This Appendix illustrates a format for a security classification guide.

(A cover page is recommended showing essentially the following:)

NAME OF THE PROGRAM, PROJECT, SYSTEM OR STUDY
(If necessary, use an acronym, short title or project number in order to keep title unclassified.)

SECURITY CLASSIFICATION GUIDE

DATE

ISSUED BY: Name and address of issuing office

APPROVED BY: Original Classification Authority.

(Statement of supersession of any previous guides.)

(Distribution Limitation Statement for the Defense Technical Information Center per DoD Directive 5230.24 (reference (e)).)

PROGRAM PROJECT, SYSTEM (ETC.) SECURITY CLASSIFICATION GUIDE

Date:

SECTION 1

GENERAL INSTRUCTIONS

1. Purpose. To provide instructions and guidance on the classification of information involved in (name of the program, project, etc.) using an unclassified identification of the effort.

2. Authority. This guide is issued under authority of (state any applicable Departmental or Agency regulations authorizing or controlling the issuance of guides, such as DoD 5200.1-R, "Information Security Program"). Classification of information involved in (identification of the effort) is governed by, and is in accordance with, (cite any applicable classification guidance or guides under which this guide is issued). This guide constitutes authority, and may be cited as the basis for classification, regrading, or declassification of information and material involved in (identification of the effort). Changes in classification required by application of this guide shall be made immediately. Information identified as classified in this guide is classified by (complete title or position of classifying authority).

3. Office of Primary Responsibility (OPR): This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to:

(Name, code, mailing address of issuing office.)

(An administrative or security office in the issuing activity may be used. Inclusion of the action officer's name and phone number/fax and e-mail is desirable.)

4. Classification Challenges. If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by appropriate authority. Classification challenges should be addressed to the OPR.

5. Reproduction, Extraction and Dissemination. Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved in (identification of the effort), including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR. (NOTE: If it is necessary to classify the guide, you may have to modify this paragraph to express any required limitations.)

6. Public Release. The fact that this guide shows certain details of information to be unclassified does not allow automatic public release of this information. Proposed public disclosures of unclassified information regarding (identification of effort) shall be processed through appropriate channels for approval. (NOTE: It may be desirable to indicate the office to which requests for public disclosure are to be channeled.)

7. Foreign Disclosure. Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in (identify applicable issuances implementing DoD foreign disclosure policy). If a country with which the Department of Defense has entered into a reciprocal procurement memorandum of understanding or offset arrangement, expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation. (If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact should be stated.)

8. Definitions. (Include in this paragraph the definitions of any items for which there may be various meanings to ensure common understanding of the details of information that are covered by the guide.)

SECTION 2

OVERALL EFFORT

9. Identification. (Include in this paragraph any necessary statements explaining the classifications, if any, to be assigned to various statements identifying the effort. These statements should be consistent with other program documentation.)

10. Goal, Mission, Purpose. Include in this paragraph any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that which must be classified. Take care to ensure that unclassified statements do not reveal classified information.)

11. End Item. Include in this paragraph statements of the classification to be assigned to the end products of the effort, whether paperwork or hardware. In this connection it is important to distinguish between classification required to protect the fact of the existence of a completed end item, and classification required because of what the end item contains or reveals. In some instances classified information pertaining to performance, manufacture, or composition of incorporated parts or materials is not ascertainable from mere use of or access to the end item. In others, the classifiable information is that which concerns total performance, capabilities, vulnerabilities, or weaknesses of the end item itself, rather than any of the parts or materials.

SECTION 3

PERFORMANCE AND CAPABILITIES

(This section includes characteristics of performance and capability of an end item, or an end item's components, parts, or materials, the performance or capabilities of which require classification. In this section also provide, in sequentially numbered items, statements that express details of performance and capabilities planned and actual. Include both those elements that warrant classification and those that are unclassified. These statements normally would not set forth the numeric values that indicate degree of performance or capability, planned or attained, but merely should identify the specific elements of performance or capability that are covered. When it is necessary to state certain limiting figures above or below which classification is required, the statement itself may warrant classification. For clarity, continuity, or ease of reference it may be desirable to include performance classification data in the sections dealing with the end item or the components or parts to which the performance data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.)

TOPIC	CLASS	DECLASS	REMARKS
Range			
a. Actual	"S"	15 June 1999	
b. Planned	"U"		
Accuracy/range rate			
a. Predicted	"C"	30 Jan 2000	
b. Measured	"C"	30 Jan 2000	
3. Altitude Operational	"C"	30 Jan 2000	
Maximum	"C"	30 Jan 2000	The statement "in excess of 50,000 feet" is "U."
4. Receiver sensitivity, selectivity, and frequency coverage.	"S"	15 Apr 2005	If standard commercial receivers are used, their characteristics are "U" but their application to this effort shall be "S."
5. Resolution Thermal			Planned or actual attained
a. Maximum attainable	"S"	15 Apr 2001	thermal resolutions above
b. Operational optimum		15 Apr 2001	0.25 degrees C. are "U."
c. Operational attainment	"S"	15 Apr 2001	
6. Speed			
a. Maximum	"S"	15 Jan 2001	Downgrade to "C" upon
b. Rate of climb	"S	15 Jan 2001	IOC.
c. Intercept	"S"	15 Jan 2001	Reference to "supersonic." speed" is "U."

SECTION 4

SPECIFICATIONS

This section includes items of information describing standards for qualities of materials and parts; methods or modes or construction, manufacture or assembly; and specific dimensions in size, form, shape, and weight, that require classification. Classification is required because the items are contributory to the national security advantage resulting from (identification of this effort), or that frequently require classification but are unclassified in (identification of this effort). Classification of specifications pertaining to performance capability are covered in section 3. (Actual figures do not need to be given, merely statements identifying clearly the specific items of information involved. If figures are necessary to establish classification levels, it may be necessary to classify the statements themselves. When necessary for clarity, continuity or ease of reference, specification classification data may be included in sections on the end product or components or parts to which the data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.)

TOPIC	CLASS	DECLASS	REMARKS
1. Burn rate	"C"	17 Sep 2001	
2. Power requirement	"S"	17 Sep 2001	Only when associated with advanced model ##; otherwise "U."
3. Chemical composition	"U"		

SECTION 5

CRITICAL ELEMENTS

This section is used only if there are specific elements that are critical to the successful operation of the end item of this effort, and are unique enough to warrant classification of some data concerning them. Provide in sequentially numbered paragraphs each significant items of information peculiar to these critical elements and the classification applicable. Also include in this section the classification to be assigned to information pertaining to components, parts, and materials that are peculiar and critical to the successful operation of the end item in this effort when such items of information are the reason for or contribute to the national security advantage resulting from this effort. Performance data pertaining to such critical elements can be included in this section instead of section 3.

SECTION 6

VULNERABILITIES AND WEAKNESSES

This section is used to specify classification to be assigned to details of information that disclose inherent weaknesses that could be exploited to defeat or minimize the effectiveness of the end product of this effort. Classification assigned to details of information on countermeasures and counter-countermeasures should be included in this section.

SECTION 7

ADMINISTRATIVE DATA

This section is used only if particular elements of administrative data, such as program information, procurement schedules, production quantities, schedules, programs, or status of the effort, and data on shipments, deployment, or transportation and manuals (field, training, etc.), warrant classification.

TOPIC	CLASS	DECLASS	REMARKS
1. Planned delivery rate.	"C"	13 Mar 2001	See item 3, below.
2. Actual routing of delivery of end items.	"C"	See remarks	Classify upon selection of route, and declassify upon completion of last delivery to site.
3. Shipping dates and and times.	"C"	See remarks	Classify upon decision to ship, and declassify upon arrival at site.

SECTION 8

HARDWARE

The degree of specificity to be included in this section will depend largely upon:

The level from which issued. When issued from a headquarters level, probably the only classification to be applied to hardware would be to the end item itself.

The channels or hands through which the guidance will travel to the ultimate user. The closer the issuer is to the user, the more detailed the guidance may become. Intermediate levels may be required to expand or elaborate on the guidance, and cover more details concerning materials, parts, components, subassemblies, and assemblies, and the classification, if any, to be assigned. Any such expansion or elaboration should be fully coordinated with the headquarters issuing the basic guide.

The ease of determining when classified information could be revealed by a particular hardware item. Obscure connections and associations that could reveal classified information may require the issuer of the guide to state classification for certain hardware items. In such cases it probably would be advisable to explain why classification is necessary.

Whether there are factors that require consideration and action at a headquarters level. National or DoD policy, intelligence data, broad operational requirements, extraneous factors, or other matters not ordinarily available below headquarters, or that require high level consideration may result in decisions to classify certain hardware items.

INFORMATION REVEALING	CLASS	DECLASS	REMARKS
End item hardware:			
a. AN/APR-999	"C"	20 Aug 2000	External views of the assembled AN/AR-999
(1) Analyzer unit	"C"		are "U."
(2) Threat display Unit	"U"	20 Aug 2000	
(3) Preamplifier	"U"		
b. AN/APR-0000	"U"		

AP5. APPENDIX 5

FORMAT VARIATIONS

This Appendix illustrates column headers and arrangements that are different from those used in section AP4. These headers and arrangements may be employed in the construction of your classification guide, and modified to suit your style and need in a given effort. For example, a column for downgrading action would not be necessary if the guide did not provide for it, or if only one or two items of information are to be downgraded. In the later case, the downgrading instruction could be placed in a "Remarks" or "Comments" column.

AP5.1. Example 1

TOPIC	CLASS	DECLASS	COMMENTS
1.4.1. System capacity	"S"	30 Jun 2004	Downgrade to "C" upon IOC.
1.4.2. Signature characteristics	"C"	19 Jun 2001	

AP5.2. Example 2

DESCRIPTION	CLASS	UNTIL	REMARKS
1.4.1. System capacity	"S"	30 Jun 2004	Downgrade to "C" upon IOC.
1.4.2.	"C"	19 Jun 2001	

AP5.3. Example 3

INFORMATION REVEALING	CLASSIFICATION/DECLASSIFICATION	REMARKS
1.4.1. System capacity	"S" DCL on 30 Jun 2004	Downgrade to "C" upon IOC.
1.4.2. Signature characteristics	"C" DCL on 19 Jun 2001	