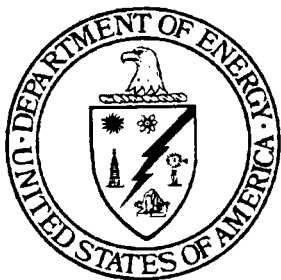


UNCLASSIFIED



CG-IN-1

DOE Classification Guide for Intelligence Information (U)

August 2001

U.S. DEPARTMENT OF ENERGY
Office of Classification
and Information Control
Washington, DC 20585

Chapter 1	Intelligence Administration and Information Management (U)
Chapter 2	Applied Technologies for Intelligence Information (U)
Chapter 3	Foreign Intelligence Information (U)
Chapter 4	Imagery Intelligence (U)

DELETED VERSION

UNCLASSIFIED

Classified by: Edith A. Chalk, Director
Technical Guidance Division
Derived from: CG-SS-4, 9/11/00
Declassify on: 25X1; When released by the DCI/FBI.

Department of Energy Declassification Review	
1 st Review Date: <u>2/7/06</u>	Dispositions (Circle Number(s))
Authority: DC DD	<input checked="" type="radio"/> 1. Classification Retained
Name: <u>W. Schmidt</u>	<input type="radio"/> 2. Classification Changed To:
	<input type="radio"/> 3. Contains No DOE Classified Info.
	<input type="radio"/> 4. Coordinate With:
2 nd Review Date: <u>2/7/06</u>	<input type="radio"/> 5. Classification Canceled
Authority: DC DD	<input checked="" type="radio"/> 6. Classified Info Bracketed
Name: <u>Ronald P. Cannon</u>	<input type="radio"/> 7. Other (Specify):

CLASSIFICATION/CONTROL GUIDANCE REQUEST

NAME: _____ DATE: ___/___/___

ORGANIZATION: _____ PHONE NUMBER: _____

SHORT TITLE OF GUIDANCE: _____

LONG TITLE OF GUIDANCE: _____

CHECK THE APPLICABLE AREA AND ENTER THE REQUIRED INFORMATION

___ I NEED ___ COPIES OF THIS GUIDANCE
JUSTIFICATION: _____

___ CHANGE OF ADDRESS: _____

___ PLEASE REMOVE MY NAME FROM THE DISTRIBUTION LIST

___ I TRANSFERRED MY COPY OF THIS GUIDANCE TO: _____

ORGANIZATION: _____

___ I MADE ___ COPIES OF THIS GUIDANCE FOR: _____

ORGANIZATION: _____

INSTRUCTIONS:

You may FAX this to the Classification Guidance Administrator, SO-10.24, at (301) 903-7444.

DOE Headquarters Elements: Send this request to the Production and Analysis Division, Office of Classification and Information Control, SO-10.2.

NNSA Headquarters Elements: Send this request to the Classification and Controlled Information Division, National Nuclear Security Administration Service Center.

Field Elements: Send this request to your local classification officer.

NOTE: THIS SAMPLE MAY BE REPRODUCED AS NEEDED; OTHER FORMATS ARE ACCEPTABLE AS LONG AS THE REQUIRED INFORMATION IS PROVIDED.



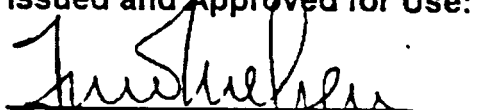
CG-IN-1

DOE Classification Guide for Intelligence Information (U)

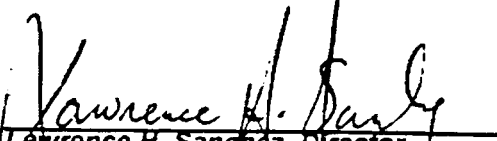
U.S. DEPARTMENT OF ENERGY

Office of Nuclear and National
Security Information
and
Office of Intelligence
Washington, DC 20585

Issued and Approved for Use:


Finn K. Neilsen, Acting Director
Office of Nuclear and National
Security Information
U.S. Department of Energy

8/13/01
DATE


Lawrence H. Sanchez, Director
Office of Intelligence
U.S. Department of Energy

08/08/01
DATE

Classified By: Andrew P. Weston-Dawkes,
Director, SO-222
Derived From: CG-SS-3, 10/16/95; CG-SS-4, 9/11/00
Declassify On: X1, X8

CG-IN-1
DOE Classification Guide for Intelligence Information (U)

RECORD OF PAGE CHANGES

Change Number:	Date of Change:	Entered by (Initial/Date):
Change 1	11/04	SO-10.2

CG-IN-1
DOE Classification Guide for Intelligence Information (U)

TABLE OF CONTENTS

INTRODUCTION

A. Use of Guide	Intro-1
B. Scope	Intro-1
C. Cancellation	Intro-3
D. Authority	Intro-3
E. Classification Categories and Levels	Intro-3
F. Use of the Designation "U"	Intro-4
G. Foreign Government Information (FGI)	Intro-4
H. Official Use Only (OUO) Information	Intro-5
I. Marking Of Documents	Intro-6
J. Special Considerations	Intro-7
K. Ranges in Classification Levels	Intro-8
L. Format of Topics	Intro-8
M. Obtaining Copies of a Guide	Intro-11
N. Questions/Suggestions	Intro-11

CHAPTER 1 - INTELLIGENCE ADMINISTRATION AND INFORMATION MANAGEMENT (U)

A. General Information	1-1
B. Broad Guidance	1-1
C. Topics	1-4
110 Intelligence Sources, Methods, Activities, Objectives, or Correlation to Intelligence Activities	1-4
120 Intelligence Administration	1-5
130 Information Management and Sensitive Compartmented Information Facility (SCIF) Management	1-6

CHAPTER 2 - APPLIED TECHNOLOGIES FOR INTELLIGENCE INFORMATION (U)

A. General Information	2-1
B. Broad Guidance	2-1
C. Topics	2-2
210 Applied Technologies	2-2

TABLE OF CONTENTS

Continued

CHAPTER 3 - FOREIGN INTELLIGENCE INFORMATION (U)

A. General Information	3-1
B. Broad Guidance	3-1
C. Topics.....	3-4
310 Intelligence Sources, Methods, Activities, Objectives, or Correlation to Intelligence Activities.....	3-4
320 Foreign Relations and Intelligence Information.....	3-4
330 Analyses of Foreign Activities	3-5
340 Classification of Information Based Upon the Source of Information.....	3-6

CHAPTER 4 - IMAGERY INTELLIGENCE (U)

A. General Information	4-1
B. Broad Guidance	4-1
C. Topics.....	4-2
410 Imagery Products, Sources, and Activities	4-2

APPENDIX A - DEFINITIONS

CG-IN-1

DOE Classification Guide for Intelligence Information (U)

INTRODUCTION

A. Use of Guide

(U) This guide is approved for use by Derivative Classifiers and Derivative Declassifiers within their programmatic areas of expertise. Topics in this guide contain guidance for determining whether information is classified or unclassified. If the information concerns a specific Department of Energy (DOE) or National Nuclear Security Administration (NNSA) site or program, a local guide pertaining to that site or program may have been issued and should be consulted. If the work being performed is not funded by DOE or NNSA and the funding organization has not issued a classification guide, this classification guide shall be used.

(U) This guide is approved for use by any DOE or NNSA employee or contractor for determining whether information is Official Use Only (OUO).

B. Scope

(U) This guide addresses classification guidance pertaining to intelligence activities performed by DOE or DOE contractors. Classified information concerning intelligence includes information that could: (1) provide meaningful assistance to an adversary in gaining unauthorized access to classified or sensitive information; (2) expose sensitive intelligence sources or activities that could compromise U.S. Intelligence Community (IC) activities; (3) weaken or eliminate IC abilities to identify and neutralize specific or general categories of adversarial activities targeting U.S. resources and information; (4) hamper or compromise U.S. IC capabilities to conduct information-gathering activities against adversarial targets; or (5) reveal strategies in countering the threat. For guidance regarding Sensitive Compartmented Information (SCI),

see Director Central Intelligence Directive (DCID) 6/6.

(U) This guide applies to all DOE elements and covered contractors performing work for DOE as provided by law and/or contract that have access to classified intelligence information and documents or that generate documents containing such information.

(U) This guide applies to intelligence related work-for-others activities where no other sponsoring agency or DOE guidance has been promulgated.

~~(OUO)~~ The mission of the Office of Intelligence (IN-1) is to:

1. (U) ensure effective use of the United States (U.S.) Government's intelligence system in support of the DOE's needs for information on global nuclear weapons development, nonproliferation, and nuclear and other energy production and consumption; and
2. (U) as a member of the IC, contribute to the IC mission with intelligence analysis and technology in DOE areas of expertise.

(U) Pursuant to Executive Order (E.O.) 12333, *United States Intelligence Activities*, the Department of Energy as a member of the IC shall:

Participate with the Department of State in overtly collecting information with respect to foreign energy matters;

Produce and disseminate foreign intelligence necessary for the [Department of Energy] Secretary to fulfill his/her responsibilities;

~~SECRET//NOFORN~~

Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

Provide expert technical, analytical, and research capability to other agencies within the IC.

~~(U)~~ Pursuant to Section 1.7 of E.O. 12333, the Secretary of Energy as the Senior Official of the Intelligence Community of DOE, or his/her designee, shall:

(U) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the Secretary of Energy, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

~~(U)~~ In any case involving serious or continuing breaches of security, recommend to the Attorney General that the case be referred to the FBI for further investigation; [For classification regarding such referrals, see the *DOE Classification Guide for Counterintelligence Information*]

(U) Furnish the Director of Central Intelligence (DCI) and the National Security Council (NSC), in accordance with applicable law, the information required for the performance of their respective duties;

(U) Report to the President's Intelligence Oversight Board, and keep the DCI appropriately informed, concerning any intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive;

(U) Protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the DCI;

(U) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the DCI;

(U) Instruct DOE employees and its contractors to cooperate fully with the President's Intelligence Oversight Board; and

(U) Ensure that the Inspector General and General Counsel have access to any information necessary to perform their duties assigned by E.O. 12333.

(U) The Secretary of Energy has designated the Director, Office of Intelligence (IN-1), as the Senior Intelligence Official for DOE.

(U) Associated functions of the Director, IN-1, that have classification concerns include:

Serving as the senior DOE representative to the National Foreign Intelligence Board (NFIB);

Developing policy and establishing procedures related to the provision and use of intelligence information concerning foreign energy situations and hostile threats;

Executing internal oversight for all DOE intelligence-related activities, in accordance with E.O. 12333;

Planning, directing, and managing the DOE Intelligence Program. Serving as the Senior Intelligence Officer for all DOE intelligence and intelligence-related activities;

Appointing DOE representatives to the committees, panels, and boards of the NFIB and other Intelligence Community bodies;

Designating authorized channels for receipt and use of intelligence within the DOE and its contractors;

Providing for a flow of intelligence to DOE policy officials and analysts;

~~SECRET//NOFORN~~

Establishing policies and procedures for the protection of all foreign intelligence information provided to DOE and its contractors;

Providing feedback to Intelligence Community members from DOE policy makers on the usefulness and timeliness of their intelligence reporting;

Conducting continuous intelligence requirement surveys on other DOE elements to ensure that overall DOE intelligence requirements are clearly articulated;

Coordinating, developing, and justifying the DOE intelligence and related budgets and DOE inputs to the National Foreign Intelligence Program budget;

Managing the DOE-sponsored Intelligence Community Education, Training, and Awareness Program;

Managing, coordinating, and sponsoring within the Intelligence Community, all DOE collection requirements for foreign intelligence information;

Managing DOE's intelligence and intelligence-related reimbursable work-for-others program; and

Developing and providing specialized technology applications to meet short-term national security requirements and technical support to varied operational missions across the Federal government's intelligence, special operations/warfighter, and law enforcement communities.

C. Cancellation

(U) No classification guides or bulletins are superseded by this guide.

D. Authority

(This portion is Unclassified.)

1. Statutory/Executive Order Authorities

E.O. 12958, *Classified National Security Information*, is the authority to classify certain

information that requires protection from unauthorized disclosure because it could cause damage to the national security.

The Freedom of Information Act (5 U.S.C. §552) is the authority for DOE's OIU program that controls unclassified but sensitive information.

2. Agency Directives

DOE M 475.1-1A, *Identifying Classified Information*, contains specific responsibilities, policies, and procedures for managing and administering DOE's classification program.

DOE O 471.3, *Identifying and Protecting Official Use Only Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, contain specific responsibilities, policies, and procedures for managing and administering DOE's program for identifying and protecting information as OIU.

Non-DOE, including non-NNSA, funded work that may generate classified information is conducted in accordance with DOE O 481.1B, *Work for Others (Non-DOE Funded Work)*, and accompanying classification guidance is developed and certified following instructions in DOE M 475.1-1A, Chapter V, paragraph 3c.

E. Classification Categories and Levels

(This portion is Unclassified.)

Each topic designating information as classified must identify both the classification category and the classification level. Classification categories and levels are defined as follows:

1. Classification Categories

Restricted Data (RD). Classified information that concerns (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, except for that information that

has been declassified or removed from the RD category under section 142 of the AEA.

Formerly Restricted Data (FRD).

Classified information concerning the military utilization of atomic weapons that has been removed from the RD category under section 142d of the AEA.

National Security Information (NSI).

Classified information that has been determined under E.O. 12958 or any predecessor Executive order to require protection against unauthorized disclosure.

2. Classification Levels

The following levels of classification, listed in descending order of sensitivity, are applied to any category of classified information:

Top Secret (TS). Information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

Secret (S). Information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

Confidential (C). Information whose unauthorized disclosure could reasonably be expected to cause either undue risk to the common defense and security (if RD or FRD information) or damage to the national security (if NSI).

F. Use of the Designation "U" (This portion is Unclassified.)

Certain topics in this guide contain the designation "U" indicating that the information is not classified. However, such information is not automatically approved for release to the public as it may be subject to other controls that are *outside* of the context of this guide.

G. Foreign Government Information (FGI)

(This portion is Unclassified.)

Under E.O. 12958 the unauthorized disclosure of FGI is presumed to cause damage to the national security. Therefore, it is important to understand FGI and the proper instructions for classification.

FGI is defined in E.O. 12958 as:

- a. Information provided to the United States (U.S.) Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
- b. Information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or,
- c. Information received and treated as "Foreign Government Information" under the terms of a predecessor Executive order.

FGI is classified based on whether the foreign government or international organization protects the information itself and expresses the desire that the United States also protect the information. Such expression may be formal (e.g., foreign classification markings, memoranda) or informal (e.g., verbal request, established precedents).

A document containing FGI retains its original classification markings or is assigned a U.S. classification marking that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Such documents need not be re-marked with U.S. classification markings if the foreign markings provide immediate recognition that the information requires special protection and control and are clear as to the level of protection required.

FGI must receive a degree of protection at least equivalent to that used by the originating foreign government or international organization. Therefore, if re-marking is necessary, it is important to select the appropriate U.S. classification level (Confidential, Secret, or Top Secret). In cases where the information is protected by the foreign government or international organization by standards less restrictive than the safeguarding standards that apply to U.S. "Confidential" information, the information may be identified as Confidential/Foreign Government Information-Modified Handling Authorized or C/FGI-MOD. Access to Top Secret, Secret, or Confidential FGI requires an appropriate access authorization and need-to-know. Access to C/FGI-MOD does not require an access authorization, but is based on whether the individual has a need to know the information to perform official duties.

A document provided to the U.S. by a foreign government may be returned to that foreign government regardless of any re-marking. If the documents were re-marked with an equivalent U.S. classification marking or a cover sheet added, then the U.S. markings are crossed out and the cover sheet is removed before the document is returned. However, if U.S. personnel added value to the information (e.g., through an analysis by U.S. experts), a Derivative Classifier must review the resulting document. If the document contains U.S.-produced FGI (e.g., an assessment of a foreign government's nuclear weapons storage facility conducted by DOE staff) at the C/FGI-MOD or unclassified level, it may be provided to the pertinent foreign government or international organization. However, if it contains any U.S. classified information, then it can only be provided to the foreign government or international organization under an existing classified information exchange agreement (i.e., for RD/FRD, an agreement for cooperation under the AEA is required; for NSI, a specific country-to-country agreement is required).

H. Official Use Only (OUO) Information (This portion is Unclassified.)

Certain unclassified information may be exempt from public release under the Freedom of Information Act (FOIA) if it has the potential to damage governmental, commercial or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE authorized activities. Such information is designated as OUO. Generally, a program or support office decides whether information under its cognizance is OUO. In this case, the Office of Intelligence (IN-1), has decided that information identified by specific topics in this guide is OUO. Any document containing such information must be marked as OUO.

Each topic that indicates information is OUO includes a notation of the proper FOIA exemption number and category to insert in the OUO front marking. A description of these categories follows. For a full discussion of the exemptions see DOE G 471.3-1, *Guide to Identifying Official Use Only Information*.

Exemption 2 - Circumvention of Statute.

Protects the internal workings of an agency that would allow someone to violate a law or agency regulation and avoid detection. (Examples: General guidelines for conducting investigations; vulnerability assessments; inspection and appraisal procedures; unclassified (and otherwise uncontrolled) portions of information classification and control guidance; agency computer access codes.)

Exemption 3 - Statutory Exemption.

Protects information whose disclosure is specifically protected by law and is not otherwise controlled. (Example: The Federal Technology Transfer Act allows Federal agencies to protect for 5 years any commercial and business confidential information that results from a Cooperative Research and Development Agreement with a non-Federal party.)

Exemption 4 - Commercial/Proprietary.

Protects trade secrets and commercial or financial information obtained from a person which would cause substantial competitive harm to the source if disclosed. (Examples: Commercial or financial information in connection with bids, contracts, or proposals and other related information received in confidence; scientific and manufacturing processes or developments submitted with a contract proposal.)

Exemption 5 - Privileged Information.

Protects the three primary statutory privileges: (1) Deliberative Process Privilege, which protects the Government's decision-making process, (2) Attorney-Work Product Privilege, which protects documents and other memoranda prepared by an authority in contemplation of litigation and (3) Attorney-Client Privilege, which protects private communications between an attorney and a client concerning a legal matter for which the client has sought professional advice. (Examples: Letters, memoranda, issue papers, reports, and other documents that contain advice, opinions, or recommendations on new or revised Government decisions and policies.)

Exemption 6 - Personal Privacy. Protects personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. (Examples: Personnel records; health records; security records.)

Exemption 7 - Law Enforcement. Protects information compiled for law enforcement purposes. (Examples: Witness statements; identity of firms or individuals being investigated for alleged irregularities involving contracting with DOE when no indictment has been obtained; information obtained in confidence in the course of a criminal investigation; law enforcement manuals.)

Exemption 8 - Financial Institutions.

Protects information for the use of any agency responsible for the regulation or supervision of financial institutions. (Examples: Bank examination reports; documents related to bank examination reports such as discussions of findings.)

Exemption 9 - Wells. Protects information concerning geological and geophysical information and data, including maps, concerning wells. (Examples: Number, location and depth of proposed uranium exploration drill holes.)

I. Marking Of Documents

(U) Derivative Classifiers and Derivative Declassifiers ensure that documents determined to contain classified information are marked appropriately. DOE M 471.2-1C, *Classified Matter Protection and Control Manual*, contains complete information on marking requirements. Documents containing any RD or FRD should not be portion marked (unless required by agreement with another agency when preparing joint documents). However, documents containing only NSI must be portion marked as required by E.O. 12958.

(U) The marking of intelligence information shall conform to the *Intelligence Community Classification and Control Markings Implementation Manual (U)* published by the Director of Central Intelligence (DCI). Intelligence information, whether originally generated within the IC or not, may have additional dissemination and declassification restrictions imposed upon it.

(U) Some intelligence documents may also be marked with "MR" for manual review, and is used in cases where E.O. 12958 requirements are superseded by statute, treaty, or other agreement. The designation of "MR" is applied to material that:

1. (U) The declassification is based upon a specific event;
2. (U) The declassification block shows that the source was marked OADR (Originating Authority Determination Required); and/or
3. (U) The material contains RD, FRD, or North Atlantic Treaty Organization (NATO) information.
4. (U) The information is FGI.

~~(OUO)~~ In this guide, the NOFORN (NF) marking, which stands for No Foreign Dissemination or Not Releasable to Foreign Nationals, is used. This marking indicates that the information contained in the document may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval. U.S. classified information is considered to be not releasable to foreign nationals unless otherwise designated, consistent with provisions of the "National Disclosure Policy." Pursuant to DCID 6/6, some of the information classified from and within the Intelligence Community is designated as "Not Releasable to Foreign Nationals" or "NOFORN". Regardless of whether the material has been marked as "NOFORN" or not, the limitation of being not releasable to foreign nationals is to be assumed unless specifically otherwise designated.

(U) The employee who determines a document contains OUO information ensures it is marked appropriately. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, contains complete information on marking requirements.

J. Special Considerations (This portion is Unclassified.)

Inconsistent Guidance. Inconsistent guidance may be ambiguous, outdated, or in conflict with other guidance. When such guidance is encountered, the Derivative Classifier or Derivative Declassifier must seek clarification from the local Classification Officer.

No Guidance. If a Derivative Classifier or Derivative Declassifier cannot determine the proper classification of an element of information using guidance approved for his/her use, the Derivative Classifier or Derivative Declassifier must contact the appropriate classification office for assistance.

"No Comment" Policy. Occasionally, classified information appears without

authorization in the public domain. Commenting on the accuracy, classification, or technical merit of the information or quoting from such information is prohibited. For further information on the "No Comment" policy, see Classification Bulletin GEN-16, *No Comment Policy for Classified Areas*.

Association. The significance of information often depends upon its context. Therefore, two unique pieces of unclassified information when considered together may reveal classified information. Similarly, two unique pieces of classified information may reveal information classified at a higher level. If the decision to classify is based on a topic, then a Derivative Classifier may make the decision. If the decision is not based on a topic, the local Federal Classification Officer with original classification authority must make the decision for NSI and the Director, Office of Classification and Information Control (SO-10.2), must make the decision for RD/FRD information. When two portions of a portion-marked document are classified based on their association, both portions must be portion marked at the same level and category.

Compilation. A document may be classified because of compilation when a large number of qualitatively similar pieces of unclassified information considered together contain some added value (such as the completeness or comprehensiveness of the information) that warrants classification. If the decision to classify is based on a topic, then a Derivative Classifier may make the decision. If the decision is not based on a topic, the local Federal Classification Officer with original classification authority must make the decision for NSI and the Director, SO-10.2, must make the decision for RD/FRD information. A document classified for this reason is never portion marked and must contain the following statement: "This document has been classified under the compilation concept and shall not be used as the source for a derivative classification decision."

REMINDER: Derivative Classifiers and Derivative Declassifiers are not authorized to use source documents as a basis for classifying another document unless the information in the document is entirely under the purview of another agency, foreign government, or international agency and no applicable guidance exists.

**K. Ranges in Classification Levels
(This portion is Unclassified.)**

A topic in a classification guide may show a range for the classification level. For example:

- U-TS Classification level can be from Unclassified to Top Secret
- U/TS Classification level is either Unclassified or Top Secret

In either case, subtopics or *NOTES* explain when each classification level applies.

**L. Format of Topics
(This portion is Unclassified.)**

RD and FRD Topics. The format of these topics is as follows:

1000 Guidance topic vCat

where

v = Classification level (TS, S, C)

Cat = Category (RD or FRD)

NSI Topics. E. O. 12958 and its implementing directive require that classification guides provide consistent reasons for classification of NSI and either prescribe declassification instructions or identify categories for exemption from automatic declassification after 25 years. Reasons for classification of NSI are:

- 1.4(a) military plans, weapons systems, or operations;
- 1.4(b) foreign government information;
- 1.4(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

1.4(d) foreign relations or foreign activities of the United States, including confidential sources;

1.4(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

1.4(f) United States Government programs for safeguarding nuclear materials or facilities;

1.4(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

1.4(h) weapons of mass destruction.

If the information is not exempt from declassification after 25 years, the following notation is used:

1000 Guidance topic vNSI[sched]

where

v = Classification level (TS, S, C)

sched = Schedule for declassification. The schedule indicates a specific declassification date (date), a specific event (EV) for declassification, or the duration of time (dur) in years that the information is to remain classified.

Some topics may not include a declassification schedule. In those instances, the topic notes will refer to other topics within the guide, in another DOE guide, or in another agency guide containing specific classification and declassification instructions.

If a specific date (mm/dd/yy) is given, the information identified is declassified on that date.

If a specific event (EV) is given, the information is declassified when the event noted in the topic occurs. If the same event applies to a group of topics

within a section, the event may be noted in the appropriate section topic rather than each individual topic.

If a duration (dur) is given, the information is declassified that number of years from the date of the document.

When the information is exempt from automatic declassification after 25 years, the following notation is used:

1000 Guidance topic **vNSI**
[25Xn; sched]

where

25X indicates the information is exempt from automatic declassification at 25 years.

n indicates the appropriate exemption category or categories from E.O. 12958. Only the exemptions that are mostly likely to occur are listed in the topics. Other exemptions may apply and may be used at the discretion of the Derivative Classifier.

sched indicates the schedule for declassification as previously noted. The schedule will be a date, event, or duration beyond 25 years. A specific date, event, or duration for declassification must be given unless the exemption pertains to the identity of a confidential human or human intelligence source, which is never automatically declassified (and is marked as "25X1-human.")

NOTE: If the event occurs before 25 years, the information is declassified at that time.

Twenty-five year exemption categories in E.O. 12958 are:

25X1: reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the

application of an intelligence source or method;

25X2: reveal information that would assist in the development or use of weapons of mass destruction;

25X3: reveal information that would impair U.S. cryptologic systems or activities;

25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

25X5: reveal actual U.S. military war plans that remain in effect;

25X6: reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

25X7: reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

25X8: reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security;

25X9: violate a statute, treaty, or international agreement.¹

Examples:

2000 The fact that...

CNSI
[11/25/15]

¹ When 25X9 is used, a determination is made that the information is subject to a statute, treaty or international agreement that formally prevents its declassification. The statute, treaty or international agreement will be identified in a topic note.

Explanation: Topic 2000 is CNSI and this fact is declassified on November 25, 2015.

3000 Information reveals... SNSI[10]

Explanation: The information in topic 3000 is SNSI and is declassified in 10 years. A document containing such information should be marked with a date (mm/dd/yy) for declassification 10 years from the date of the document.

4000 Information reveals... SNSI[EV]

NOTE: The information will be declassified when....

Explanation: The information in topic 4000 is SNSI and is declassified when a particular event occurs. The note will define a specific event as a declassification instruction; for example, when a security vulnerability has been corrected or a facility has been closed. A paraphrase of this note must be included on the "Declassify On" line on the document. The information is not exempt from automatic declassification at 25 years.

5000 Information reveals... SNSI [25X2, 8; 40]

Explanation: The information in topic 5000 is SNSI and is exempt from automatic declassification at 25 years because it reveals information that would assist in the development or use of weapons of mass destruction (25X2) and reveals information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security (25X8). A document containing such information should be marked

with a date (mm/dd/yy) for declassification 40 years from the date of the document.

6000 Information reveals... SNSI [25X2; EV]

NOTE: This information will be declassified when... the technology is no longer in use and official disclosure of the technology and its use have been made.

Explanation: Topic 6000 is SNSI and is exempt from automatic declassification at 25 years because it reveals information that would assist in the development or use of weapons of mass destruction (25X2). The note will define a specific event as a declassification instruction; for example, when a proliferation detection technology is no longer in use and official disclosure of its technology and use have been made. A paraphrase of this note must be included on the "Declassify On" line on the document. If the specified event occurs before 25 years, the information will be declassified at that time.

7000 The fact that... CNSI [25X1-human]

Explanation: Topic 7000 is CNSI and concerns a confidential human source or a human intelligence source (25X1). The marking "25X1-human" denotes that the identity of a confidential human source or human intelligence source is never automatically declassified.

8000 The fact that... CNSI [25X9; EV]

NOTE: This fact is subject to the Nuclear Non-Proliferation Treaty and will be declassified when...

Explanation: Topic 8000 is CNSI and is exempt from automatic declassification because it reveals Foreign Government

Information (25X9). The information is exempt from automatic declassification at 25 years and will be declassified when an event occurs. The note will specify the statute, treaty or international agreement that formally prevents its declassification and will define a specific event for declassification. A paraphrase of this note must be included on the "Declassify On" line on the document. If the specified event occurs before 25 years, the information will be declassified at that time.

9000 Information reveals... U-SNSI

NOTE: Refer to the appropriate program guidance for classification and declassification instructions.

Explanation: The classification level of topic 9000 may range from U to SNSI. Refer to the appropriate program guidance for classification and declassification instructions.

M. Obtaining Copies of a Guide (This portion is Unclassified.)

Unless otherwise indicated on the guide or by SO-10.2, local copying of a guide is permitted. However, to ensure that each person with a copy of a guide receives change notices and revisions, the person's name must be on a distribution list for that guide maintained by Headquarters or the local Classification Officer.

Inside the front cover of this guide is a Classification/Control Guidance Request that

may be used to obtain guides or to report distribution changes.

N. Questions/Suggestions (This portion is Unclassified.)

Any comments or suggestions may be forwarded through the local classification office to the Production and Analysis Division Director using the Classification Issue/Comment Sheet inside the back cover of this guide. The completed comment sheet can be sent, as appropriate, to the following classified or unclassified addresses:

Classified Address

Production and Analysis Division
Office of Classification and Information
Control
Attention: SO-10.2 (*Intended Recipient*)
U.S. Department of Energy
P.O. Box A
Germantown, MD 20875-0963

Unclassified Address

Production and Analysis Division
Office of Classification and Information
Control
SO-10.2/Germantown Building
U.S. Department of Energy
1000 Independence Avenue, SW.
Washington, D.C. 20585-1290

For questions concerning administrative aspects or distribution of the guide, please contact the Technical Guidance Administrator at (301) 903-3417.

~~SECRET//NOFORN~~

THIS PAGE INTENTIONALLY LEFT BLANK

~~SECRET//NOFORN~~

CHAPTER 1

INTELLIGENCE ADMINISTRATION AND INFORMATION MANAGEMENT (U)

A. General Information

(U) All Information Systems (IS) processing intelligence information will be accredited by the Department of Energy's Senior Intelligence Officer (SIO), who is also the Director of the Office of Intelligence.

(U) In addition to hardware and software security measures (collectively referred to as IS security measures), other security measures, such as physical security, communications security (COMSEC), and transient electromagnetic pulse standard (TEMPEST) are applied to IS. In evaluating vulnerabilities of IS, the overall security system must be addressed, not just one or a few of its components.

(U) In classification determinations involving IS, it is essential to understand that it is the information that is classified and that classification markings are applied to the objects or media that contain or convey information. It is the information that can be revealed, not the medium through which it is conveyed, that must be evaluated for classification. With this concept in mind, the term "classified IS" is a short title meaning that an IS has been approved for processing classified information and that it may or may not currently contain classified. An "unclassified IS" is one that has not been approved for processing classified information.

(U) There are circumstances where it must be presumed that a particular storage medium (e.g., removable diskette) may contain classified information and, therefore, must be protected. When a diskette is introduced into a classified IS and is used to record unclassified information, there is the potential to unknowingly write classified information onto the diskette as extra

segments embedded in the unclassified file. There are many ways that such a compromise of classified information could occur. If a storage medium is removed from a classified IS, the medium should be assumed to contain classified information until it is determined otherwise.

(U) When classified information is inadvertently stored in or transferred through a previously unclassified IS, then the system must be protected at the highest level and category of the classified information. Only when the IS has been sanitized by an approved method and is free of the classified information may it revert to an unclassified IS. When all of the system's components cannot have the classified information eliminated, then such components require removal and replacement or the application of other approved mitigating countermeasures.

B. Broad Guidance

(U) Systems that process classified information provide potentially lucrative targets for compromise. In conjunction with the security measures required at IS facilities processing classified information, necessary precautions must be taken to protect details of those IS security measures, themselves, that meaningfully aid in their own subversion. The basic principle underlying classification policy for IS security is to protect information that is of meaningful assistance in gaining unauthorized access to the classified information being processed using an IS.

(U) Some IS software and its security features may require classification to ensure that the programming and security features are not defeated. There are some security features (e.g., the use of access passwords or encryption algorithms) the existence of

which are not, and cannot be, classified, although lists of actual passwords for classified IS or details of encryption are classified.

(U) In order to protect intelligence activities and information, it may be necessary to classify certain facets of information not already officially released that could disclose the following:

- (U) Organizational structure of an intelligence community (IC) agency;
- (U) Numbers and assignments of such agency's personnel;
- (U) Size and composition of the budget for such an agency, or for all or any part of the National Foreign Intelligence Program (NFIP);
- (U) Logistical and associated support activities, including those applicable to the fields of communications and IS; or

•

DOE
b(1)

(U) The most difficult area in classification policy for IS security involves IS software vulnerabilities. Software is one of the most complex parts of a system and rarely can be described as absolutely "bug-free." It is important to note that the analysis, characterization, and classification of IS vulnerabilities must include all aspects of the security of the total system. This includes system hardware as well as software, plus system operations management, and the various types of other access restrictions that may be present, such as physical security. The classification level of information concerning IS vulnerabilities is determined by

the sensitivity of the information accessible through exploitation of the vulnerabilities identified in this total system and by the level of detail revealed about the vulnerabilities.

(U) Information describing the nature or location of an IS vulnerability may be handled separately and classified differently from the descriptions of the procedures required to remove/mitigate the vulnerability. Once a vulnerability has been eliminated, by either temporary or permanent methods, the fact of its prior existence is unclassified, unless its existence, or details thereof, lead to a new or continued vulnerability. The description of a vulnerability that has been corrected remains classified until it has been determined that it does not exist or has been corrected in all classified IS. A vulnerability is considered to be corrected if procedural or other types of interim actions to prevent its exploitation have been instituted, even though permanent hardware or software solutions remain to be implemented.

(U) In situations where interim actions only limit exploitation, the vulnerability information remains classified but at a lower level than when there are no such actions. Classified information stored and processed by an IS is of two types: (1) information involving subject matter classified by other guidance; and (2) information involving the IS itself that makes it possible to gain unauthorized access to the first type of information. Classification of IS security information, as such, is designed for the sole purpose of protecting the classified information that is stored or processed by the system.

(U) Specifically, the following types of information are classified:

•

DOE
b(1)

- (U) Justifications and details concerning budget submissions that reveal classified mission details or submissions for the National Foreign Intelligence Program budget;

- (U) Intelligence methods, sources, or activities; including strategies, targets, or objectives;
- (U) Information pertaining to intelligence-related methodologies, techniques, formulas, equipment, programs, or models, including computer simulations, ranging from initial requirements through planning, source acquisitions, contract initiation, research, design, testing, production, training, and operational use;
- (U) Information that could identify research, procedures, or data used in the acquisition and processing of foreign intelligence or counterintelligence or the production of finished intelligence, when such identification could reveal the particular intelligence interest, the value of the intelligence, or the extent of knowledge of a particular subject of intelligence or counterintelligence interest;
- (U) Information that could reveal, jeopardize, or compromise a cryptographic device, procedure, or system or intelligence data resulting from the employment of such device, procedure, or system or the sites, facilities, systems, and technologies used or proposed for use in collection, interpretation, evaluation, or dissemination of signals intelligence; and
- (U) Information that could disclose criteria and procedures for the handling of critical intelligence that could affect the national security of the U.S. or its allies and that requires the immediate attention of senior officials.

C. Topics

The topics in this section reveal sensitive intelligence activities; therefore, this section is classified SNSI//NF by topic and compilation.

DOE DCU

DOE
b(1)

b(1)

DOE 600



DOE
b(1)

009 500

CHAPTER 2

APPLIED TECHNOLOGIES FOR INTELLIGENCE INFORMATION (U)

A. General Information

~~(S//NF)~~ This chapter provides classification guidance for the development and potential uses of specialized technology applications in support of intelligence and other sensitive U.S. Government operations/missions, specifically, the Applied Technologies Program (ATP):

- (U) Facilitates the transition of enabling technologies to meet near-term national security requirements within the federal government's intelligence, special operations, and law enforcement communities;
- (U) Maintains a network across the DOE laboratories, with an on-call capability to rapidly identify and provide technical support to federal agencies' varied missions/operations where unique DOE expertise/technologies may be of assistance; and
- (U) Maintains liaison throughout the community for the coordination of operational requirements, identification of applicable DOE technology, and formulation of appropriate investment strategies for developing new capabilities.

B. Broad Guidance

(U) Intelligence-related activities are conducted in compliance with requirements set forth in E.O. 12333 and the ATP Charter, as authorized by the Under Secretary of Energy. Related information could reveal methods, techniques, and/or capabilities used or being developed to support sensitive

intelligence, military, or law enforcement activities.

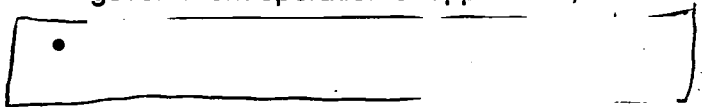
~~(S//NF)~~ It is necessary to protect and classify intelligence methods, sources, and activities to deny adversarial efforts to counter, deceive, or defeat U.S. intelligence activities. The classification of special technologies plays an important role in the overall national security. A cradle-to-grave approach is imperative for the classification of the research and development (R&D) of special technology and its correlation to the IC. Specifically, classification is factored into all phases of equipment life cycle, from the initial concept, through R&D and fielding, up to final retirement, and sometimes beyond.

(U) Much of the classification guidance for special technologies is classified by source documents, in most cases as specified in an operational requirements document or, in some instances, as indicated and/or implied by Memorandum of Agreement (MOA) with other U.S. Government agencies.

(U) Many of the details concerning special technologies are classified based upon:

- ~~(S//NF)~~ Association with the intelligence community, and/or sensitive government operation or application;

DOE
b(1)



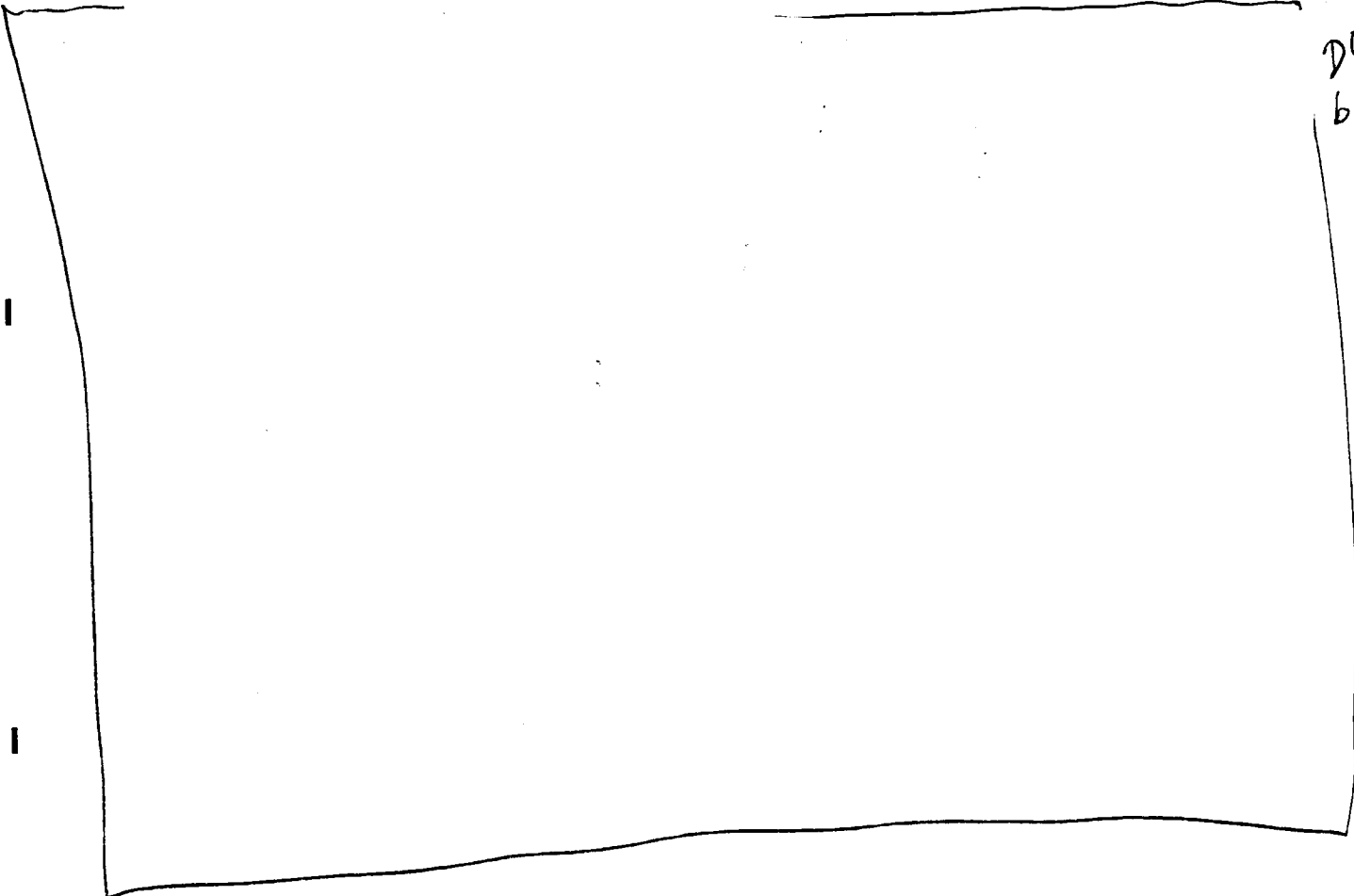
- (U) Significance of breakthrough technology, i.e., provides a unique and/or enhanced capability or, conversely, reveals or implies a significant deficiency/vulnerability that sponsor agencies do not wish to be known by possible adversaries.

C. Topics

The topics in this section reveal sensitive intelligence activities; therefore, this section is classified **SNSI//NF** by topic and compilation.

DOE . BCU

DOE
b(1)



THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3

FOREIGN INTELLIGENCE INFORMATION (U)

A. General Information

(U) Most foreign intelligence and terrorist information is generated and reviewed for classification by agencies outside of the DOE. Their classification determinations are the basis for the derivative classification of most DOE documents containing such information. Generally, information revealing U.S. knowledge of foreign military plans, weapons or operations, or the extent or degree of success achieved by the U.S. in collecting the same, is classified. Intelligence information released to the U.S. Government by a foreign government with the understanding that it would be kept in confidence is classified. All information that would reveal intelligence sources, methods, procedures, or equipment that has been or may be used to acquire foreign and terrorist intelligence is classified

reasons. Since information of intelligence value is closely held by governments, the disclosure that it has been compromised may provide useful information as to the source of the information. It may also implicitly compromise the methods or equipment used in its acquisition. In some cases, it may be information that the United States has agreed not to reveal, and in still others it might affect the conduct of U.S. or a friendly-power foreign policy. The release of some foreign intelligence may lead to an increase in international tensions, a condition of civil disorder that could threaten U.S. lives and property, or the initiation of hostile actions against U.S. forces.

(U) Much of the intelligence information analyzed by DOE is classified based on the source document. The following information produced by or for the IC is classified:

- (U) Military plans, weapons, or operations:
 - (U) Information concerning foreign military intentions, capabilities, or activities
 - (U) Information that could reveal the extent or degree of success achieved by the U.S. in the collection of intelligence information on and assessment of foreign military plans, weapons, capabilities, or operations.
- (U) Intelligence activities, sources, or methods:

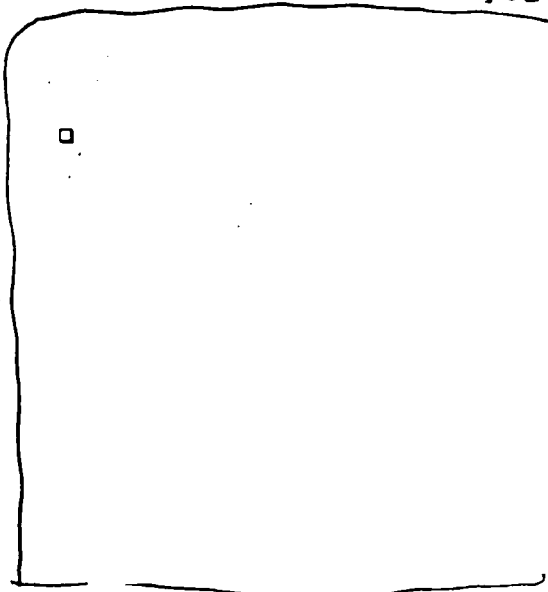
DOE b(2)

B. Broad Guidance

(U) Foreign intelligence and terrorist information may be classified for many

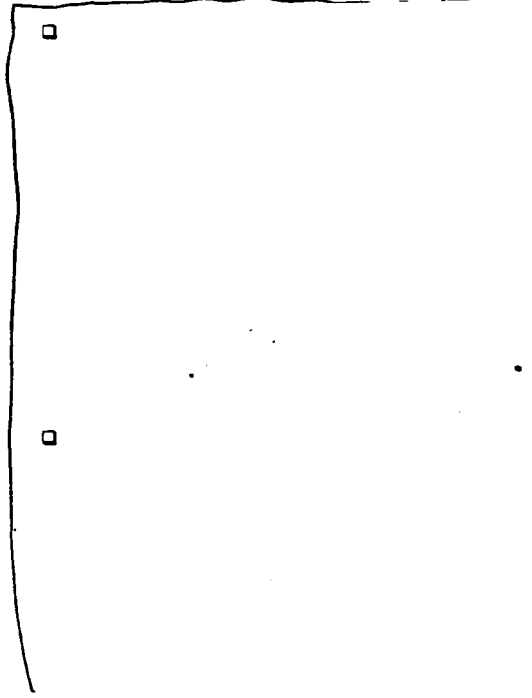
DOE b(2)

DOE
b(2)



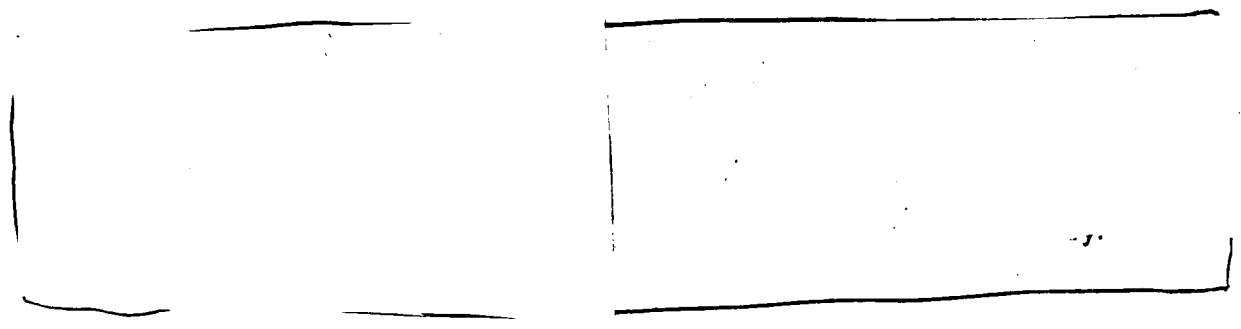
- (U) Foreign relations or foreign activities of the United States:
 - (U) Foreign intelligence information that, if disclosed, could lead to foreign political, economic, or military action against the United States or other nations;
 - (U) Foreign intelligence information that, if disclosed, could create, stimulate, or increase international tensions in such a manner as to impair the conduct of U.S. foreign policies;

DOE b(2)



DOE
b(1)

DOE
b(2)



C. Topics

The topics in this section reveal sensitive intelligence activities; therefore, this section is classified SNSI//NF by topic and compilation.

(1) 9 300

7

DOE
b(1)



- DOE b(1)

DOE
b(1)

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4

IMAGERY INTELLIGENCE (U)

A. General Information

(U) Most information concerning imagery intelligence is generated and reviewed for classification by agencies outside of the DOE. Their classification determinations are the basis for the derivative classification of DOE documents containing such information.

(U) E.O. 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*, defines imagery as "the product acquired by space-based national intelligence reconnaissance systems that provides a likeness or representation of any natural or man-made feature or related objective or activities and satellite positional data acquired at the same time the likeness or representation was acquired."

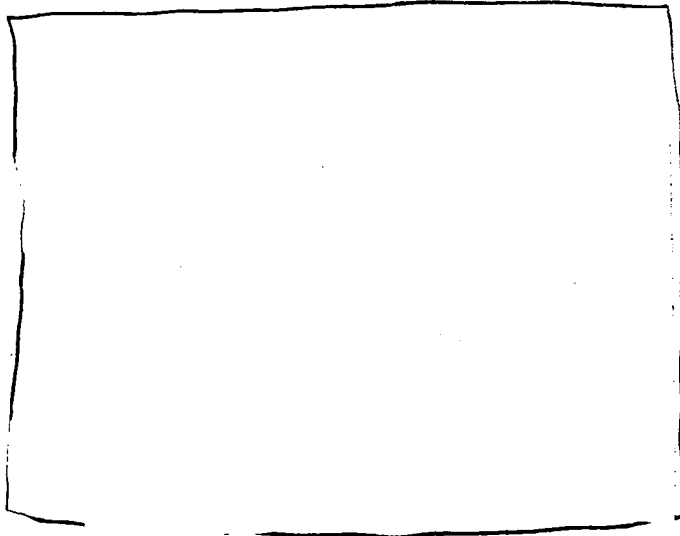
B. Broad Guidance

~~(SUC)~~ Imagery intelligence information is classified to protect intelligence methods, sources, and activities. Such information is classified to deny an adversary that information that would assist in the disruption, decoying, degradation, or defeat of U.S. collection efforts. This includes, but not limited to, the capabilities and limitations of the

equipment, techniques, and resulting analyses.

(U) Much of the imagery intelligence analyzed by DOE is classified based on the source document. The following information produced by or for the intelligence community (IC) is classified:

- (U) Information that could reveal the extent or degree of success achieved by the U.S. in the collection of intelligence information (e.g., targets)
- (U) Intelligence activities, sources, or methods

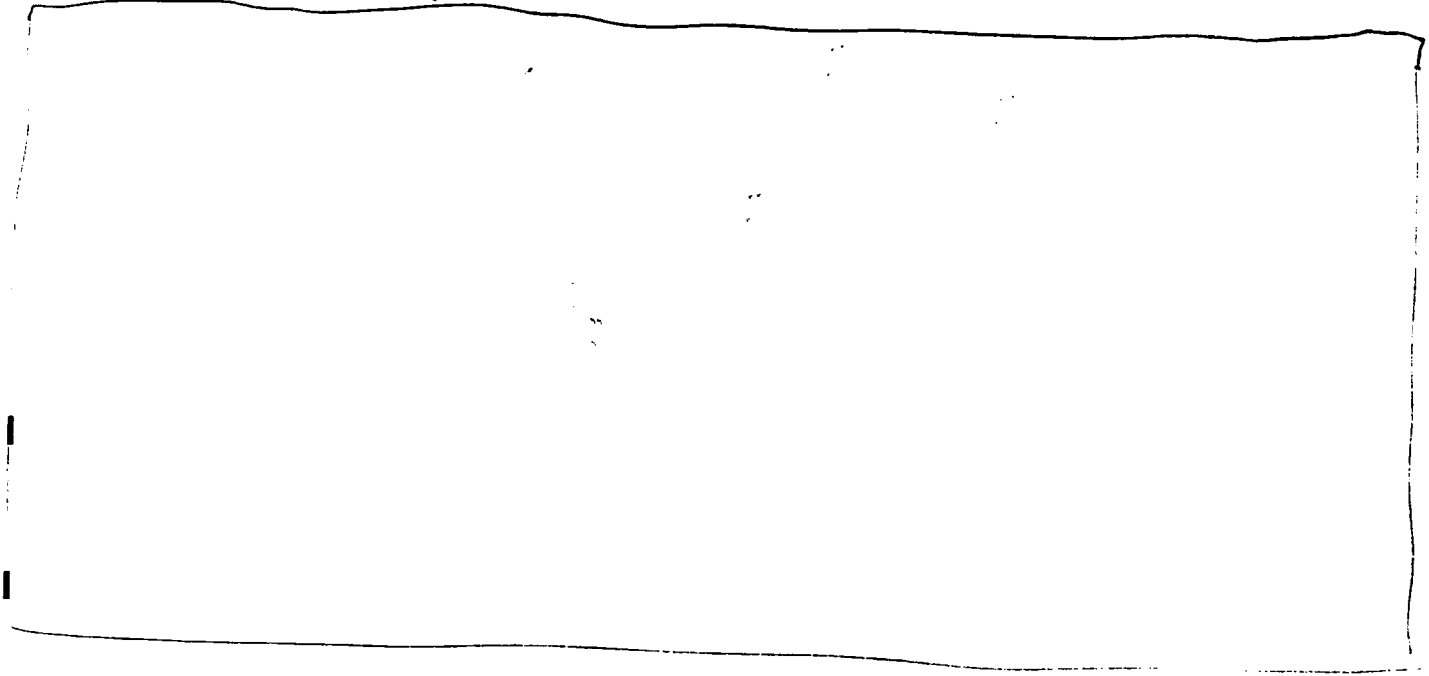


DOE b(2)

C. Topics

The topics in this section reveal sensitive intelligence activities; therefore, this section is classified SNSI//NF by topic and compilation.

b(1)
DOF



APPENDIX A

DEFINITIONS

Accreditation of SCI Facilities (SCIFs) (U) - The formal certification of a specific place referred to as a SCIF that meets prescribed DCID 6/9 physical and technical security standards. (U)

Automated information system security (U) - Compilation of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy. This includes: all hardware/software functions, characteristics, and features; operational procedures; accountability procedures; access controls at all computer facilities; management constraints; physical protection; control of compromising emanations (TEMPEST); personnel and communication security; and other security disciplines. (U)

COMSEC (Communications Security) (U) - Protective measures taken to deny unauthorized persons information derived from telecommunications related to national security and to ensure the authenticity of such communications. Communications security protection results from the application of security measures to electrical systems which generate, handle, process, or use classified information. These measures involve proper application of cryptography, TEMPEST, and physical and transmission security standards. (U)

Countermeasure (U) - Action taken to defeat or degrade performance of an adversarial action against a friendly target. (U)

Counter-countermeasures (U) - Action taken to defeat or degrade performance of a countermeasure. (U)

Counterintelligence (or support thereto) (U) - Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs. (U)

Covered contractors (U) - A seller of supplies or services having access to and protection of classified matter/information, nuclear materials, or other safeguards and security interests under a procurement contract or subcontract. (U)

Derivative Classifier (formerly referred to as an Authorized Derivative Classifier) (U) - An individual authorized to determine that documents/materials are either, (a) unclassified or, (b) classified as Restricted Data, Formerly Restricted Data, or National Security Information, in accordance with existing guidance or source documents. (U)

Energy intelligence (U) - Intelligence relating to the technical, economic, and political capabilities and programs of foreign countries to engage in development, utilization, and commerce of basic and advanced energy technologies. This includes the location and extent of foreign energy resources and their allocation; foreign government energy policies, plans, and programs; new and improved foreign energy technologies; economic and security aspects of foreign energy supply, demand, production distribution, and utilization. (U)

FRD (Formerly Restricted Data) (U) - Classified information jointly determined by the Director of Security Affairs (DOE) and the Department of Defense to be related primarily to the military utilization of atomic weapons and removed by the Director of Security Affairs from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data. (U)

Foreign Intelligence (U) -

1. (U) Information and product materials resulting from the collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power, which is significant to the national security, foreign relations, or economic interests of the United States and which is provided by a government agency that is assigned an intelligence mission (i.e., an intelligence agency);
2. (U) Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons (i.e., positive intelligence), but not including counterintelligence (with the exception of information on international terrorist activities); or
3. (U) Information relating to the ability of the United States to protect itself against actual or potential attack by, or other hostile acts of, a foreign power or its agents, or against the activities of foreign intelligence services.

IC (Intelligence Community) (U) - The aggregate of those organizations and departments of the U.S. Executive Branch that conduct or support various intelligence activities comprising the total national intelligence effort. Pursuant to E.O. 12333, the IC is comprised of the following:

- a. (U) Central Intelligence Agency (CIA);
- b. (U) National Security Agency (NSA);
- c. (U) Defense Intelligence Agency (DIA);
- d. (U) Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
- e. (U) Bureau of Intelligence and Research of the Department of State;
- f. (U) Intelligence elements of the Army, Navy, Air Force, and Marine Corps, Federal Bureau of Investigation (FBI), Department of Treasury, Department of Energy; and
- g. (U) Staff elements of the Director of Central Intelligence

Imagery (U) - The product acquired by space-based national intelligence reconnaissance systems that provides a likeness or representation of any natural or man-made feature or related objective or activities and satellite positional data acquired at the same time the likeness or representation was acquired. (U)

Intelligence information (referred to as "intelligence" in this guide) (U) - Information and related materials resulting from activities conducted within the United States Intelligence Community (U.S. I.C.) pursuant to E.O. 12333. "Intelligence" (regardless of media: spoken, written, electronic, etc.), classified pursuant to E.O. 12958 or any predecessor or successor Executive order, includes the following:

1. (U) Foreign intelligence and counterintelligence defined in the National Security Act of 1947, as amended, and in E.O. 12333;
2. (U) Information describing U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence, foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from U.S. intelligence collection efforts; and
3. (U) Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security)

IS (Information System) (U) - As used in this guide, IS refers to any telecommunications and/or computer-related equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog), including software, firmware, and hardware. In the context of this guide, it applies to those systems processing intelligence information including collateral systems as well as systems classified at the Sensitive Compartmented Information (SCI) level. (U)

MR (manual review) (U) - A marking used on some intelligence material that:

1. (U) The declassification is based upon a specific event;
2. (U) The declassification block shows that the source was marked OADR (Originating Authority Determination Required); and/or
3. (U) The material contains RD, FRD, or North Atlantic Treaty Organization (NATO) information

Multilevel IS (U) - A type of IS that is capable of operating in multiple accreditation levels simultaneously (U)

NFIP (National Foreign Intelligence Program) (U) - Includes the following activities, though its composition is subject to review by the National Security Council and modification by the President: Central Intelligence Agency programs, the Consolidated Cryptologic Program (CCP), the General Defense Intelligence Program (GDIP), and elements or programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance, other programs of agencies within the Intelligence Community designated jointly by the Director of Central Intelligence (DCI), and the head of the department, or by the President, as national foreign intelligence or counterintelligence activities, and activities of the staff elements of the DCI. Intelligence activities required for planning and conduct of tactical operations by the United States military forces are tactical intelligence and related activities (TIARA) and not included in the NFIP. (U)

Need-to-know -

1. (U) The fundamental security principle in safeguarding classified information, which ensures that such information is accessible only to those persons with appropriate clearance, access approval, and clearly identified requirement authorized by the U.S. Government for the information; and/or
2. (U) A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his/her official or contractual duties of employment.
3. (U) Pursuant to DCID 6/1, the need-to-know determination is made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function. Such person shall possess an appropriate security clearance and access approval in accordance with DCID 1/14.

NF (NOFORN) (U) - See NOFORN (U)

NOFORN (No Foreign Dissemination) (U) - Caveat used for intelligence information to denote that the information is not releasable to foreign nationals. (U)

NSI (National Security Information) (U) - Information that has been determined, pursuant to E.O. 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of the national defense or foreign relations. (U)

RD (Restricted Data) (U) - All data concerning: (1) design, manufacture, or utilization of atomic weapons; (2) production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act of 1954. (U)

SAP (Special Access Program) (U) - A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (U)

SCI (Sensitive Compartmented Information) (U) - Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. (U)

SCIF (SCI Facility) (U) - An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed. (U)

SIO (Senior Intelligence Officer) (U) - The highest ranking military or civilian individual charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, command, or element of an Intelligence Community organization. When an SIO has been assigned responsibilities under DCID 6/1. or delegated authorities by the Senior Official of the Intelligence Community (SOIC), the SIO is responsible for implementing the policies and procedures of the DCID. (U)

Special Technology (U) - Research, development, fielding, and operation of specialized technology that have potential applications in support of intelligence and other sensitive U.S. Government operations/missions. (U)

TEMPEST (Transient Electromagnetic Pulse Standard) (U) - The investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (U)

TSCM (Technical Surveillance Countermeasures) (U) - Systematic and effective measures for the detection and/or nullification of technical surveillance penetrations, technical surveillance hazards, and physical security weaknesses. (U)

THIS PAGE INTENTIONALLY LEFT BLANK

(Classification when filled in)

CLASSIFICATION ISSUE/COMMENT SHEET

TO:

(See Introduction for Classified/Unclassified address)

THRU: _____

(Local Classification Officer or HQ Classification Representative)

FROM: _____

(Organization)

NAME: _____

DATE: _____

CLASSIFICATION ISSUE: (Describe the problem including the classification guide short title and the affected topics. Use additional pages/attachments as necessary.)

RECOMMENDED SOLUTION: (To be completed by submitter. Use additional pages/attachments as necessary.)

ANALYSIS:

RECOMMENDATION:

For Use By SO-10.2 Only

ACTION NUMBER:

ACTION OFFICER:

(Classification when filled in)

SECRET//NOFORN

UNCLASSIFIED

CG-IN-1

DELETED VERSION

SECRET//NOFORN

UNCLASSIFIED