

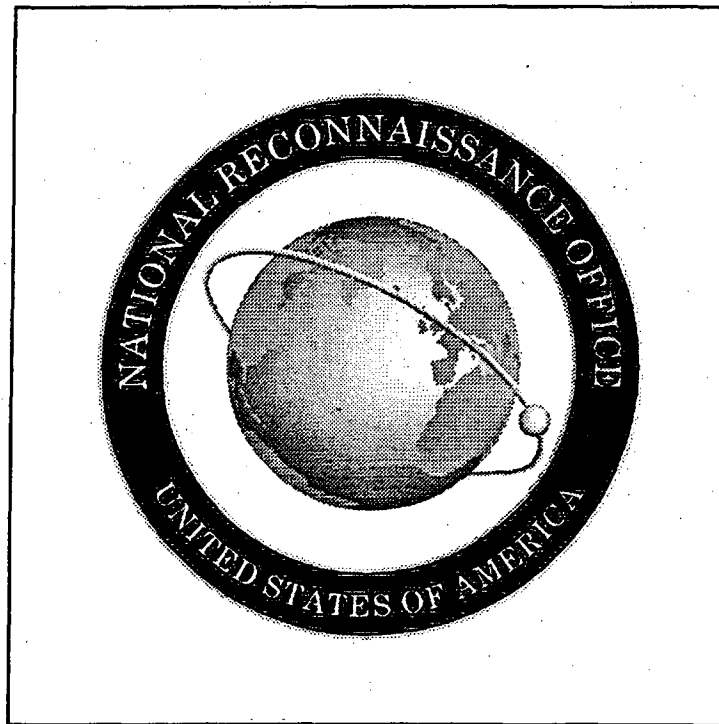
BC00882062  
UNIT TC ~~copy~~  
BYE-137832-95 ✓  
Copy ~~13~~

22 00004251D  
Series B ayl

# NRO CLASSIFICATION GUIDE (U)

VERSION 4.0

Updated: 14 October 1995



Classify By: J.D. Hill, DD/NRO  
Reason: (1.5 c) Intelligence Sources and Methods  
Declassification On: (X1) Intelligence Sources and Methods  
Derived From: Original Classification Authority  
Multiple Sources, see pages 19 and 20

~~SECRET~~

BYE-137832-95

## TABLE OF CONTENTS

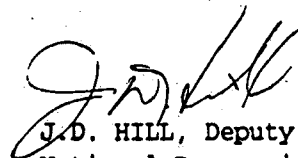
AUTHORITY.....	3
MEMORANDUM FOR THE RECORD.....	4
FOREWORD.....	5
PREFACE.....	6
SECTION I - GENERAL.....	8
PURPOSE AND SCOPE.....	8
BACKGROUND.....	8
RESPONSIBILITY/AUTHORITY.....	10
CLASSIFICATION CRITERIA.....	11
SECURITY AND CLASSIFICATION RECOMMENDATIONS.....	12
SECTION II - CLASSIFICATION AND INFORMATION.....	19
1.0 GENERAL FACTS OF AND ABOUT NRP/NRO.....	21
2.0 SYSTEMS DESCRIPTION.....	27
3.0 COLLECTION, PLANNING AND TARGETING.....	35
4.0 MISSION GROUND STATIONS.....	37
5.0 LAUNCH ACTIVITIES.....	39
6.0 DEVELOPMENT AND ACQUISITION.....	47
7.0 PRODUCT RELATED INFORMATION.....	50
8.0 TERMS AND CODEWORDS.....	54
SECTION III - POST LAUNCH MATRICES.....	57
SECTION IV - DEFINITIONS.....	59

~~SECRET~~

BYE-137832-95

**AUTHORITY**

~~(S/B)~~ This Interim Release of the NRO Classification Guide is approved for use by all NRO, Intelligence Community and contractor personnel authorized to classify National Reconnaissance Program information when making BYEMAN Control Channel classification decisions.

  
J.D. HILL, Deputy Director  
National Reconnaissance Office

~~SECRET~~

BYE-137832-95

MEMORANDUM FOR THE RECORD

14 October 1995

(U) The following changes to Version 3.0, 31 August 1995 NRO Classification Guide incorporate the provisions of Executive Order 12958. Effective 14 October 1995, the NRO changed the way it marks classified material.

(U) It is important to understand with the implementation of EO 12958 that only a limited number of individuals within the NRO will have Original Classification Authority. The remaining individuals will classify information derivatively.

(U) The NRO Classification Guide should be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information.

~~(FOUO)~~ The EO mandates portion marking for all classified information. However, the NRO has been exempted from this requirement for information generated and maintained within the NRO government and contractor base. Information disseminated external to the NRO Government and contractor facilities must be portion marked and contain a document accountability number (DAN). External to the NRO is defined as beyond the direct cognizance of the Director of the NRO. Prior to disseminating the NRO Classification Guide external to the NRO, individuals must first contact the NRO Classification Guide Focal Point by phone [redacted]  
[redacted]

(b)(3)

~~SECRET~~

BYE-137832-95

## FOREWORD

(U) The NRO Classification Guide provides authoritative classification guidance for frequently recurring items of national reconnaissance program information. The use of an item in the Guide to classify a document is considered a derivative classification decision. Should there be discrepancies, between this guide and program classification guides or contractual specifications, then the program specific guides and current contracts take precedence. For classification decisions on information not referenced in the Guide, users must apply guidance contained in program classification guides, or the Intelligence Community sources listed on page 19 of the Guide, or contact the Classification Guide Focal Point via the mechanisms described below.

~~(S/B)~~ Procedures used for marking derivatively classified information within the BYEMAN Control Channel are explained in the ensuing pages and in the BYEMAN SECURITY MANUAL.

~~(FOUO)~~ Discrepancies or conflicts regarding classification issues need to be brought to the attention of the Classification Guide Focal Point via the appropriate program security offices in order that this guide may be properly amended. Once the program security office determines that there is cause for changing the NRO Classification Guide, those recommended changes will be brought before the Classification Guide Review Committee chaired by the Classification Guide Focal Point. Otherwise, questions or comments may be brought to the attention of the Focal Point by phone [REDACTED]

[REDACTED]

(b)(3)

~~SECRET~~

BYE-137832-95

## PREFACE

(U) This NRO Classification and Security Guidance document was prepared by the Director of Security/National Reconnaissance Office (DOS/NRO), and coordinated with NRO Program Offices and other components internal and external to the NRO. It outlines **general** classification guidance relating to National Reconnaissance Program (NRP) information and activities. Guidance on more detailed and technical information is contained in the program classification guides.

~~(S/B)~~ The overall objectives of the guide are the proper classification determinations for NRP and NRO matters and the protection of sensitive satellite intelligence sources and methods within the BYEMAN Security Control System and product control systems. The guide serves as baseline guidance for the definition of BYEMAN: "a unique DCI Security Control System which protects key, specific and fragile details of reconnaissance satellite design and operation." Such delineation of BYEMAN and non-BYEMAN information facilitates accurate determinations for access to the respective control systems. It serves to standardize categories of information in classification guides, such as common components, practices and procedures, and to promote uniform implementation of the BYEMAN Security Control System, consistent with intelligence sources and methods protection.

~~(S/B)~~ An imperative for proper classification and access determination is that user communities have sufficient technical information at non-BYEMAN levels to ensure understanding of capabilities to task satellite systems and analyze products effectively.

~~(S/B)~~ Based on senior government initiatives over the past year, including the National Reconnaissance Program Task Force Final Report (the "Woolsey Report," September 1992) and a DCI memorandum which called for a 50-percent reduction in security compartments, the DOS/NRO established a joint government industry task force that recommended a BYEMAN compartmentation restructure. This restructure, approved by the DCI on November 4, 1993, reduced operational system/integration compartments and studies into a single major compartment--BYEMAN (BYE).

~~(S/B)~~ This document incorporates applicable portions of the Security Implementation Plan for BYEMAN Compartmentation

~~SECRET~~

**BYE-137832-95**

Restructure; the Implementation Plan For Further  
Decomartmentation and Declassification of the National  
Reconnaissance Office; the Classification Guide for National  
Reconnaissance Imagery (Imagery Policy Series); Signals  
Intelligence Security Regulations (SISRs); Security Control Manual  
and Classification Guide for National Measurement and Signature  
Intelligence Reconnaissance Materials (MASINT Policy Series); and  
current BYEMAN and TALENT-KEYHOLE security policy and procedures.  
The guide has been prepared in concert with a major protection and  
classification review by NRO Program Offices, with invaluable  
assistance from staffs of the Central Imagery Office (CIO); SIGINT  
Overhead Reconnaissance Sub-committee (SORS); SIGINT and MASINT  
Committees; and Central Intelligence Agency Collection  
Requirements Evaluation Staff (CIA/CRES).

~~**SECRET**~~

BYE-137832-95

SECTION I: GENERAL**1. PURPOSE AND SCOPE**

~~(S/B)~~ This guide provides general security classification guidance for information, products and activities relating to satellite systems within the National Reconnaissance Program (NRP) and the National Reconnaissance Office (NRO). It is designed for use by NRO and other Intelligence Community personnel engaged in security classification and access determinations in the BYEMAN, TALENT-KEYHOLE and COMINT Security Control Systems. Classification determinations appear in general categories common to all NRO-operated systems. The guide acknowledges BYEMAN compartmentation restructure and serves to complement specific NRP systems classification guides and relevant imagery intelligence (IMINT), signals intelligence (SIGINT), and measurement and signature intelligence (MASINT) security control policy manuals and related classification guides. It also acknowledges intelligence information, products and activities derived from non-BYEMAN sources such as the Defense Support Program (DSP).

~~(S/TK)~~ The user should know that most non-COMINT, denied area products of satellite systems are classified at the SECRET, non-SCI, level. For example,  Electro-Optical, and 99% of Operational Electronic Intelligence products are SECRET COLLATERAL. Care should be taken not to over-classify given the inherently close interrelationship between system information and information needed by the consumers of the products of these systems.

(b)(1)  
(b)(3)**2. BACKGROUND**

~~(S/B)~~ On August 26, 1960, President Eisenhower approved the establishment of the TALENT-KEYHOLE Security Control System to protect satellite reconnaissance information and products. On December 20, 1961, the BYEMAN Security Control System was established to protect information regarding sensitive reconnaissance satellite design, acquisition and operations, and formally protect certain activities of the NRP and its implementing organization, the NRO.

~~(S/B)~~ The BYEMAN and TALENT-KEYHOLE Security Control Systems were instituted to protect critical satellite reconnaissance systems and programs--through the research, development, acquisition,

~~SECRET~~



BYE-137832-95

operations and exploitation phases. Selective system/sensor data, which included general capabilities of the systems, was made available in both control systems. The TALENT-KEYHOLE user community used this information for satellite tasking and intelligence product analysis, while NRO contractors needed this information at the BYEMAN level. (No product information from denied area collection is in the BYEMAN System.) To help assist in making these classification decisions, and in response to the user community, the first BYEMAN/TALENT-KEYHOLE Classification Guide was published in November 1970. The last update was issued in August 1977, April 1994, September 1994, and August 1995.

(U) Classification policy of National Reconnaissance Programs evolved as the NRP and the NRO became increasingly "overt." President Carter admitted the "fact of" satellite photo-reconnaissance in October 1978. The unclassified provisions of National Security Decision Directive-42, revised in June 1987 as a result of the Samuel Morison trial, and National Security Directive-30 on National Space Policy (November 2, 1989 updated March 8, 1995) revealed certain "facts about" satellite photo-reconnaissance. The Acting Secretary of Defense issued a Memorandum on September 18, 1992, that declassified the existence of the NRO and certain facts about its organization and the NRP.

~~(S/B)~~ The end of the Cold War and the "globalization" of space technologies also caused a broadening of U.S. national security strategy, a changed focus of overhead collection and a reassessment of the nature and scope of defense intelligence needs. These changes compelled a re-examination of the BYEMAN Security Control System.

~~(S/B)~~ One effect of these changes was the BYEMAN compartmentation restructure approved by the DCI on November 4, 1993. The BYEMAN Control System is now based on a risk management philosophy and "need-to-know" information exchange. Certain security procedures have changed and internal compartmentation has been virtually eliminated. However, the requirement to protect BYEMAN information as SCI remains. Program names remain valid only as "platform identifiers" for use in document/information management and dissemination. Exceptionally sensitive information, such as survivability and vulnerability data, may be protected separately as program/project "Special Handling" (SH). The release of BYEMAN information to foreign nationals continues in accordance with government-to-government agreements. Foreign disclosure of BYEMAN

~~SECRET~~

BYE-137832-95

information beyond specific second party agreement is permissible upon approval by the DNRO and specific delegation of access approval authority.

### 3. RESPONSIBILITY/AUTHORITY

~~(S/B)~~ The BYEMAN, TALENT-KEYHOLE and COMINT Security Control Systems, as SCI control mechanisms for the protection of intelligence sources and methods, are statutory responsibilities of the DCI.

~~(S/B)~~ While DCI directives provide the baseline guidance for execution of the BYEMAN Security Control System, the Director, National Reconnaissance Office (DNRO) is the overall BYEMAN Program Manager. His responsibilities include: Implementation of DCI directives; establishment and maintenance of security for BYEMAN activities and programs; execution of contracts; determination of what constitutes BYEMAN information and determination of classification level (TOP SECRET or SECRET) of BYEMAN information; publication of security classification guides, including this Classification Guide; and accountability for access control.

~~(S/B)~~ The DNRO is the sole approving authority for determination of "need-to-know" access requirements for BYEMAN information. This authority extends to U.S. Government, contractor, and foreign government personnel having or requiring access to BYEMAN material. Delegations of this authority are specific and in writing.

~~(S/B)~~ The DCI has delegated security policy formulation authority for the BYEMAN Security Control System to the Director of Personnel Security, CIA (DOPS/CIA). The Director of Security, NRO, (DOS/NRO) is responsible; however, for implementation and is the senior security advisor to the DNRO.

~~(S/TK)~~ The TALENT-KEYHOLE Security Control System is jointly managed for the DCI by the Director, Central Imagery Office (CIO); the Chairman, National SIGINT Committee; and the Chairman, MASINT Committee. Changes and modifications to the system require coordination by each Director/Chairman and approval of the DCI/DDCI. The COMINT Security Control System is managed for the DCI by the Director, National Security Agency (NSA). Signals Intelligence Security Regulations (SISRs) constitute the basic implementation of the system for SIGINT and SIGINT-related information. Detailed

~~SECRET~~

BYE-137832-95

security and control procedures for IMINT and MASINT are contained in relevant policy series manuals.

#### 4. CLASSIFICATION CRITERIA

~~(S/B)~~ **Assignment of Information to Control Systems.** Various information about the NRO and its systems will be exclusively BYEMAN, exclusively TALENT-KEYHOLE, or either BYEMAN or TALENT-KEYHOLE. Certain SIGINT product information may be exclusively COMINT or require COMINT Control System protection. As a general rule, "products," product characteristics and information relating to the understanding of general program capabilities for collection tasking purposes should be controlled within the TALENT-KEYHOLE and COMINT Security Control Systems. When deemed necessary, future capabilities information may be controlled within the Talent-Keyhole Control System. This information may be afforded additional protection through the use of Talent-Keyhole subcompartments to limit access to only those persons needing the information for planning purposes.

~~(S/B)~~ **BYEMAN.** BYEMAN is a security system which protects sensitive sources and methods used in the research, development and operation of space-based reconnaissance systems: budgeting and funding details; relationships; integration of launch and sensor platforms; command and control operations; key design and development details; and, survivability and vulnerability of systems.

~~(S/TK)~~ **TALENT-KEYHOLE.** Information controlled exclusively in the TALENT-KEYHOLE Control System includes specific capabilities and related collection targeting and tasking to include data, and certain products of overhead collection. Some SIGINT collection may also require compartmentation within the COMINT Control System.

~~(S/B)~~ **Either BYEMAN or TALENT-KEYHOLE.** Examples of information that can be compartmented in either control system (but not both simultaneously) are system characteristics and program capabilities. In such cases, the determination of the control system to be used will be made based upon the audience. For instance, not all contractors are accessed at the Talent-Keyhole level; therefore, certain information would need to be protected in BYEMAN channels especially when generated in company development and manufacturing facilities. However, the same information could most likely be handled in the Talent-Keyhole System when going to the Intelligence Community. For either

~~SECRET~~

BYE-137832-95

audience, avoid the use of terms that would cause joint compartmentation to be required. For instance, for a TALENT-KEYHOLE audience, do not use BYEMAN "platform identifiers" when mission numbers would serve the same purpose and permit the document to be controlled only within TALENT-KEYHOLE. If information on system design is needed in a TALENT-KEYHOLE document, beyond that which is normally allowed, publish a separate BYEMAN annex to avoid restricting the distribution of the basic document.

~~(S/B)~~ **BYEMAN Special Handling (SH)**. Selective information that is critical to the NRO mission such as vulnerability/survivability data may be placed within distinct BYEMAN security controls that are termed "Special Handling." Such information is nominated by government Program Directors and approved by the DNRO or DDNRO. Program Directors have access approval authority; each program will establish its own procedures.

~~(S/B)~~ **Not Releasable to Foreign Nationals (NOFORN)**. Most classified intelligence information relating to intelligence sources and methods is NOFORN. Release of NRO-related classified information to foreign governments or individuals at the COLLATERAL, COMINT, TALENT-KEYHOLE or BYEMAN level must be in accordance with arrangements between NRO, NSA, and CIA/Collection Requirements and Evaluation Staff (CRES). Potential data release must also satisfy the applicable requirements outlined in DCID 1/7, DCID 5/6, SISRs Volumes I/II, and the Imagery Policy Series. In addition to its SIGINT responsibilities, CRES is the DCI-designated focal point for all imagery-related intelligence community disclosures to foreign officials. Release of unclassified NRO-related satellite technology is subject to export controls as established by the Departments of Commerce and State, in coordination with Department of Defense. Certain organizations/agencies have authorized memoranda of understanding (MOUs) or other agreements that permit the release of non-BYEMAN classified intelligence information to foreign nationals. Release of information is bound by the specific terms of the agreements and may supersede other caveats and restrictions.

## 5. SECURITY AND CLASSIFICATION RECOMMENDATIONS.

~~(S/B)~~ **Classification or Control System Resolution**. The classification tables in this guide specify the classification and/or control system for information relating to NRP systems, products and data. Where the security control system or

~~SECRET~~

BYE-137832-95

classification is not readily apparent from the table or system SCGs information, products and activities will be protected at the applicable level with the most limited distribution, pending a control and classification system review by the NRO for BYEMAN issues and the respective functional program managers within the DIA, CIO, or NSA for TALENT-KEYHOLE, COMINT and collateral classification matters.

# **Executive Order 12958 "Classified National Security Information"**

(U) Under the provisions of Executive Order 12958, the NRO changed the way it classifies material effective 14 October 1995. It is important to understand that only a limited number of individuals within the NRO will have Original Classification Authority. The remaining individuals within the organization will classify information derivatively.

(U) **Classification Identifier.** As part of personal accountability for classification, on the face of each classified document individuals will apply their unique six digit classification ID Number on the "Classified By" line. An example might be:

**Classify By:** Classification ID Number (123456)  
**(CL BY:)**

(U) **Reason for classification.** The classifier shall identify the reason(s) for the classification decision. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to the classification category identified in Section 1.5 of EO 12958:

- (a) "military plans, weapons systems, or operations;"
- (b) "foreign government information;"
- (c) "intelligence activities (including special activities), intelligence sources or methods, or cryptology;"
- (d) "foreign relations or foreign activities of the United States, including confidential sources;"
- (e) "scientific, technological, or economic matters relating to the national security;"
- (f) "United States Government programs for safeguarding nuclear materials or facilities;" or

~~SECRET~~

BYE-137832-95

(g) "vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security."

CL BY: 123456  
 CL REASON: 1.5(c)  
 or  
 1.5(c)(e)

(U) **Declassification Instruction.** The duration of the classification decision shall be placed on the "Declassify On" line. The classifier will apply one of the following instructions.

(U) The classifier will apply a date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which may not exceed 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, mark that date or event as follows:

CL BY: 123456  
 CL REASON: 1.5(c)  
 DECLASSIFY ON: 14 October 2005  
 (DECL ON) or  
 DECL ON: Completion of Operation

(U) At the time of original classification individuals with original classification authority may determine that certain information must remain classified beyond 10 years. The classifier will apply the letter "X" plus a brief recitation of the exemption category(ies), or the letter "X" plus the number that corresponds to that exemption category(ies) in section 1.6(d) of EO 12958:

**X1:** "reveal an intelligence source, method, or activity, or a cryptologic system or activity;"

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

**X3:** "reveal information that would impair the development or use of technology within a United States weapons system;"

**X4:** "reveal United States military plans, or national security emergency preparedness plans;"

**X5:** "reveal foreign government information;"

**X6:** "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

~~SECRET~~

BYE-137832-95

period greater than that provided in paragraph (b);

**X7:** "impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized;" or

**X8:** "violate a statute, treaty, or international agreement."

CL BY: 123456

CL REASON: 1.5(c)

DECL ON: X1

(U) **Derivative Classification.** Derivative classification is the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. On the face of each derivatively classified document the identity of a source document(s) or classification guide to include date shall appear on the "Derived From" line. An example might appear as follows:

Classify By: 123456

CL REASON: 1.5(c)

DECL ON: X1

DERIVED FROM: NRO SCG #4.0 14 October 1995

(DRV FROM) or

DRV From: NRO Director's Note 001, 14 October 1995

(U) When a document is classified derivatively on the basis of more than one source document or classification guide, the "Derived From" line shall appear as follows:

**Derived From: Multiple Sources**

(U) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. When practicable, this list should be included in or with all copies of the derivatively classified document.

(U) The classification tables in this guide specify the classification and/or control system for information relating to NRP systems, products and data. Certain information will surface or be handled through or under collateral cover organizations. Classification authorities for those organization will derivatively classify NRP information under the authority of this

~~SECRET~~

BYE-137832-95

guide. In those cases the derivative classification source will be protected and/or masked appropriately; and the related source list will be protected at the highest appropriate level and controlled with the appropriate control system(s).

(U) A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" shall cite the source document on its "Derived From" line rather than the term "Multiple Sources."

(U) For IMAGERY material under Talent-Keyhole control derived from the CIO Policy Series: DRV FROM: CIOPS 1 June 1994

~~(S/TK)~~ For information derived from the Signals Intelligence Security Regulations: DRV FROM: SISR Aug 1981

(U) For MASINT material under Talent-Keyhole control derived from the MASINT Policy Series: DRV FROM: MPS 002-88 June 1989

(U) The highest level of classified information contained in a document shall be marked in a way as to distinguish it clearly from the informational text. Conspicuously place the overall classification at the top and bottom of the front cover, on the title page, on the first page, and on the outside of the back cover. Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document. In the lower right corner of BYEMAN documents, include the handling caveat marking: "Handle via BYEMAN Channels Only" All documents must be dated on the front page.

~~(S/B)~~ **Portion Marking.** Each classified document being distributed to agencies, offices, and commands external to the NRO community shall, by marking, indicate which portions are classified, with the applicable classification level. External is defined as beyond the direct cognizance of NRO Security (i.e., NSA, DOE, DoD, Congress, etc.) Each portion, ordinarily a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding the portion to which it applies. The following are examples of portion marking abbreviations for both collateral and BYEMAN information:

~~SECRET~~



BYE-137832-95

(TS) TOP SECRET

(S) SECRET

(TS/B) TOP SECRET Handle via BYEMAN Channels Only

(S/B) SECRET Handle via BYEMAN Channels Only

(TS/B/TK) TOP SECRET Handle via BYEMAN/TALENT-KEYHOLE Channels Jointly

(U) Documents that are not portion marked may not be cited as source documents for derivative classification. These documents shall be marked **"Warning-this document shall not be used as a source for derivative classification."** This "warning" marking will be prominently placed on the first page of the document.

~~(S/B)~~ Information that was previously program or platform specific has been marked with a "◆" (Black Diamond) symbol in the NRO Classification Guide. When information is marked with a "◆" then the portion marking should include the applicable platform identifier. "Using the [ ] (i.e., "◆" Black Diamond information) an example may be:

(TS/B- [ ]) TOP SECRET Handle via BYEMAN Channels Only

(b)(1)  
(b)(3)

(U) Classified material being distributed external to the NRO, information marked with a "◆", or other technical/project data when specifically identified by the cognizant program office or directorate must possess a document accountability number (DAN)

(U) All existing programs will be reviewed annually to ensure they meet the guidelines and requirements of Executive Order 12958 and DCID 3/29, "Control Access Program Oversight Committee (CAPOC)."

~~SECRET~~

Overall classification level of document	SECRET	BYE-XXXXXX-95 CY 1 14 October 1995
Document date	Memo For Director, DIA Subject: Fact of Satellite Reconnaissance (U)	
Portion marking	(U) Fact of near-real time satellite photo-reconnaissance. (S/B) Ground collection and planning computer software when associated with program activities. (S) General description of mission.	
Classification block	CL BY: 123456 CL REASON: 1.5(c) DECL ON: X1 DRV FROM: NRO SCG 4.0	
Handling caveat	14 October 1995	Handle via BYEMAN Channels Only

Joe Doe  
Chief Administrator

SECRET

(U) The above example document identifies: the overall classification level of the document; identifying number of the person marking the document; reason for classification; duration of classification; and, classification authority. Since this example is a document that is going external to the NRO, it includes a document accountability number (DAN).

~~SECRET~~

BYE-137832-95

**SECTION II: CLASSIFICATION AND INFORMATION**

~~(S/B)~~ Section II provides a series of classification tables that outline eight basic information categories that relate to satellite reconnaissance and classification determinations for such information. D/NRO is the original classification authority for BYEMAN information. Information listed as TALENT-KEYHOLE, COMINT or COLLATERAL derives from classification/compartmentation guides issued by the CIO, SIGINT Committee and MASINT Committee.

~~(S/B)~~ Prior to the BYEMAN compartmentation restructure, CODEWORD markings in documents were used to facilitate general need-to-know determinations as well as which data could be disseminated or transferred to certain foreign governments. There is still a need for platform or program identifiers for similar reasons. In the BYEMAN column in the following tables, information that was previously program or platform specific has been marked with a "◆" symbol.

~~(S/B/TK)~~ The user should ensure that data in these categories are marked with the pertinent program or platform identifier to set the limits of what can be appropriately released to a foreign government. For reference purposes, the Section II tables include a "SOURCE" column that reflects the original authority for the derivative classification. Unless otherwise specified, the sources are coded as follows:

- 1) Central Imagery Office (CIO) Imagery Policy Series Interim Imagery Classification Chart
- 2) Signals Intelligence Security Regulations (SISR)
- 3) Security Control Manual and Classification Guide for National MASINT Reconnaissance Materials (MASINT Policy Series)
- 4) Program Security Guides
- 5) Security Implementation Plan for BYEMAN Compartmentation Restructure, November 18, 1993
- 6) BYEMAN/TALENT-KEYHOLE Compartmentation Guide, August 23, 1977
- 7) NRO Staff Memoranda/DNRO briefings

~~SECRET~~

**BYE-137832-95**

8) The Decompartmentation and Declassification of the National Reconnaissance Office, 24 April 1995

9) Executive Order 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems, 22 February 1995"

10) Amendment to National Security Directive-30 regarding National Space Policy, 08 March 1995

11) Declassification of the terms "Talent-Keyhole" and the satellite mission designator "KH" and their general relationship to intelligence, 23 February 1995.

~~SECRET~~

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**



**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**



**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**



**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**



**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**

**Page Denied**



**Page Denied**

**Page Denied**

BYE-137832-95

**SECTION IV: DEFINITIONS**

**Air Force Program (AFP) Number**-Unclassified number assigned by the System Program Office (SPO).

(b)(1)

(b)(3)

**BYEMAN Security Control System**-BYEMAN is a unique DCI Security Control System that protects key, specific and fragile details of reconnaissance satellite design and operation. Generally, information requiring exclusive BYEMAN protection includes: (1) budgeting and funding details; (2) relationships (Between Government and contractors); (3) integration of launch and sensor platforms; (4) command and control operations, (5) key design and development details; and (6) survivability and vulnerability of systems.

**Classified:** Information or material that requires protection against unauthorized disclosure in the interest of national security. This material consists of three categories:

- 1) TOP SECRET - applied to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.
- 2) SECRET - applied to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.
- 3) Confidential - applied to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Security classification judgments must be made based on an approved System Classification Guide (SCG) or by an original classification authority, in accordance with the rules for such determinations set forth in Executive Order 12958. Confidential is not used in the BYEMAN Control System.

**COMINT Security Control System:** COMINT is a DCI special access Security Control System expressly authorized for handling or transmitting communications derived from satellite intelligence and other sources. COMINT categories have been established to distinguish among the classes of COMINT which differ in sensitivity and are designated by distinctive codewords.

**Common Name**-Name assigned to the satellite by its owner/operator. The common name appears in the unclassified Spacecom Satellite Catalogue (SATCAT). The common name is not the satellite's BYEMAN name. For example, the common names for

~~SECRET~~

BYE-137832-95

**Derivative classification-** Means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance.

**FOR OFFICIAL USE ONLY:** For Official Use Only (FOUO) is not a security classification. Information identified as FOUO in this guide is exempt from mandatory disclosure.

**Imagery Intelligence (IMINT):** The collection and analysis of photography and electronic imaging across the electromagnetic spectrum, to include visual, radar, infrared, and ultraviolet data.

**International Designator (INT DES)-**A number made up of year and chronological number of the launch for that year to include the suffix that defines each piece associated with the same launch (also known as the ID#). (b)(1)  
(b)(3)

**Inter-Range Operations Number (IRON)-**Number assigned by CSTC/VOI at Onizuka AFB, CA for identifying satellites in the Air Force Satellite Control Network (AFSCN)

**Operations Number-**Number assigned by the launch agency.

**Mission-**The NRO mission of the satellite.

**Mission Number-**Number assigned to identify specific NRO satellites, e.g., [redacted] etc. [redacted]

**Non-Compartmented National Security Information-**In instances where compartmented security controls are not warranted for added protection, classified information may be placed within a non-Sensitive Compartmented Information (SCI) system for safeguarding national security information. This is especially important for military users of product information.

(b)(3)

**Original classification authority-**Means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

**Signals Intelligence (SIGINT):** The interception, analysis and reporting of information comprising either individually or in combination, all COMINT, ELINT, and FISINT. SIGINT includes both raw data and the analysis product of that data. Subsets of SIGINT include:

~~SECRET~~

**BYE-137832-95**

1) **Communications Intelligence (COMINT)**: Technical and intelligence information derived from foreign communications by other than the intended recipients. Special Intelligence (SI) is the unclassified term which is used to identify COMINT in the unclassified environment.

2) **Electronic Intelligence (ELINT)**: Technical and intelligence information derived from foreign electromagnetic non-communications transmissions by other than intended recipients, and foreign non-communications electromagnetic radiation emanations from other than atomic detonation or radioactive sources.

3) **Foreign Instrumentation Signals Intelligence (FISINT)**: Technical and intelligence information derived from the intercept of foreign instrumentation signals (i.e., electromagnetic emissions) associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems. Signals include telemetry, beaconry, electronic interrogators, tracking/fusing/arming/command systems, and video data links:

**Measurement and Signature Intelligence (MASINT)**-Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter or sender and facilitating subsequent identification and/or measurement of the same.

(b)(3)

**TALENT-KEYHOLE** Security Control System-TALENT-KEYHOLE is a DCI special access Security Control System which protects technical data used in collection tasking, imagery processing/exploitation techniques for collected data, and intelligence products derived from overhead reconnaissance programs. Generally, TALENT-KEYHOLE protects information, products and activities relating to the following intelligence disciplines: Imagery intelligence (IMINT), signals intelligence (SIGINT), electronic intelligence (ELINT), communications intelligence (COMINT), foreign instrumentation signals intelligence (FISINT), and measurement and signature intelligence (MASINT)

~~SECRET~~