(U) National Reconnaissance Office (NRO)

(U) Imagery Systems Acquisition and Operations Directorate (IMINT)

(U) IMINT Program Classification Guide (IPCG)

Version 4.0
21 May 2005

//Signed//
Scott F. Large
(U) Director, Imagery Systems Acquisition and Operations Directorate

CL By:
CL Reason: 1.4c
DECL On: 25X1
DRV From: NRO CG 5.1
1 MAY 2000

(b)(3)

~~TOP SECRET//TALENT KEYHOLE//RSEN,NOFORN//25X1~~

RFC IMS-0024

(U) Section I

1.0 (U) Record of Change

Version	Change Date	Table Element(s) Changed	Authority/Description of Change
4.0	May 2005		Re-Baseline Document

Changes to this document are yellow highlighted to indicate where changes from the previous version were made.

(U) Table of Contents

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

IPCG

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

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

1.1 (U) How to Use This Guide

(U) The IMINT Program Classification Guide (IPCG) was not designed to be read from cover to cover. The IPCG was designed with the expectations of it being a softcopy document (Adobe Acrobat document), thus users would use the relatively powerful "Find" & "Find Again" functions to locate the specific information they desired. However, for those who prefer to, or must work with a hardcopy document *(NOT RECOMMENDED – SINCE THE IPCG IS A LIVING DOCUMENT AND IS CONSTANTLY UPDATED)*, the IPCG was designed exactly as most books and reference documents you would commonly use. It has a comprehensive "Table of Contents" and a very detailed "Index" to aid users in locating a specific topic.

(U) It is recommended that you treat this guide as you would any other reference document, utilizing the "Table of Contents" or "Index" to locate the topic of interest. The IPCG is broken down into eight sections, with the core of the document contained between Section III & Section VII. These five sections contain classification tables, which are divided into specific segments. This will assist you in navigating and searching through the many categories of information, and in locating specific topics contained within the guide.

1.2 (U) Foreword

(U) The security objectives of the IMINT Directorate are to streamline and modernize the security policies and practices and to incorporate risk management strategies. Each classification decision must recognize the necessity of classifying only the information that requires protection. Executive Order 12958, as amended, dictates that the classification, or declassification, of our activities must be guided by clear goals and principles based on the identified threat. The classification level of the elements contained in the classification tables in this guide were chosen only after taking a number of factors into account – the changing national security environment and the issuance of Executive Order 12958, as amended, being the primary drivers.

(U) The use of an item in this guide to classify a document is considered a derivative classification decision. Should there be discrepancies between this guide and program contractual specifications, the current contracts take precedence. For classification decisions on information not referenced in this guide, users should coordinate with an IMINT Program Security Officer (PSO) and, if appropriate, submit a Request For Change (RFC) to update this document.

1.3 (U) Introduction

1.3.1 (U) Preface

(U) This IMINT Program Classification Guide establishes the general classification guidance relating to the IMINT Program including detailed guidance for IMINT System(s)/subsystem(s), Computer Software Configuration Items (CSCIs), Hardware Configuration Items (HWCIs), and relationships between those

components, as well as organizational relationships during the total life cycle of IMINT Program phases and activities.

(U) A significant change in this guide was caused by the retirement of the BYEMAN Control System. All information formerly marked as BYEMAN has been recompartmented to the TALENT KEYHOLE control system. The term BYEMAN is obsolete at the close of business 20 May 2005, and has been declassified. The term may still be seen on older intelligence information, but must be changed to TALENT KEYHOLE with appropriate dissemination controlsbefore the information can be redistributed.

1.3.2 (U) Purpose

(U) The purpose of this document is to ensure the proper classification determinations for IMINT activities in order to protect sensitive satellite intelligence sources and methods within the TALENT KEYHOLE security control system. It serves to standardize categories of information and to promote uniform implementation of the TALENT KEYHOLE Security Control System consistent with intelligence sources and methods protection.

1.3.3 (U) Scope

~~(S//REL)~~ This document ensures the proper classification determinations for all IMINT activities, including but not limited to, relationships and data relating to IMINT Research & Development (R&D), engineering design, specifications, algorithms, interface controls, test plans, operations manuals, and reference documents; equipment and computers involved in the operation of the IMINT System to include launch vehicle(s), spacecraft, sensor(s), and mission ground station equipment; computer programs used to operate IMINT hardware to include launch, spacecraft maintenance, command and control, targeting, sensor operation, image data conversion, processing, and exploitation operations, as well as the overall and detailed funding profile for both the development and operation of the IMINT System.

1.4 (U) Overview – Background

1.4.1 (U) Rethinking Classification

(U) There have been serious efforts in recent years to improve classification management practices. Part of that effort is a growing recognition of the need to replace a risk avoidance approach, which seeks to anticipate all risks in the protection of assets, with a risk management approach which attempts to concentrate limited resources on those assets, the loss of which would have the most profound effect on the mission. The number of special access programs and compartments designed to provide additional protection beyond the CONFIDENTIAL, SECRET and TOP SECRET levels have been reduced. Progress has been made in moving large quantities of information out of the remaining compartments/programs and into the three classification levels, where a broader range of "customers" more easily uses it.

(U) A meaningful assessment of the need for protection over the long term requires revisiting the initial decision to classify throughout the period in which the information is of value (throughout the life cycle of that information). This life cycle approach recognizes that both classified and unclassified information exists throughout a life span in which decisions must be made with respect to creation, management and use, and final status (destruction/preservation/release). The management of classified information should include the important initial consideration of whether the information should be classified at all. The "life-cycle risk assessment" of classified information should encompass an analysis at each stage of the information's "life" of whether the information requires protection, given the risks, threats, and vulnerabilities, as well as the cost of protecting or declassifying the information. It is understood that this approach may lead to different results at different stages of the life cycle.

1.4.2 (U) Executive Order 12958, as amended

(U) Executive Order 12958, as amended, like prior executive orders, lays out the rules governing the identification and protection of information, the unauthorized disclosure of which could cause "damage to the national security." What distinguishes this order from those of the past is its emphasis on declassification. The (03/25/03) Amendment [known as EO 13292] continues the emphasis on declassification, but has given the community an extension to the automatic declassification guidance provided in the original executive order. The new declassification deadline is 31 December 2006 and affects all records that are currently 25 years old or older and are determined to have historical value. Previous executive orders focused on classification, how to make original classification decisions and how to continue classification into out years.

(U) Even though Executive Order 12958, as amended, emphasizes declassification, it defines categories of information that should be considered for classification. Again, what distinguishes this executive order from those of the past is that for the first time, EO 12958, as amended, includes thresholds for classification. In previous executive orders, any information concerning the "foreign relations and foreign activities of the United States" could be considered for classification. Under EO 12958, as amended, such information is still eligible for classification, but only if it would impair those "relations" or "activities," theoretically requiring classifiers to make a reasoned evaluation of whether the information truly warrants classification. The EO amendment uses slightly different words, but the intent is the same.

1.4.3 (U) The Levels of Classification

(U) When it has been decided to classify a piece of information, the level of classification of that information must be determined. Executive Order 12958, as amended, preserves the three classification levels of Confidential, Secret and Top Secret that have long served as the foundation for protecting classified information. While the specifics of these three classification levels have varied over time, their basis has remained based on the concept of "damage" since the

1950s. EO 12958, as amended, requires classifiers to be able to "identify and describe" the damage to the national security if the information were disclosed.

(U) The amount of "damage" caused by the unauthorized disclosure of information determines the classification level assigned to that information. The damage descriptions and associated classifications are detailed in paragraph 1.2.2.

(U) The dissemination of classified information is intended to be limited to those who both (1) hold the appropriate clearance(s), and (2) need the information to properly perform their duties. The extent to which the "need-to-know" principle is adhered to is becoming more and more difficult to enforce with the advent of the "information highway." Intelink, which allows cleared personnel access to a wide range of classified information, is a notable example of how need-to-know is becoming harder to enforce in the "Information Age."

1.4.4 (U) Special Access Programs

(U) Access to information considered to be particularly sensitive is controlled through a range of special access programs, which involve access controls and security measures typically in excess of those normally required for access to classified information contained in the three-tiered collateral classification system.

(U) President Eisenhower approved the establishment of the TALENT KEYHOLE (TK) Security Control System, to protect Satellite reconnaissance information and products, on August 26, 1960. The BYEMAN (BYE) Control System was established, to control information regarding sensitive reconnaissance satellite design, acquisition and operations, on December 20, 1961. The BYEMAN Control System was officially retired 20 May 05.

(U) The BYEMAN (BYE) and TALENT KEYHOLE (TK) Security Control Systems were instituted to protect critical satellite reconnaissance systems and programs – through the research, development, acquisition, 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 (TK) user community used this information for satellite tasking and intelligence product analysis. To assist in making classification decisions, and in response to the user community, the first BYEMAN/TALENT KEYHOLE Classification Guide was published in November 1970. The guide was updated in August 1977, April 1994, September 1994, August 1995, and October 1995.

(U) The classification policy for National Reconnaissance Programs evolved as the NRP and NRO became increasingly "overt."

- President Carter admitted the "fact of" satellite photoreconnaissance in October 1978.

- The unclassified provisions of National Security Decision Directive-42, and National Security Directive-30 on National Space Policy revealed certain "facts about" satellite 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.

(U) 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 served as a basis to re-examine the BYEMAN Security Control System.

(U) The BYEMAN Control System was also re-examined after the terrorist attacks of Sep 11th. To comply with the Horizontal Integration movement across the Intelligence Community the NRO decided to retire the BYEMAN Control System so its intelligence information could be shared with the rest of the community.

1.5 (U) Security and Classification

1.5.1 (U) Classification or Control System Resolution

(U) The classification tables in this guide specify the classification and/or control system pertaining to information relating to IMINT systems, products, relationships and data. Where the security control system or classification is not readily apparent from the table(s) or other information in this guide – information, products, relationships and activities will be protected at the applicable level with the most limited distribution, pending a control and classification system review.

1.5.2 (U) Classification Levels

(U) Executive Order 12958, as amended, states that information may only be classified at one of three levels: Top Secret – applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe; Secret – applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe; and Confidential – applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

1.5.3 (U) Classification Authority

(U) With the implementation of Executive Order 12958, as amended, only a limited number of NRO officials have Original Classification Authority. All remaining NRO personnel have the authority to classify information derivatively. In establishing the information categories and classification levels of an item of information, the EO further directs that the Original Classification Authority must

be able to identify or describe why unauthorized disclosure would result in either damage, serious damage, or exceptionally grave damage to the national security.

1.5.4 (U) Classification Sources

(U) For completeness, this IMINT Classification Guide contains information that deals with programs outside the management and cognizance of the Director of Imagery Systems Acquisition and Operations. These items were derivatively classified after consulting a number of documents to identify the Original Classification Authority for the specific items of information. The documents are listed in Section 2.

1.5.5 (U) Reason for Classification

(U) Under the provisions of Executive Order 12958, as amended, information may not be considered classified unless it falls under one or more of the categories listed below. Additionally, the reason(s) for the classification decision must be documented. To meet this requirement, EO 12958, as amended, specifies that, at a minimum, reference to the pertinent classification category or categories described in Section 1.4 of the Executive Order plus the letter or letters that correspond to the category or categories should be listed. The classification categories preceded by their corresponding letter designators are:

(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, which includes defense against transnational terrorism."

(f) "United States programs for safeguarding nuclear materials or facilities."

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

(h) "Weapons of mass destruction."

1.5.6 (U) Declassification Instructions

(U) Executive Order 12958, as amended, maintains the automatic declassification requirement, but has given the community an extension to the deadline imposed by the original executive order. The new deadline is 31 December 2006. This affects all records that are currently 25 years old or older and are determined to have a historical value. Individuals with Original Classification Authority may determine that certain information must remain classified beyond the date specified in the Executive Order. In those cases, the information must be annotated with the letter "X" plus a numerical designation that corresponds to a specific exemption category or set of exemption categories described in Section 3.3 of EO 12958, as amended. The NRO uses the number 25 in front of the X exemptions to depict that the information is further exempted from being automatically declassified after 25 years. (See: NRO Director of Security Note 03-009, 18 Dec 2003, for implementing instructions). The X markings and corresponding declassification exemptions are:

X1 "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."

X2 "Reveal information that would assist in the development or use of weapons of mass destruction."

X3 "Reveal information that would impair U.S. cryptologic systems or activities."

X4 "Reveal information that would impair the application of state of the art technology within a U.S. weapon system."

X5 "Reveal actual U.S. military war plans that remain in effect."

X6 "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."

X7 "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."

X8 "Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or project relating to the national security"

X9 "Violate a statute, treaty, or international agreement."

On 15 June 2000, the IPSCOM ([DCI's] Imagery Policy and Security Committee) approved a standard marking convention for all NTM imagery and annotated NTM imagery. The new policy indicates that the reason for classification is "EO 12951," and that only the DCI is authorized to declassify the data. Those Information Elements in the guide referring to primary imagery/imagery products reflect the above nomenclature in the appropriate columns.

1.5.7 (U) Portion Marking

(U) Executive Order 12958, as amended, mandates that all classified information, regardless of its physical form, indicate which portions are classified. The NRO has been granted a limited waiver from the requirement to portion mark information. The NRO is not required to portion mark information generated and maintained within the NRO by its government staff and/or contractors. Information produced by the NRO that is disseminated externally must be portion marked. In this case, the term external is defined as any organization or entity outside the management cognizance of the Director of the NRO. Prior to disseminating this classification guide to an organization external to the NRO, permission from the Director of IMINT Security must be obtained.

1.5.8 (U) Original Classification Authority (OCA)

(U) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

(U) The Director Central Intelligence (DCI), has delegated the following officials from the National Reconnaissance Office (NRO) with original classification authority:

(a) Director, National Reconnaissance Office (D/NRO)

(b) Deputy Director, National Reconnaissance Office (DD/NRO)

(c) Chief of Staff (CoS)

(d) Deputy Director for Military Support (DDMS)

(e) Deputy Director for National Support (DDNS)

(f) Deputy Director Business Plans and Operations (BPO)

(g) Deputy Director for System Engineering (DDSE)

(h) Director, IMINT Systems Acquisition and Operations Directorate (IMINT)

(i) Director, SIGINT Systems Acquisition and Operations Directorate (SIGINT)

(j) Director, Communications Systems Acquisition and Operations Directorate (COMM)

(k) Director, Advanced Systems and Technology Directorate (AS&T)

(l) Director, Management Services and Operations Office (MS&O)

(m) Director, Operational Support Office (OSO)

(n) Inspector General (IG)

(o) Director, Office of Contracts (OC)

(p) Director, Office of Security (DOS)

(q) Director, Office of Space Launch (OSL)

1.5.9 (U) Releasability / Disclosure Instructions

(b)(3)

[redacted]

~~(S//NF)~~ Entries that are marked NOFORN (Not Releasable to Foreign Nationals) may not be released or disclosed under any circumstances without prior approval

from the NRO Designated Intelligence Disclosure Official (DIDO) in accordance with DCIDs 6/6, 6/7.

~~(S//NF)~~ Information is to be considered NOFORN if it falls into the following categories:

(a) Information that reveals information about the recipient country derived from U.S. Intelligence collection

(b) Information that reveals information obtained from a liaison service without prior approval of that country

(c) The information contradicted U.S. laws, agreements, or treaties

(d) The information constitutes intelligence on a U.S. person

(e) The information jeopardizes a liaison relationship or diplomatic, intelligence, national security, or law enforcement activities

(f) The information jeopardizes HUMINT sources, methods, plans and targets

(g) The information reveals details of SIGINT, IMINT or MASINT activities expected to jeopardize collection opportunities

(h) The information reveals U.S. Counterintelligence activities

(i) The information could be used against the U.S. or jeopardize U.S. sources and methods

(j) Intelligence that would jeopardize the safety and welfare of individuals connected to an intelligence activity

(k) Information that could be reasonably expected to be acquired by a hostile entity

(l) Information that reveals NRO budget data in totality and/or substantial subsets

(m) Information protected in the RESERVE compartment that foreign nationals do not have the need-to-know

(n) Information that pertains to a classified association that parties do not wish to reveal

(o) Information that reveals vulnerabilities of an entire NRO system or architecture

(p) Information that contains operational or mission specific details, which would reveal sensitive U.S. activities

(q) Information that pertains to the application of leading edge technologies that are beyond the scope of existing cooperation guidelines

1.5.10 (U) Compilation / Aggregation of Information

(U) *Executive Order 12958, as amended, Classified National Security Information*; 1.7 (e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

- **(U) Documents**
  In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document. In this instance, the portions of a document classified in this manner need not be marked.

- **(U) Portion of a Document**
  If a classified document contains certain portions that are unclassified when standing along, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on the page, and a statement shall be added to the page, or to the document, to explain the classification of the combination or association to the holder. This method of marking may also be used if classified portions on a page, or within a document, will reveal a higher classification when they are combined or associated than when they are standing alone.

Note: (U) Users of this guide need to be sensitive to issues of compilation / aggregation. It is the individual's responsibility to make compilation classification determinations. When necessary, IMINT Security will assist with any compilation classification decisions.

1.5.11 (U) What Are We Protecting ?

(U) The information contained within this section describes in basic terms what we are trying to protect by classifying a specific item.

- ~~(S//REL)~~ **National Reconnaissance Office (NRO)**

  Now that the NRO is an openly acknowledged organization, many facts, including its structure and purpose have been placed in the public domain as unclassified. We continue to protect detailed organizational specifics, some personnel affiliations and some relationships (b)(1) (b)(3)

- ~~(S//REL)~~ **Satellite System Designators & Codewords**

  IMINT mission numbers and codewords have been downgraded to SECRET. (b)(1) (b)(3)

  Earlier KH designators are unclassified, while those of later (some retired) systems remain classified (GAMBIT, HEXAGON); rule of thumb is if the program is classified, so is the designator.

- (U) **Miscellaneous Facts**

  Many "general facts" about what IMINT does are unclassified. Specifics of how we do it, and how successfully, are invariably classified. It is also easy to assume something is unclassified just because it's a familiar subject or the information has been "published" that may in fact not be the case; even though it may be an "open secret," it may be classified. The other caution is that of association. Two (or more) totally unclassified statements may reveal classified information when associated.

- (U) **Contracting**

  In the past, all contract actions were protected as BYEMAN *(officially retired)*. In today's more "open" environment, (in many instances) the fact of a contract and the identity of the contractor are unclassified. The details of the contract (scope, statement of work and dollar value) are still usually classified, but not necessarily under the TALENT KEYHOLE umbrella. Since the contracting process varies, and changes from time to time, one should consult with the appropriate Program Security Officer or Contracting Officer for specifics.

- (U) **Contractor Roles/Identities**
  Even though more and more contractors have unclassified relationships with IMINT, at various levels, some relationships remain classified. Identities and locations of those contractors are often protected to hide classified/sensitive missions, operating locations or even an advanced or specialized technological expertise. Since this varies from contractor to contractor, one should consult with the Program Security Officer or Contracting Officer for guidance.

- (U) **Acquisition Documentation**
  Detailed IMINT acquisition documentation and associated activities are almost always classified – the level of classification depending on factors such as level of detail, technology involved, IMINT/contractor association, etc. System/segment development and/or design specifications are usually TALENT KEYHOLE because of the detailed technical content. Many procedural documents are SECRET or UNCLASSIFIED, however depending on the capabilities they reveal, they may be protected in the TK compartment. It should be noted that FIA employs a new acquisition process and care must be used not to confuse the "traditional" acquisition documentation with that used by FIA.

- (U) **Funding**
  Specific Program cost and budget figures, including system/subsystem costs are almost always classified, although the level of classification usually is dependent on the particular program/system. Funding levels can reveal particular interest or increased activity in a unique area, and/or may indicate a potential new technology, source and method, etc. Since this varies from project to project, one should consult with the Program Security Officer or Contracting Officer for guidance.

- (U) **Plans, Schedules and Status**
  Detailed engineering specifications and documentation are generally protected in TALENT KEYHOLE channels. Detailed transition, integration, etc. plans are usually in the TK compartment. Many "high-level" schedules are classified SECRET. Generally if the level of detail reveals (fairly reliable) dates of new capabilities, schedule slips that may reveal "gaps" in capabilities, health of systems, or information that reveals (potential) vulnerabilities, the information is protected in SCI channels.

- ~~(S//REL)~~ **Satellite Systems Information**
  KH-1 through KH-6 systems have been declassified; KH-7 imagery and KH-9 mapping camera imagery have also been declassified; but all programmatic data [e.g., capabilities] pertaining to these systems remain classified at the TALENT KEYHOLE level, as does everything about the KH-8 system except the program designator GAMBIT and mission numbers which are SECRET. Capabilities of current systems, such as

exact response times, etc. are usually protected at TK; future systems/capabilities are TK and technical/engineering details of current and future systems are usually TALENT KEYHOLE. These "rules of thumb" often don't hold true due to the classification/declassification processes that are sometimes lengthy – some items in the guide are awaiting declassification

- ~~(S//TK//REL)~~ **Capabilities and Limitations**
  System capabilities and limitations are almost always classified (b)(1) (b)(3)

- ~~(S//TK//REL)~~ **Payloads and Sensors** (b)(1) (b)(3)

- ~~(TS//TK//REL)~~ **Operational Data**
  As a general rule, operational data is classified. (b)(1) (b)(3)

- (U) **Reliability, Availability and Maintainability**
  System reliability and availability information is generally protected at the TK level, the reasoning being that some in the user community need that type of data for planning purposes. Maintenance related data (MTBF [mean time between failure], etc.- that could possibly reveal vulnerabilities in the form of downtimes, and/or related outages is generally protected as TALENT KEYHOLE. Any specific anomalies are almost always TK (fact of, return to service, info, etc.) in order to communicate to the user community need these details.

- (U) **Launch Data**
  Future IMINT launch dates are classified; dates to the nearest year are usually SECRET, while dates to the nearest month and years are typically S//TK. (b)(1) (b)(3)

- ~~(TS//TK//REL)~~ **Collection Information**
  The great majority of classified information in this category is classified (b)(1) (b)(3)

- (U) **Mission Ground Stations**
  The fact that IMINT operates satellite mission ground stations is unclassified. Information that reveals general locations of those facilities is SECRET. If the specific location of the ground station is revealed, that data is treated as S//TK. (b)(1) (b)(3)

- ~~(TS//TK//REL)~~ **Imagery/Product**
  "Standard" IMINT products are classified SECRET. Those same products when associated with technical support data may be classified at a higher level. (b)(1) (b)(3) are generally S//TK or TS//TK because they reveal a technical capability deserving protection.

- ~~(S//TK//REL)~~ **Product Dissemination**
  (b)(1) (b)(3)

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

- **(U) Exploitation**
  The "standard" IMINT product is SECRET (due to the need to make the product available to the "warfighter"). Generally speaking, the exploitation of the product is done at the SECRET level.

(b)(3)

- **(U) Communication (IMINT Related)**
  The communications infrastructure supporting IMINT

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

  Relay Satellites are necessary for near real-time IMINT operations – the fact that we need and use them is unclassified. The identification of a specific relay used by an IMINT system is protected in the TK compartment.

- **(U) Up Link**
  IMINT command frequencies and characteristics are protected in the TALENT KEYHOLE compartment

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

- **(U) Down Link**
  IMINT telemetry frequencies/characteristics are protected in the TALENT KEYHOLE compartment

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

- **~~(S//TK//REL)~~ Cross Link**
  Cross-links are communications paths between IMINT mission satellites and relay satellites. The fact that we have and need them is unclassified.

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

[redacted] (b)(1) (b)(3)

- (U) **Terrestrial Communications** (b)(1) (b)(3)

[redacted]

- (U) **Cryptographic Equipment (Use on the Program)**
  Classification varies from UNCLASSIFIED (the fact that the NRO uses crypto equipment) to TALENT KEYHOLE (information/details related to techniques, design or implementation of such equipment). Generally

[redacted] (b)(1) (b)(3)

- (U) **FIA Activities**
  FIA is a future IMINT system and as such is generally protected in TK channels. However, since the user community, developed the FIA requirements as active participants during pre-acquisition activities, some FIA details normally protected at TK may be treated as SECRET or even unclassified.

- (U) **EIS Activities**
  The IMINT Program Office, as a rule, protects future activities and capabilities in the TALENT KEYHOLE compartment. The majority of the Information Elements in this section are classified SECRET or TOP SECRET TALENT KEYHOLE because EIS is a future system/capability. Much of the information will not be protected in the TK compartment [redacted] and will be classified generally at the SECRET level, in order to make operational data available to a wider audience. (b)(3)

- [redacted] (b)(1) (b)(3)

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

1.6 (U) Classification Criteria

(U) In some instances IMINT information may be Unclassified or UNCLASSIFIED/FOR OFFICIAL USE ONLY. Classified information about IMINT and its systems may be exclusively TALENT KEYHOLE (TK), or SECRET COLLATERAL. As a general rule, products, product characteristics and information revealing, or contributing to an understanding of, general program capabilities for collection tasking purposes should be classified SECRET. Future capabilities information is most often controlled within the TALENT KEYHOLE (TK) Control System.

1.6.1 (U) BYEMAN (BYE)

(U) BYEMAN was an SCI compartment used to protect information revealing sensitive sources and methods used in the research, development and operation of space-based reconnaissance systems; program/project budget and funding details; command and control capabilities and operations; key design, development and technological details; and survivability and vulnerability of systems. BYEMAN officially retired *20 May 2005,* all data that was marked BYEMAN has been recompartmented into the TALENT KEYHOLE control system.

1.6.2 (U) TALENT KEYHOLE (TK)

(U) Information controlled in the TALENT KEYHOLE Control System includes budget and funding details, specific capabilities and related collection targeting and tasking, data, and certain products of overhead collection.

1.6.3 (U) A Note About FOUO

(U) FOUO – For Official Use Only – is an administrative marking that is used to limit dissemination of certain categories of unclassified information. It is not a classification category, and does not afford any protection of classified information. Its use should never be used, as a substitute for classification and the marking can never be attached to information that is not otherwise UNCLASSIFIED.

- (U) The NRO guidance for the use of FOUO is contained in (NRO) Policy Directive 50-12.

1.7 (U) Changes to this Guide

(U) The IMINT Program Classification Guide is under IMINT Configuration Control (IMCCB). Changes to the document may only be made via the RFC process, and submitted through the normal CCB process.

(U) Section II

2.0 (U) Reference Documents

(U) The following documents are applicable to the IMINT security program as stated herein.

2.1 (U) Executive Orders[1]

2.1.1 (U) Executive Order 12356

(U) (April 1982 – Effective August 1982) National Security Information.
Prescribes a uniform system for classifying, declassifying and safeguarding national security information.
(Revokes EO 12065 – June 1978)

2.1.2 (U) Executive Order 12951

(U) (February 1995) Release of Imagery Acquired by Space-based National Intelligence Reconnaissance Systems.
Declassifies all imagery from CORONA, ARGON, and LANYARD.
Is used as the authority for imagery marking and declassification

2.1.3 (U) Executive Order 12958, as amended

(U) (March 25, 2003) Classified National Security Information.
Prescribes a uniform system for classifying, safeguarding, and declassifying national security information. EO 12958, as amended, provides the guidance used to produce this document.

2.2 (U) Director of Central Intelligence Directives (DCIDs)[1]

2.2.1 (U) DCID 6/6

(U) (April 1995) Security Controls on the Dissemination of Intelligence Information.
Provides a policy statement that reflects a risk management approach to the dissemination of intelligence. Eliminates NOCONTRACT and WNINTEL.

2.3 (U) DoD Documents

1. (U) DoD Guide to Marking Classified Documents, DoD 5200.1-PH

2.4 (U) NRO Related Documents

1. (U) NRO Classification Guide, Version 6.0

[1] *Note: Although, there are numerous Executive Orders and DCIDs, only the ones applicable to this document have been sighted above.*

Approved for Release: 2018/12/21 C05102145

2.5 (U) Classification Sources:

1. (U) National Geospatial-Intelligence Agency Imagery Policy Series
2. (U) Signals Intelligence Security Regulations (SISR)

[redacted] (b)(1) (b)(3)

4. (U) Security Implementation Plan for BYEMAN Compartmentation Restructure, November 18, 1993
5. (U) Implementation Plan for Further Decompartmentation and Declassification of the National Reconnaissance Office, April 24, 1995
6. (U) Executive Order 12951, Release of Imagery Acquired by Space-Based National Reconnaissance Systems, February 22, 1995
7. (U) Declassification of the terms "TALENT KEYHOLE" and the satellite mission designator "KH" and their general relationship to intelligence, February 23, 1995
8. (U) Presidential Decision Directive/NSC-49 & NSTC-8: National Space Policy September 14, 1996

2.6 (U) Program Document(s)

1. [redacted] (b)(1) (b)(3)

[redacted] (b)(1) (b)(3)

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

Approved for Release: 2018/12/21 C05102145

(U) Section VIII Appendixes

8.0 (U) Acronyms

~~(S//TK//REL)~~ Classifying acronyms can sometimes be a tough call; therefore, we have removed the portion markings from the acronym list. Acronyms are classified when the "context" in which they are used reveal a classified fact, association, term, source and/or method. (b)(1) (b)(3)

If you have questions on whether or not to classifying an acronym, consult your Program Security Officer (PSO).

5D	(U)	Demand Driven Dissemination of Digital Data
A/D	(U)	Analog to Digital
AFP	(U)	Air Force Program
AFSCN	(U)	Air Force Satellite Control Network
AFT	(U)	Array Flight Test
AFWA	(U)	Air Force Weather Agency
AMP	(U)	All-Mode Processor
API	(U)	Activity Planning Item
ASPAM	(U)	Atmospheric Slant Path Analysis Model
AWBC	(U)	Alternate Wideband Communications (System)
BUCS	(U)	Backup Control System
BYE	(U)	BYEMAN *(officially retired as an SCI control system)*
C	(U)	CONFIDENTIAL
CAAS	(U)	Contracted Assistance and Advisory Service
CAS/PCD	(U)	Collection Activity Schedule/Processing Control Data
CCF	(U)	Communications Control Facility
CCS	(U)	Command and Control System
CIA	(U)	Central Intelligence Agency
CIA/OD&E	(U)	Central Intelligence Agency/Office of Development & Engineering
CIO	(U)	Central Imagery Office – now known as CITO (Central Imagery Tasking Office), a component of NGA
CMG	(U)	Control Moment Gyro
COMIREX	(U)	Committee on Imagery Requirements and Exploitation – no longer exists, function(s) performed by NGA
COMM	(U)	Communications
COTS	(U)	Commercial-Off-the-Shelf
CPAT	(U)	Collection Planning and Targeting
CPCI	(U)	Computer Program Configuration Item

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

(b)(3)

CSCI	(U)	Computer Software Configuration Item
CSD	(U)	Covariance Support Data
[redacted]		(b)(1) (b)(3)
D/A	(U)	Digital to Analog
[redacted]		(b)(1) (b)(3)
DCI	(U)	Director of Central Intelligence
DCID	(U)	Director of Central Intelligence Directive
DDP	(U)	Defense Dissemination Program
DDS	(U)	Defense Dissemination System
DEM	(U)	Digital Elevation Model
DMSP	(U)	Defense Meteorological Satellite Program
DNRO	(U)	Director of the National Reconnaissance Office
DoD	(U)	Department of Defense
DPE	(U)	Data Provider Element
DP/F	(U)	Data Processing/Facility
DSCS	(U)	Defense Satellite Communications System
DSM	(U)	Data System Modernization
ECS	(U)	Enhanced Collection System.
EELV	(U)	Evolved Expendable Launch Vehicle
EIS	(U)	Enhanced Imaging System
EO	(U)	Electro Optical
EO	(U)	Executive Order
ESD	(U)	Exploitation Support Data
ESD	(U)	Ephemeris Support Data
ESR	(U)	Engineering Study Request
[redacted]		(b)(1) (b)(3)
FIA	(U)	Future Imagery Architecture
FOC	(U)	Final/Full Operating Capability
FOUO	(U)	For Official Use Only
GCP	(U)	Ground Collection Planning (and Targeting)
GEO	(U)	Geostationary/Geosynchronous Earth Orbit
GGIS	(U)	Global Geospatial Information Services
GPE	(U)	Ground Performance Evaluation
GPS	(U)	Global Positioning System/Satellite
GPU	(U)	Ground Privacy Unit
GRA	(U)	Gyro Reference Assembly
GRD	(U)	Ground Resolved Distance
GRT	(U)	Ground Real-Time (Support)
GSD	(U)	Ground Sample Distance
GSR	(U)	Glint Smear Reduction
HANU	(U)	High Accuracy Navigation User (GPS)
HEO	(U)	Highly Elliptical Orbit
HQ USAF / XOW	(U)	U.S. Air Force Weather Agency
[redacted]		(b)(1) (b)(3)
I & W	(U)	Indications and Warning
[redacted]		(b)(3)
I/S	(U)	Imaging Satellite

ICA	(U)	Image Chain Analysis
IDP	(U)	Imagery Derive Product
IMINT	(U)	Imagery Intelligence
IMPS	(U)	Imagery Partial Segment
IOC	(U)	Initial Operating Capability
IPCD	(U)	Image Process Control Data
JWICS	(U)	Joint Worldwide Intelligence/Integrated Communications System
KH	(U)	KEYHOLE
LDT	(U)	Large Diameter Target
LEO	(U)	Low Earth Orbit
LIR	(U)	Laser Image Reconstructor/Recorder
LV	(U)	Launch Vehicle
MASINT	(U)	Measurement and Signature Intelligence
MC&G	(U)	Mapping, Charting & Geodesy
MCC	(U)	Mission Control Center/Complex
MCS	(U)	Mission Control Station
MGS	(U)	Mission Ground Station
MIND	(U)	Mission Integration and Development
MLE	(U)	Mean Life Estimates
MMD	(U)	Mean Mission Duration
MSD	(U)	Mensuration Support Data
MOA	(U)	Memorandum of Agreement
MSK	(U)	Medium Shift Keying
NASA	(U)	National Aeronautics and Space Administration
NGA	(U)	National Geospatial-Intelligence Agency
NGA/IA	(U)	NGA Imagery Analysis Office (formerly NPIC)
NIIRS	(U)	National Imagery Interpretability Rating Scale
NIS	(U)	New Imaging System
NOFORN	(U)	Not Releasable to Foreign Nationals
NPIC	(U)	National Photographic Interpretation Center
NRO	(U)	National Reconnaissance Office
NROL	(U)	National Reconnaissance Office Launch
NRP	(U)	National Reconnaissance Program
NSA	(U)	National Security Agency
OCA	(U)	Original Classification Authority
OD-4	(U)	Operating Division 4
ODPE	(U)	Optical Data Provider Element

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

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

OS	(U)	Optical Sub-system
OSL	(U)	Office of Space Launch
OSO	(U)	Operational Support Office
P/L	(U)	Payload
P0	(U)	Payload Zero
PDC	(U)	Processing and Distribution Center

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

PP/F	(U)	Photographic Production Facility
PSO	(U)	Program Security Officer
PVM	(U)	Pixel Variability Map
R/F	(U)	Receive Facility
R/S	(U)	Relay Satellite

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

RF	(U)	Radio Frequency
RMS	(U)	Requirements Management System
RMS IDMF	(U)	Requirements Management System Integrated Development & Maintenance Facility

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

RSEN	(U)	Risk Sensitive (formerly RUFF Sensitive)
S	(U)	(Collateral) Secret
S//TK	(U)	SECRET//TALENT KEYHOLE

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

SCG	(U)	Security Classification Guide
SCI	(U)	Sensitive Compartmented Information
SCIF	(U)	Sensitive Compartmented Information Facility
SECDEF	(U)	Secretary of Defense
SETA	(U)	Support Engineering and Technical Assistance
SGLS	(U)	Space Ground Link System
SIDS	(U)	Secondary Imagery Dissemination System
SIGINT	(U)	Signals Intelligence
SOCOMM	(U)	Special Operation Communications
SOW	(U)	Statement of Work
SPO	(U)	System Program Office

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

STS	(U)	Shuttle Transportation System
SYERS	(U)	Senior-Year Electro-Optical Reconnaissance System (See IPCG/ETP)
SV	(U)	Satellite Vehicle
TAS	(U)	Transmission Activity Schedule

TDPS	(U)	Transducer Data Processing Subsystem
		(b)(1) (b)(3)
TK	(U)	TALENT KEYHOLE
TOT	(U)	Time Over Target
TPAS	(U)	Target Planning and Scheduling
TPED	(U)	Tasking, Processing, Exploitation & Dissemination
TS	(U)	TOP SECRET
TWT	(U)	Traveling Wave Tube
TWTA	(U)	Traveling Wave Tube Assembly
U	(U)	UNCLASSIFIED
USIGS	(U)	United States Imagery and Geospatial Information System
VAFB	(U)	Vandenberg Air Force Base
WBCS	(U)	Wideband Communications System
WBID	(U)	Wideband Image WBID – Wideband Image Data
		(b)(1) (b)(3)

8.1 (U) Definitions

8.1.1 (U) Security Terms

(Table is UNCLASSIFIED//~~FOUO~~)

Access to Classified Information	The ability and opportunity for an individual to obtain knowledge of information that has been determined pursuant to EO 14291, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure (EO 12968, Sec. 1.1(d))
Accreditation	The formal approval of a specific place, referred to as a Sensitive Compartmented Information Facility (SCIF), that meets prescribed physical, technical, and personnel security standards. (DCID 6/1, Glossary) Also, official management authorization to operate an Automated Information System (AIS) under various conditions. (DCID 6/3, Annex C)
Agency	Any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C 102, and any other entity within the executive branch that comes into the possession of classified information, including DIA, NSA, and the NRO. (EO 12968, Sec. 1.1 (a))
Automated Information Systems	An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. (EO 12958, as amended, Sec. 4.1(f))
Automatic Declassification	The declassification of information based solely on (1) the occurrence of a specific date or event as determined by the original classification authority or (2) the expiration of a maximum time frame for duration of classification established under EO 13292. (EO 12958, as amended, Sec. 3.3(a))
BYE Security Control System	A former DCI Security Control System that protects key, specific and fragile details of reconnaissance satellite design and operation. *Officially retired - May 20, 2005*
Classification Guide	A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. (EO 12958, as amended, Sec. 6.1(g))
Classified National Security Information	Information that has been determined pursuant to EO 12958, as amended or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. (EO 12958, as amended, Sec. 6.1(h))

(Table is UNCLASSIFIED~~//FOUO~~)

Codeword	Any of a series of designated words or terms used with a security classification to indicate that the material classified was derived through a sensitive source or method. Constitutes a particular type of SCI, and is therefore accorded limited distribution. (DoD S-5105.21-M-1)
Collateral Information	Information identified as National Security Information under the provisions of EO 12958, as amended but which is not subject to enhanced security protection required for Special Access Program Information (DoD 5200.1-R)
Compartment	A system which strictly controls the dissemination, handling and storage of a specific class of classified information, limiting access to individuals with a specific need to know, in order to protect sources and methods. (NSA/CSS Classification Manual 123-2, Chapter 1)
Compromise	Unauthorized disclosure of classified information (DoD 5200.1-R)
CONFIDENTIAL	Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (EO 12958, as amended, Sec. 1.2 (a))
Damage to the National Security	Harm to the national defense or foreign relations of the US from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information. (EO 12958, as amended, Sec. 6.1 (j))
Declassification	The authorized change in the status of information from classified information to unclassified information. (EO 12958, as amended, Sec. 6.1 (k))
Declassification Authority	The official who authorized the original classification, if that official is still serving in the same position; The originator's current successor in function; A supervisory official of either, or Officials delegated declassification authority in writing by the agency head or the senior agency official. (EO 12958, as amended, Sec. 6.1 (l))
Declassification Guide	Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified. (EO 12958, as amended, Sec. 6.1(m))
Derivative Classification	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. It includes the classification of information based on classification guidance. (EO 12958, as amended, Sec 6.1(n))

(Table is UNCLASSIFIED//~~FOUO~~)

Decompartmentation	The removal of information from a compartmentation system without altering the information to conceal sources, methods, or analytical procedures. (SISR, Vol. I, Section 1)
Downgrading	A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level. (EO 12958, as amended, Sec. 6.1 (p))
Intelligence Community	Refers to the following agencies or organizations: CIA; NSA; DIA; the offices within the DoD for the collection of specialized national foreign intelligence through reconnaissance programs (including NRO); Bureau of Intelligence and Research, Department of State; the intelligence elements of the Army, Navy, Air Force, Marine Corps, FBI, Treasury, and Energy; and the staff elements of the DCI. (EO 12222, 3.3(f))
Intelligence Sources and Methods	The classified sources and methods the DCI protects under Section 102 of the National Security Act of 1947 and EO 12333. (DoD S-5105.21-M-1)
Mandatory Declassification Review	The review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.6 of EO 13292. (EO 12958, as amended, Sec. 6.1 (w))
National Security	The national defense or foreign relations of the US. (EO 12958, as amended, Sec. 1.1(a))
ORCON	"Dissemination and Extraction of Information Controlled by Originator." This marking may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. (DCID 6/6, Section 10.1)
Original Classification	The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. (EO 12958, as amended, Sec. 6.1 (b))
Original Classification Authority	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 that, in the interest of national security, requires protection against unauthorized disclosure. (EO 12958, as amended, Sec. 6.1 (c))
Safeguarding	Measures and controls that are prescribed to protect classified information. (EO 12958, as amended, Sec. 4.1(a))

(Table is UNCLASSIFIED~~//FOUO~~)

SCI Control System	The system of procedural protective mechanisms used to regulate or guide each program established by the Director of Central Intelligence as Sensitive Compartmented Information (SCI). A Control System provides the ability to exercise restraint, direction, or influence over or provide that degree of access control or physical protection necessary to regulate, handle, or manage information or items within an approved program. (DCID 6/1)
SECRET	Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (EO 12958, as amended, Sec. 1.2 (a))
Special Access Programs	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. (EO 12958, as amended, Sec. 6.1 (k))
TK	TALENT KEYHOLE. A DCI special access control system for compartmentation of information related to, or derived from, satellite reconnaissance systems, and products. (SISR, Vol II, Section II)
TOP SECRET	Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. (EO 12958, as amended, Sec. 1.2 (a))
Unauthorized Disclosure	A communication or physical transfer of classified information to an unauthorized recipient. (EO 12958, as amended, Sec. 6.1 (n))

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

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