~~SECRET~~

National Reconnaissance Office (U)

SIGINT Program Classification Guide (U)

September 16,1998

(Signed)
Orginal copy on file in the SIGINT Office of Security

Dennis D. Fitzgerald, Director
SIGINT Systems Acquisition & Operations Directorate (U)

Classified By: [redacted] (b)(3)
Classification Reason: 1.5 (a,c,e,g)
Declassify On: X1
Derived From: Multiple Sources (see pg 20)

Table of Contents

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

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

1.0 (U) GENERAL INSTRUCTIONS

_ 1.1 (U) Purpose

(U) The SIGINT Classification Guide compiles into one document all guidance for the classification of National Reconnaissance Office information for all SIGINT programs. As such, it is the baseline classification document for SIGINT operations and activities. It provides the basis for maintaining configuration control of classification management decisions. In conjunction with the "Life Cycle Security" process it will function to provide management with a tool for assessing the impact of change.

1.2 (U) Scope

~~(C)~~ The provisions of this guide apply to all SIGINT plans, systems, subsystems, and operations funded by, or under the cognizance of the SIGINT Systems Acquisition & Operations Directorate (SA&OD). This includes research, development, test and evaluation (RDT&E); application; production; related technology; and operational use of SIGINT systems. The information contained in this guide has been compiled from numerous source documents, which are listed in Section 23. For additional information or assistance in making classification determinations, contact the Program Security Officer (PSO) for the system in question, the SIGINT Security Office, or for contractor personnel, your BYEMAN Industrial Facility Security Control Officer (BIFSCO).

2.0 (U) APPLICABILITY & EFFECTIVE DATE

(U) This SIGINT Classification Guide applies to all personnel who have access to information addressed in this guide. It is effective as of the date on the title page.

3.0 (U) APPROACH

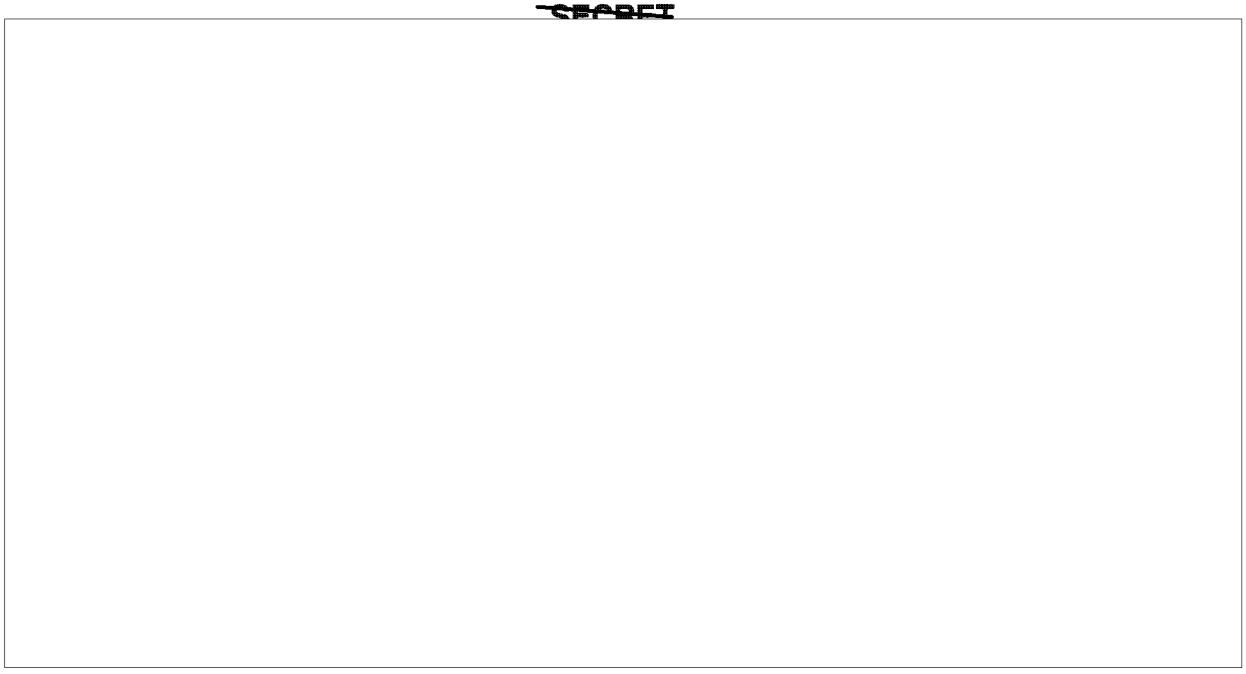
(U) The SIGINT classification development team used a "Life Cycle Security Process" to develop this guide. The process included analysis of the program life cycle, threat, open source, program segments, work breakdown structure, sensitive technologies, classification decision tool, risk management, and program protection architecture.

(U) The SIGINT classification development team was comprised of government and contractor personnel. It was coordinated with applicable System Program Offices (SPOs), field sites, contractors, and all Headquarters Directorates and Offices.

~~(S/B)~~ The SIGINT CG [redacted] nd draft [redacted] In developing the SIGINT CG all criteria from the previous guides were considered. (b)(1) (b)(3)

[redacted]

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



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

5.0 (U) OFFICE OF PRIMARY RESPONSIBILITY

(U) This guide is issued by the NRO SIGINT (SA&OD). The SIGINT CG establishes original classification guidance for NRO SIGINT operations and activities and is approved by the Director, NRO SIGINT (SA&OD).

6.0 (U) CLASSIFICATION AUTHORITY

(U) The Director, SIGINT SA&OD (an original classification authority) has established the classification level of and control system for some information contained in this guide. Other information is derived from guidance provided/documented in the:

1. National Space Policy, NSC-49, dated September 1996.
2. NRO Security Classification Guide, Version 4.0, dated 15 Oct 95.
3. Security Classification Guide for Integration and Launch of NRO Satellites on the Titan and Atlas Launch Vehicle Systems, 8 April 1997.
4. Signals Intelligence Security Regulations (SISR), "Review Comment and Coordination DRAFT," 29 April 1997.
5. Declassification of the "Fact of" Overhead SIGINT, The National SIGINT Committee memorandum, dated, 1 December 1995.
6. National Imagery and Mapping Agency Policy Series, Section 5, Part A, Classification Tables, dated 17 Sep 97.
7. Security Control Manual and Classification Guide for National MASINT Reconnaissance Materials (MASINT Policy Series).

7.0 (U) LEVELS OF SECURITY CLASSIFICATION AND CONTROL SYSTEMS

7.1 (U) National Security Classification Levels

(U) **TOP SECRET** shall be 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.

(U) **SECRET** shall be 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.

(U) **CONFIDENTIAL** shall be 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.

7.1.1 (U) Control Systems:

7.1.1.1 ~~(S)~~ BYEMAN Control System.

~~(C)~~ BYEMAN is a DCI sensitive compartmented information (SCI) control system which protects sensitive sources and methods used in the research, development and operation of space-based reconnaissance systems; some relationships; integration of launch and sensor platforms; command and control operations; key design and development details, acquisition documentation and plans, budget; and, survivability and vulnerability of systems.

7.1.1.2 (U) The TALENT-KEYHOLE Control System.

(U) A DCI SCI control system which protects technical data used in collection tasking, imagery or signals 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:

1. Imagery Intelligence (IMINT),
2. Signals Intelligence (SIGINT),
3. Electronic Intelligence (ELINT) [redacted] (b)(3)
4. Communications Intelligence (COMINT),
5. Foreign Instrumentation Signals Intelligence (FISINT); and,
6. Measurement and Signature Intelligence (MASINT).

7.1.1.3 (U) The COMINT Control System.

(U) A DCI SCI control system expressly authorized for handling or transmitting communications intelligence derived from satellite surveillance and other sources.

8.0 (U) CHOICE OF CONTROL SYSTEMS

~~(S/B)~~ The intended user community for the information is of key consideration when deciding which control system(s) to use for control of classified information. Some information may be handled by either the BYEMAN Control System or the TALENT-KEYHOLE Control System. Wherever practical, T-K should be the system of choice. Unless the information is in a category of information requiring BYEMAN protection exclusively, or unless there is a valid, well established reason for maintaining the information within BYEMAN system, T-K should be used. Care should be exercised to avoid BYEMAN controls on a document simply because a BYEMAN platform identifier (e.g. a codeword lik[redacted]was used when a T-K mission number would have served the same purpose. (b)(1) (b)(3)

~~(C)~~ For example, sensor sub-system design information is handled in the BYEMAN Control System by contractors building the space vehicle. Specific collection subsystem performance information may be handled in the TALENT-KEYHOLE Control System by analysts, planners and tasking personnel. The classification tables in this guide have several such examples. Just because the classification tables indicate an item may be protected within multiple control systems does not mean a document containing that item must be marked for joint handling. Use the control system most appropriate to the context and intended audience. Avoid joint handling, except when necessary.

~~(C)~~ There will be some instances when joint handling is appropriate. Suppose that for clarity it is necessary that a document include items of information one of which is exclusively controlled in the BYEMAN system while another item is exclusively controlled in the T-K system. Originators of classified documents should be careful to not unnecessarily cause joint handling and thereby needlessly restrict dissemination.

9.0 ~~(C)~~ CLASSIFICATION LEVELS FOR BYEMAN INFORMATION

9.1 ~~(C)~~ The following categories of BYEMAN information are considered "TOP SECRET":

a. ~~(C)~~ System survivability or vulnerability information, including satellites and ground facilities; susceptibility to countermeasures; and measures employed by these threats to the system. This particular set of data may be additionally protected by the BYEMAN Special Handling (SH) restrictions to distribution (see paragraph 10.0).
b. (U) Information or material, from which, the total system design can be determined.
c. ~~(C)~~ Technology advances in the state-of-the-art capabilities or unique use of new capabilities for obtaining additional valuable intelligence. This information may be Special Handling (SH) protected.

9.2 ~~(C)~~ The following categories of BYEMAN information are considered "SECRET":

a. (U) Operations data which would reveal system design details.
b. (U) Information describing general performance of the system not needed for product analysis.
c. (U) Technical design information or material pertaining to a classified subsystem, e.g., engineering reports, drawings, specifications, etc., which reveal specific subsystem design details.
d. (U) Integration information, which would reveal facts about the system.
e. (U) Contractual or administrative information about the system.
f. (U) Identity of participants, e.g., contractors, when identified with the Program.
g. (U) Data, material, or information which would reveal the identity of the program sponsor.

10.0 ~~(C)~~ BYEMAN SPECIAL HANDLING (SH) INFORMATION

~~(C)~~ Selected BYEMAN information that is critical to the mission may be designated for "SPECIAL HANDLING (SH)". When an NRO Program Director determines that certain BYEMAN information meets the specified conditions of sensitivity and the Director of the NRO concurs, all BYEMAN information relating to that especially sensitive information will be incorporated under the "SPECIAL HANDLING (SH)" restrictions. The sensitivity of BYEMAN SPECIAL HANDLING (SH) information may be based on various considerations, including, but not necessarily limited to the following:

1. (U) Cooperation with other organizations and/or governments when disclosure of such cooperation might prove damaging to those organizations, governments, the national security, or to the U.S. Government.
2. (U) Compromise of the successes of a particular activity could gravely impair our collection efforts or continued success.
3. (U) Sophisticated or otherwise sensitive efforts, methods, techniques, or technological phenomena, when related to reconnaissance collection activities that warrant such protection.
4. (U) Information obtained from other programs (SAP/SAR as an example).
5. (U) Vulnerability information on the total system, including the satellites; ground facilities; susceptibility to countermeasures; and measures employed to avoid these threats to the system.
6. (U) Intentionally uncorrected deficiencies that, under certain circumstances, result in vulnerabilities or inability to perform mission.

~~(C)~~ If persons involved in SIGINT Programs generate information they believe meets the criteria for "SPECIAL HANDLING (SH)," they should tightly control the information and advise the Program PSO for interim guidance. Requests to nominate BYEMAN information for "SPECIAL HANDLING" must be forwarded through the Program Director, coordinated through the Director of Security then to the Director or Deputy Director of the NRO for approval.

11.0 (U) CLASSIFICATION OR CONTROL SYSTEM CONFLICT RESOLUTION

~~(S/B)~~ The classification tables in this guide specify classification and control system(s) for information related to SIGINT systems and their products. Where control system or classification is not readily apparent from the table, or if a user believes conflicting, inaccurate, or unclear guidance has been provided, protect the information, products or activities at the highest applicable level pending resolution. Request guidance from the responsible SIGINT Program Security Officer or the NRO Director of SIGINT Security. A control system and classification review will be made by the NRO for BYEMAN matters and the functional program managers within DIA, NIMA, NSA, National SIGINT Committee and the MASINT Committee for TALENT-KEYHOLE matters.

(U) The fact that classified information has been inadvertently disclosed or released does not mean that it is automatically declassified. Unauthorized disclosures will be reviewed by the SIGINT SA&OD and other Directorates and Offices to determine appropriate and/or necessary courses of action.

12.0(U) COMPILATION/AGGREGATION OF INFORMATION

~~(C)~~ In some instances, the combination of several items of information produces a synergistic effect, i.e., the classification of all items of a similar type, when combined together is a higher level of classification than that of the individual items. For example, in the classification tables, classification of a single subsystem design is S/B, but if you have the design of all subsystems (i.e., the Satellite Vehicle (SV) design spec) the classification is TS/B. The higher classification is warranted due to the specificity and completeness of the information that could permit an adversary to completely avoid detection by this system. Users of this guide need to be sensitive to issues of compilation/aggregation.

13.0(U) FOR OFFICIAL USE ONLY

(U) Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public for one or more of the reasons cited in the Freedom of Information Act exemptions 2 through 9 shall be considered as being for official use only. No other material shall be considered or marked "For Official Use Only" and FOUO is not authorized as an anemic form of classification to protect national security interests. See DOD 5400.7-R DOD Freedom of Information Act Program and Policy Directive 001/97 - NRO Policy on use of "For Official Use Only", for addition guidance.

14.0(U) NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)

~~(C)~~ All 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 coordinated with the NRO security staff and with CIA/CRES/IPG. 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 single focal point for all imagery-related intelligence community disclosures to foreign officials. Release of NRO-related satellite technology which is unclassified is subject to export controls established by the Departments of Commerce and State with DoD coordination.

~~(C)~~ For each BYEMAN project, a record is maintained by the NRO security staff on information releasable to specific countries. Where the U. S. and a second party are involved in [redacted] ntegrated activity, U.S. personnel must be aware of the disclosure limits pertaining to the specific BYEMAN project, as well as any limitations concerning TALENT-KEYHOLE, COMINT, or COLLATERAL information. (b)(1) (b)(3)

NOTE: Certain organizations or agencies have authorized memoranda of understanding (MOUs) or other agreements allowing the release of non-BYEMAN classified intelligence information to foreign nationals. Release of information is bound by the specific terms of the agreements and supersede NOFORN caveats and restrictions.

15.0(U) ADMINISTRATION

15.1 (U) Visits by Representatives of State/Federal Governments

(U) The appropriate SIGINT Program Security Officer (PSO) will be notified of any contemplated visits by members of any legislative or Executive Branch of any State or Federal Government to any contractor or government agency if any portion of the visit could involve SIGINT Programs. The notification will include name, position, and area of interest of each visitor and the date of the proposed visit.

15.2 (U) Visits by Foreign Citizens or Representatives of Foreign Governments or Organizations

(U) The SIGINT cognizant Program Security Officer (PSO) will be notified of any contemplated visits by foreign citizens or representatives of any foreign governments, space agencies, or contractors to any United States contractor or government agency if any portion of the visit could involve access to any SIGINT Program information. The notification will include name, position, and area of interest of each visitor and the date of the proposed visit.

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

15.3 (U) Public Release of Information

(U) Only the NRO Office of Corporate Communications (NRO/OCC) may release information pertaining to SIGINT Programs. Prime and associate contractors are responsible for ensuring their subcontractors are aware of and comply with, this requirement. Unilateral public release of information pertaining to the NRO and its SV programs, operations, and launches is expressly prohibited.

15.4 (U) How to request changes to this guide.

(U) As circumstances or policies change, there will be a requirement to change information in this guide. The form below should be completed by individuals and forwarded through your security organization. They in turn will forward it by secure means to the SIGINT Security Office for review and comment.

SIGINT CLASSIFICATION GUIDE
CHANGE REQUEST

(to be filled out by Program Office PSO)

TO: SIGINT CLASSIFICATION AND POLICY UNIT

FROM: _____ _____
(PSO P.O.C.) (Office)

Originator: _____
(name, organization,
_____
functional activity) _____

Date: ____/____/____ Proposed Change: New Item___ Modification___ Challenge___

Item/Listing:
(guide section, item number, page) _____

Change description: _____
(include other _____
items affected) _____

Rationale: _____
_____
_____

(to be completed by the SIGINT Classification and Policy Unit)

Date: ____/____/____

Action Officer: _____

Request approved: Yes No
(circle one)

If NO state justification: _____
_____
_____

Coordinated with: _____
_____

Final Classification Determination: _____

Date approved by OCA: ____/____/____ Name of OCA: _____

16.0(U) USE OF THIS GUIDE

~~(C)~~ The Guide is classified SECRET and is controlled within the BYEMAN and TALENT-KEYHOLE Control Systems Jointly. The following guidelines will be strictly enforced:

(U) Reproduction of this document or any part is permitted for use in program activities. Requests for copies for other uses should be directed to the SIGINT Program Security Officer (PSO).

(U) Dissemination of this guide to organizations outside the security cognizance of the NRO must be approved by the SIGINT PSO and NRO Office of Security Policy and Operational Support.

~~(C)~~ The BYEMAN compartmentation restructure continues the requirement of each accessed individual to be personally responsible to determine the "need-to-know" of another BYEMAN accessed person before revealing Program information. Government program management personnel, PSOs, and contractor security personnel will ensure strict adherence to the DNRO's "must-know" access requirement policy. PSOs and security officers may extract information from this guide to tailor security classification guidance for tasks, as needed.

(U) CAUTION! Exact situations and classifications cannot always be specified in advance. Protect the information and refer questions to Program security. Any deviation from this guide must be approved by the SIGINT Program Director or PSO.

17.0(U) NRO DOD PROGRAM DESIGNATOR

(b)(3)

18.0(U) NRO LAUNCH DESIGNATOR

(b)(3)

19.0(U) SUBSTITUTE IDENTIFIER

~~(S)~~ Replacing the SV program name, number, or an NRO DoD program designator, with any substitute identifier in order to avoid classification of budgets, analyses, hardware, engineering processes, tests and associated documentation must meet the criteria listed in the paragraphs below. Information relative to SV mission, capability, vulnerability and operations can NOT be declassified through disassociation. Those items that can be handled as unclassified when disassociated from a specific SV program are explicitly identified in the classification tables.

(U) A substitute identifier may be any combination of numbers, letters, or an unclassified name. However, the substitute identifier must be randomly selected for the sole purpose of being used as a substitute identifier with no derivable unclassified relationship between the substitute identifier and the program, satellite vehicle contractor (SVC), or the NRO DoD program designator.

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

(U) DoD collateral usage of substitute identifiers must be approved by the OSL prior to implementation. All other usage of substitute identifiers must be approved by the applicable NRO Directorate or Office.

20.0(U) SECURITY AND CLASSIFICATION RECOMMENDATIONS

(U) All users of this guide are encouraged to assist in improving and maintaining its currency and relevancy. Comments and recommendations should be forwarded through security offices to the Program Security Officer (PSO) or to the NRO, Director of Security. (See change request form in Section 14.0).

21.0(U) CLASSIFICATION TABLE LAYOUT AND EXPLANATION

(U) The following table provides security guidance itemized by program segments. The table is not and cannot be all inclusive. Absence of a particular item does not imply that the item can be considered UNCLASSIFIED. Refer questions to the Program Security Officer (PSO). If the table indicates that an item of information can be protected in more than one security control system, use the guidelines in section 8.0 (Choice of Control Systems).

(U) The classification column contains the classification level, the control system column contains the symbol for a control system if applicable. The Rationale/Remarks column will contain a rationale for the classification level and other comments.

~~(C)~~ The following key is provided for understanding the symbols used in the classification tables:

EO 12958 CLASSIFICATION LEVELS		CONTROL SYSTEMS	
TS	- TOP SECRET	B	- BYEMAN
S	- SECRET	TK	- TALENT-KEYHOLE
C	- CONFIDENTIAL	SI	- COMINT

OTHER DATA	
U	- UNCLASSIFIED
FOUO	- FOR OFFICIAL USE ONLY
NF	- NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)
LIMDIS	- LIMITED DISTRIBUTION
SHI	- SPECIAL HANDLING INFORMATION
5 EYES	- US/UK/NZ/CAN/AUS
CRYPTO	- CRYPTOGRAPHIC
OCA	- ORIGINAL CLASSIFICATION AUTHORITY

(b)(3)

22.0(U) REASON FOR CLASSIFICATION

(U) Under the provisions of E.O. 12958, the reason(s) for a classification decision must be documented. To meet this requirement, the E.O. specifies that, at a minimum, reference to the pertinent classification category(ies) described in Section 1.5 of E.O. 12958 plus the letter(s) that correspond to the category(ies) should be listed. The classification categories preceded by their corresponding letter designators are listed below:

(a) "Military plans, weapons systems, or operations."
(b) "Foreign government information."
(c) "Intelligence activities, intelligence sources or methods, or cryptology."
(d) "Foreign relations or activities of the United States, including confidential sources."
(e) "Scientific, technological, or economic matters relating to the national security."
(f) "United States programs for safeguarding nuclear materials or facilities."
(g) "Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security."

23.0(U) DECLASSIFICATION INSTRUCTIONS

(U) Executive Order (E.O.) 12958 specifies that the original classification authority will apply a date, not to exceed 10 years, or event for declassification that corresponds to the lapse of the information's national security sensitivity. Individuals with original classification authority may determine that certain information must remain classified beyond 10 years. In this case, 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 1.6 of E.O. 12958 (e.g. X1 equates to: Reveals an intelligence source, method, or activity, or a cryptology system or activity). The X markings and corresponding declassification exemptions are as follows:

X1 - "Reveals an intelligence source, method, or activities or a cryptology system or activity."
X2 - "Reveals information that would assist in the development or use of weapons of mass destruction."
X3 - "Reveals information that would impair the development or use of technology within a United States weapons system."
X4 - "Reveals United States military plans, or national security emergency preparedness plans."
X5 - "Reveals foreign government information."
X6 - "Would damage relations between the United States and foreign government, reveal a confidential source, or undermine diplomatic activities that are reasonably expected to be ongoing for period greater than in paragraph (b).
X7 - "Would impair the ability of responsible United States Government officials to protect the President, the Vice President, and or other individuals for whom proactive services, in the interest of national security, are authorized."
X8 - "Would violate a statute, treaty, or international agreement."

24.0(U) PORTION MARKING

(U) Executive Order (E.O.) 12958 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 that will be maintained internal to 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 security cognizance of the Director of the NRO.

(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.

25.0(U) REFERENCE DOCUMENTS

1. (U) Executive Order (E.O.) 12958, Classified National Security Information, dated 17 April 1995.
2. (U) Executive Order (E.O.) 12951, Release of Imagery Acquired by Space -based National Intelligence Reconnaissance Systems, dated 22 February 1995.
3. (U) NRO Classification Guide, Version 4.0, 14 October 1995.
4. (U) National Space Policy, NSC-49, dated, September 1996.
5. (U) Declassification of the "Fact of" Overhead SIGINT, The National SIGINT Committee memorandum, dated, 1 December 1995.
6. (U) Director of Central Intelligence Directive (DCID) 1/19, Security Policy for Sensitive Compartmented Information (SCI) and its accompanying Security Policy Manual for SCI Control Systems (Attachment A).
7. (U) Director of Central Intelligence Directive (DCID) 5/5, Conduct of SIGINT Liaison with Foreign Governments and the Release of U.S. SIGINT to Foreign Governments, dated May 1983.
8. (U) Director of Central Intelligence Directive (DCID) 5/6, Intelligence Disclosure Policy, dated 30 Jun 98.
9. (U) Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information, dated 30 Jun 98.
10. (U) Signals Intelligence Security Regulations (SISR), "Review Comment and Coordination DRAFT," July 1998.
11. (U) DOD Freedom of Information Act Program, DoD 5400.7-R, dated May 1997.
12. (U) Sensitive Compartmented Information (SCI) Security Manual, Communications Intelligence (COMINT) Policy, DoD TS-5105.21-M-2, July 1985.
13. (U) National Imagery and Mapping Agency Policy Series, Section 5, Part A, Classification Tables, dated 17 Sep 97.
14. ~~(C)~~ BYEMAN Security Manual, 8 June 1993. (Interim)
15. ~~(C)~~ Security Implementation Plan for BYEMAN Compartmentation Restructure, 18 November 1993.
16. (U) The Implementation Plan for Further Decompartmentation and Declassification of the National Reconnaissance Office, 24April 1995.
17. ~~(C)~~ The BYEMAN Restricted Knowledge (BRK) for BYEMAN Special Handling Information, 14 October 1993.
18. (U) Further Declassification of NRO Contractor Associations, 1 August 1997.
19. ~~(S/B)~~ SOCOMM message, "Declassification of NRO Launch and Associated Facts," 072114 March 1997, Cite 8496, aka Policy Notice 001/97.
20. (U) Implementation Plan for NRO Launch Declassification, 1 March 1997.

21. (U) OPNAL Notice 5510 (Limited Dissemination Controls) 29 Dec 89.
22. [redacted] (b)(1)
23. (b)(3)
24.
25.
26.
27. (U) National Imagery and Mapping Agency Policy Series, Section 5, Part A, Classification Tables, dated 17 Sep 97.
28. (U) Data Communications Group Classification Guide, 25 September 1997.
29. (U) Security Classification Guide for Integration and Launch of NRO Satellites on the Titan and Atlas Launch Vehicle Systems, 8 April 1997.
30. (U) Security Control Manual and Classification Guide for National MASINT Reconnaissance Materials (MASINT Policy Series).
31. (U) Declassification of the terms "TALENT-KEYHOLE" and the satellite mission designator "KH" and their general relationship to intelligence, February 23, 1995.
32. [redacted] (b)(1) (b)(3)
33. (U) Declassification of the terms "TALENT-KEYHOLE" and the satellite mission designator "KH" and their general relationship to intelligence, February 23, 1995.

26.0(U) RATIONALE

(U) The following list is the rationale used to decide what type of information would be revealed by a compromise of data. The number which corresponds to the appropriate rational appears in the classification table in the rationale/remarks column.

1. (U) Reveals a covert or classified relationship.
2. (U) Reveals vulnerability or survivability.
3. (U) Reveals total system design to include communications network and connectivity details.
4. (U) Reveals technology advances in state-of-the-art capabilities or unique new capabilities.
5. (U) Reveals system design and communications network details.
6. (U) Reveals sub-system design and communications network details.
7. (U) Reveals system performance not needed for product analysis.
8. (U) Integration information revealing design details or mission.
9. (U) Reveals intelligence mission.
10. (U) Reveals command and control techniques heightening vulnerability.
11. (U) Launch schedules and logistics revealing system design details, capabilities, or mission.
12. (U) Contractual or administrative information revealing system design details, communications network infrastructure, capabilities or mission.
13. (U) Reveals contractor or other relationship that is covert, compartmented, or classified.
14. (U) Reveals program sponsor (i.e., the NRO).
15. (U) Reveals sensitive sources and methods.
16. (U) Reveals operational, system, communications network or other information which may lead to degradation or negation of mission objectives.
17. (U) Reveals information which may allow an adversary to gain technical competence or advantage.
18. (U) Reveals details of collection capability over denied area that cannot be attributed to any sensor other than a satellite.

ACRONYM LIST (U)

NOTE: ASTERISKED ITEMS ARE CONTROLLED WITHIN S/TK CHANNELS WHEN ASSOCIATED WITH THE NRO. DOUBLE ASTERISKED ITEMS ARE S/B WHEN ASSOCIATED WITH THE NRO.

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

(U)AFP	Air Force Program.
(U)AFSCN	Air Force Satellite Control Network.
(U)AFSPACECOM	Air Force Space Command.
(U)AFSPC	Air Force Space Command.
(U)AGE	Aerospace Ground Equipment.
(U)AOTES	Automated Operational Technical Exchange System.
(U)ARV	Aerospace Research Van.
(U)AS&TD	Advanced Systems & Technology Directorate.
(U)ASE	Aerospace Support Equipment.
(U)ASPO	Army Space Program Office.
(U)ATP	Advanced Tracking Prototype.
(U)BV	Booster Vehicle.
~~(C)~~BYE	~~(S/B)~~ BYEMAN.
(U)CAAS	Contract Advisory & Assistance Services.
(U)CALS	Computer Aided Logistics Support.
(U)CALVAN	Calibration Van Group.
(U)CCO	COMINT Channels Only.
(U)CDRL	Contract Data Requirements Lists.
(U)CIA	Central Intelligence Agency.
(U)CIA/OD&E	Central Intelligence Agency/Office of Development & Engineering.
(U)Classic Wizard*	UNCLASSIFIED Program Name.
(U)CMCC	Command Management Control Center.
(U)COMINT	Communications Intelligence.
(U)COMSEC	Communications Security.
(U)CONOPS	Concept of Operations.
(U)CONUS	Continental United States.
(U)CPEG	Cross Program ELINT Geolocation.
(U)CRITICOMM	Critical Intelligence Communications Systems.
(U)CSTC	Consolidated Space Test Center.
(U)CW	Continuous Wave.
(U)DARPA	Defense Advanced Research Projects Agency.
(U)DCI	Director of Central Intelligence.
(U)DCID	Director Of Central Intelligence Directive.
(U)DEFSMAC	Defense Special Missile and Astronautics Center.
(U)DNRO	Director of the National Reconnaissance.
(U)DOD	Department of Defense.
(U)DRSP	Defense Reconnaissance Support Program.
(U)DSCS	Defense Satellite Communications System.
(U)DSP	Defense Support Program.
(U)DSSCS	Defense Special Security Communications System.
(U)EAGE	Electrical Aerospace Ground Equipment.
(U)ECI	Exceptionally Controlled Information.

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

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

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

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

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

(U)ELINT	Electronic Intelligence.
(U)Elsets	Element sets. A set of six numbers (mean motion, eccentricity, inclination, right ascension of the ascending node, argument of perigee, and mean anomaly) that make up the element set and describe the satellite's orbit). The orbital elements are used by the satellite owner/operator and the space surveillance sites to track space objects.
(U)ELV	Expendable Launch Vehicle.
(U)EMC	Electro-magnetic Compatibility.
(U)EMI	Electro-magnetic Interference.
(U)EMP	Electro-magnetic Pulse.
(U)EPDS	Electronic Processing Data System.
(U)ER	Eastern Range.
(U)ERP	Effective Radiated Power.
	(b)(1)
~~(S/B)~~FARRAH (F-I, F-II, etc.)	Satellite nickname. (b)(1) (b)(3)
(U)FOC	Final Operational Capability.
(U)FOSC	Facility Operations Support Center(s).
(U)FOUO	For Official Use Only.
(U)GEO	Geostationary/ Geosynchronous Earth Orbit.
~~(S/B)~~GLORIA (G-I, G-II, etc.)	Satellite nickname.
(U)GTG	Ground Terminal Group.
(U)HEMP	High Energy Magnetic Pulse.
(U)HEO	Highly Elliptical Orbit.
(U)HULTEC	Hull to Emitter Correlation.
(U)I&W	Indications and Warning.
(U)ICEBOX	Improved communication Equipment Enclosure.
(U)ILC	Initial Launch Capability.
(U)IMINT	Imagery Intelligence.
	(b)(1) (b)(3)
(U)IRON	Inter-range Operations Numbers.
	(b)(1) (b)(3)
(U)LCO	Launch Communications Office (b)(1) (b)(3)
(U)LEO	Low Earth Orbit.
(U)LEO SPO	System Program Office for Low Altitude Programs.
(U)LMCC	Launch Management Control Center.
(U)LOCC	Launch Operations Control Center.
~~(S/B)~~LORRI (L-I, L-II, etc.)	Satellite nickname.
(U)LPO	Launch Program Office.
(U)LSI SPO (SAF/SP)	Launch Systems Integration Systems Program Office (SAF/SP).
(U)LSI SPO (SMC/IMO)	Launch Systems Integration Systems Program Office (SMC/IMO).
(U)LSI SPO (SAF/SL)	Launch Systems Integration Systems Program Office (SAF/SL).
(U)LSIC	Launch Systems Integration Contractor.
(U)LV	Launch Vehicle.
	(b)(1) (b)(3)
(U)MAGE	Mechanical Aerospace Ground Equipment.
(U)MASINT	Measurement and Signature Intelligence.
(U)MCC	Mission Control Center.
(U)MCS	Mission Control Station.

(U)MECO	Main Engine Cut-Off.
(U)MGS	Mission Ground Station.
(U)MOSC	Mission Operations Support Center at NRL (Bldg 259).
(U)MRC	Midway Research Center.
(U)MS&O	Office of Management, Services & Operations.
(U)MSF	Mission Support Facility.
(U)NAVSOC	Navy Space Operations Center.
(U)NAVSPACMD	Navy Space Command.
(U)NCST	Navy Center for Space Technology
	(b)(1) (b)(3)
(U)NRL	Naval Research Laboratory.
(U)NRO	National Reconnaissance Office.
(U)NRP	National Reconnaissance Program.
(U)NSA	National Security Agency.
(U)NSG	Naval Security Group.
(U)NSOC	National Security Operations Center.
(U)NSRL	National SIGINT Requirements List.
(U)OBP	On-board Processing.
(U)OCA	Original Classification Authority.
(U)OCMC	Overhead Collection Management Center
	(b)(3) (b)(1)
(U)OPELINT	Operational Electronic Intelligence.
(U)OPSCOMM	Operational Communications.
(U)OPSEC	Operations Security.
~~(S)~~OSF	Operations Support Facility.
(U)OSL	Office of Space Launch.
(U)OSO	Operational Support Office. (b)(1)
(U)P&A	Office of Plans & Analysis. (b)(3)
(U)P/L	Payload
(U)P-989*	Inactive Program Name
	(b)(1) (b)(3)
(U)PADS	Prototype Analysis Display System.
(U)PARAGON	Prototype Air Reporting and Ground Operating Node
	(b)(1) (b)(3)
(U)Pathfinder	A test to verify the compatibility between the SV and its facilities.
(U)PAWS	Prototype Analyst Work Station.
(U)PD-14 (OLD SPAWAR-40)	Program Directorate - 14.
(U)PDEC	Product Development Evaluation Center.
(U)PDMS	Payload Data Management System.
(U)PLF	Payload Fairing.
(U)POCC	Payload Operations Control Center.
~~(S/B)~~POPPY	Inactive Program Name.
(U)PRI	Pulse Repetition Interval.
(U)PROFORMA	Machine to machine signals.
(U)PSO	Program Security Officer.
(U)R&D	Research & Development
	(b)(1) (b)(3)
~~(S)~~RAQUEL (R-I, R-II, etc.)	Satellite nickname.
(U)RF	Radio Frequency.
(U)RFP	Requests for Proposal.

(U)RRC	Regional Reporting Center.
(U)RSOC	Regional SIGINT Operations Center.
	(b)(1) (b)(3)
(U)S	Collateral Secret.
~~(C)~~S/B	~~(C)~~ SECRET BYEMAN.
(U)S/C	Spacecraft.
(U)S/TK	SECRET/TALENT-KEYHOLE.
	(b)(3)
(U)SAF/SL	Secretary of the Air Force /Space Launch.
(U)SAF/SO	Secretary of the Air Force/Space Operations
(U)SAF/SP	Secretary of the Air Force/Special Projects.
(U)SAF/SS**	Secretary of the Air Force/Space Systems.
(U)SAO	Space Applications Office
(U)SAF/ST	Secretary of the Air Force /Science & Technology.
	(b)(1) (b)(3)
(U)SBS	Spacecraft Bus System.
(U)SCC	Space Classified Catalog.
(U)SCC	Spacecraft Control Center.
(U)SCG	Security Classification Guide.
(U)SCI	Sensitive Compartmented Information.
(U)SCIF	Sensitive Compartmented Information Facility.
(U)SCTS	Space Cargo Transportation System.
(U)SE/GE	Space Element/Ground Element.
	(b)(1) (b)(3)
(U)SECDEF	Secretary of Defense.
(U)SED	Signal Externals Data.
(U)SELORS	Ship Emitters Location Report.
(U)SEO	Systems Engineering Office
(U)SETA	Support Engineering and Technical Assistance.
(U)SGLS	Space Ground Link System.
~~(C)~~SH	Special Handling.
(U)SI	Special Intelligence.
(U)SIGINT	Signals Intelligence.
	(b)(1) (b)(3)
(U)SMC/CL	Space Missile Center/Launch Programs Office.
(U)SMC/CLM	Space Missile Center/Atlas Program Office.
(U)SMC/CLX	Space Missile Center/Operations Support & Integration Office.
(U)SMC/IMO	Space Missile Center/Information Management Office.
~~(S)~~SOCOMM	Special Operations Communications.
(U)SOI	Signals of Interest.
(U)SOW	Statements of work.
(U)SPO	Systems Program Office
(U)SSD/IMO	Space Systems Division/Information Management Office.
(U)SSD/OD-1	Space Systems Division/Operating Division - 1
(U)SSIC	Space Segment Integration Contractor.
(U)SSPO	Space Systems Program Office.
(U)STS	Space Transportation System.
(U)SV	Satellite Vehicle.
(U)SV SPO	Satellite Vehicle, Systems Program Office.
(U)SVC	Satellite Vehicle Contractor.
	(b)(1) (b)(3)
(U)TAXDIS-B	Tactical Data Information Exchange System Broadcast.

	(b)(1) (b)(3)
(U)TENCAP	Tactical Exploitation of National Capabilities.
(U)TEP	Tactical ELINT Processor.
(U)TK	TALENT-KEYHOLE.
(U)T-K	TALENT-KEYHOLE.
(U)TLD	Titan Launch Dispenser.
(U)TMGS	Transportable Mobile Ground Station.
(U)TOPS	Tactical On-Board Processing System.
	(b)(1)
(U)Trailblazer	A test to verify the compatibility of the SV and its interface with the LV. (b)(3)
(U)TS	TOP SECRET.
~~(C)~~TS/B	~~(C)~~ TOP SECRET/BYEMAN.
(U)TS/SI	TOP SECRET/COMINT .
(U)TS/TK	TOP SECRET/TALENT-KEYHOLE.
(U)TSF	Technical Support Facility.
(U)TT&C	Telemetry, Tracking & Commanding.
(U)TUDE	Teletype User Data Entry.
~~(S/B)~~URSALA (U-I, U-II, etc.)	Satellite nickname.
(U)USA	U.S. Army.
(U)USAF	U.S. Air Force. (b)(1)
(U)USMC	U.S. Marine Corps. (b)(3)
(U)USN	U.S. Navy.
(U)VRK	Very Restricted Knowledge.
	(b)(1) (b)(3)

Table above is classified ~~S/B/TK.~~

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692

Approved for Release: 2018/12/21 C05102692