DEPARTMENT OF DEFENSE
AIR FORCE PROGRAM EXECUTIVE OFFICER FOR SPACE (AFPEO/SP)

Military Communications Systems Wing (MCSW)
LOS ANGELES AFB, CA 90245

GLOBAL BROADCAST SERVICE SECURITY CLASSIFICATION/DECLASSIFICATION GUIDE (SCG)

29 April 2007
(Date)

Approved By
Air Force Program Executive Officer for Space (AFPEO/SP)

Issued By
Air Force MILSATCOM Systems Wing (MCSW)
483 N. Aviation Blvd.
El Segundo CA 90245-2808

This Security Classification Guide supersedes the System Protection Guide (SPG) Annex C of 15 October 1999.

Distribution A Applies: Approved for public release; distribution unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
16-05-2007	Classification Guide	29 04 2007 - 29 04 2009

4. TITLE AND SUBTITLE
Global Broadcast System (GBS) Classification/Declassification Guide, 29 Apr 07

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
N/A

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
MILSATCOM Systems Wing (MCSW)
483 North Aviation Blvd
El Segundo, Ca 90245

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Air Force (USAF)
Space and Missile Systems Center (SMC)
483 North Aviation Blvd
El Segundo, Ca 90245

10. SPONSOR/MONITOR'S ACRONYM(S)
USAF/SMC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
A. Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
This Security Classification Guide supersedes the GBS System Protection Guide (SPG) Annex C of 15 October 1999.

14. ABSTRACT
The Global Broadcast Service (GBS) is an extension of the Global Information Grid (GIG) that provides worldwide, high capacity, one-way transmission of video, imagery, and other high-bandwidth information, via Transmit Suites (including Theater Injection Points (TIP's)) to Receive Suites, supporting the nation's command centers and joint combat forces in garrison, in transit, and deployed within global combat zones. It employs readily available satellite-based broadcast commercial technologies, which are relatively inexpensive and easily integrated into existing systems and processes. To this end, GBS currently uses broadcast payloads on three Ultra-High Frequency Follow-On (UFO) satellites and leased commercial satellite transponders as required.

15. SUBJECT TERMS
N/A

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Gerald D. Jones, GS-11, DAFC
UNCLAS	UNCLAS	UNCLAS	Approved for public release; distribution	44	19b. TELEPHONE NUMBER *(Include area code)* (310) 653-9773

CHANGE NOTICE REGISTER (CNR)

This Change Notice Register (CNR) will be updated to reflect all issuances of interim changes, updates or revisions to this SCG with entries listed in consecutive order. The change transmittal correspondence shall be filed immediately beneath the CNR in reverse chronological order (most recent on top) until revised or updated SCG incorporating changes is received.

CHANGE NOTICE REGISTER

Change No.	Date	Description

FOREWORD

DESCRIPTION

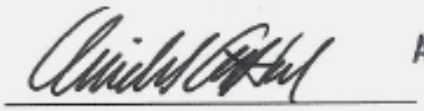
The Global Broadcast Service (GBS) is an extension of the Global Information Grid (GIG) that provides worldwide, high capacity, one-way transmission of video, imagery, and other high-bandwidth information, via Transmit Suites (including Theater Injection Points (TIP's)) to Receive Suites, supporting the nation's command centers and joint combat forces in garrison, in transit, and deployed within global combat zones. It employs readily available satellite-based broadcast commercial technologies, which are relatively inexpensive and easily integrated into existing systems and processes. To this end, GBS currently uses broadcast payloads on three Ultra-High Frequency Follow-On (UFO) satellites and leased commercial satellite transponders as required.

Starting in FY08, the constellation of up to five Wideband Gapfiller Satellites (WGS) will also carry GBS. Theater Injection Point (TIP) terminals provide a deployable Ka-band uplink capability that can operate directly from a Combatant Commander's Area of Responsibility.

Information resources deliver products for daily broadcast to two Satellite Broadcast Managers (SBMs) based on defined mission profiles approved by Theater Information Managers. At the SBM, the Planning and Management (P&M) application schedules broadcasts to users as well as keep users, products, and mission profiles current.

To obtain a more detailed description of the GBS System, please consult the System Security Authorization Agreement on the GBS Website (https://sharepoint.hanscom.af.mil/sites/GBSJPO/default.aspx).

APPROVED BY:



APR 2 9 2007

MICHAEL A. HAMEL
Lieutenant General, USAF
AFPEO/SP

TABLE OF CONTENTS

SECTION I - GENERAL INFORMATION

1.0 PURPOSE

This SCG provides guidance for uniform security classification, declassification, management and protection of classified information for the Global Broadcast Service (GBS) Program and activities associated with its systems, plans, programs, projects and user information (e.g. Section II, paragraphs 2.0 and 3.0). It applies to the GBS Ground Segments (Transmit Suites (including Theater Injection Points (TIP's)) and Receive Suites). This SCG also includes guidance for the protection of unclassified technical data, controlled unclassified information (CUI) and For Official Use Only (FOUO) information. SPAWAR PMW 146 controls security guidance for the UFO satellites (Contact Information: PEO Space Systems, PMW 146, 4301 Pacific Hwy, San Diego, CA 92110-3127, (619) 524-7756). Security aspects of GBS systems operations are covered in the GBS Concept of Operations (CONOPS) (Contact Information: Global Broadcast Service SATCOM Operations Manager (SOM), Offutt AFB, NE 68102, (402) 294-2814).

2.0 AUTHORITY

This SCG is issued under the authority of the Air Force Program Executive Officer for Space (AFPEO/SP). The AFPEO/SP holds delegation authority from the Secretary of the Air Force to exercise Top Secret Original Classification Authority (OCA) and to establish security classification policy and guidance over all AFPEO/SP funded technology, development and acquisition programs for National Security Space (NSS) systems. This SCG is required and complies with the provisions of Executive Order (E.O.) 12958 as amended, "Classified National Security Information;" DoD 5200.1-R, "Information Security Program"; and AFI 31-401, "Information Security Program Management". For Secret Republic of Korea and US (S-ROKUS) information, please refer to UNC/CFC Regulation 380-1.

3.0 APPLICABILITY AND SCOPE

This SCG shall be cited as the basis for classifying, reclassifying, or declassifying information associated with the GBS Program. It provides overarching classification guidance and is to be used in conjunction with the GBS System Security Authorization Agreement.

4.0 OFFICE OF PRIMARY RESPONSIBILITY (OPR)

The OPR for this guide is the GBS Joint Program Office (JPO), in coordination with the AFPEO/SP's staff office, Space and Missile Systems Center, Acquisition Systems Protection and International Programs, (SMC/PIP). The GBS JPO provides the technical expertise to develop this SCG oversees application of and administers classification guidance relative to GBS classified information. SMC/PIP, as staff to AFPEO/SP, coordinates proposed security classification policy guidance for consistency and uniformity across all AFPEO/SP programs. All inquiries concerning content, interpretations, and clarifications of this SCG shall be forwarded to the OPR and MILSATCOM Systems Wing, Security Office (MCSW/OM) at the addresses below for subsequent staffing as appropriate.

Office of Primary Responsibility:

GBS Joint Program Office
5275 Leesburg Pike
Falls Church, VA 22041
Attn: GBS Program Manager
(781) 271-6027

MILSATCOM Systems Wing

MCSW/OM
483 N. Aviation Blvd
Los Angeles AFB
El Segundo, CA 90245
(310) 653-1321

5.0 CLASSIFICATION CURRENCY

Changes will be made to this guide as necessary to provide users with the most current classification guidance available. Consequently, this SCG will be reviewed for currency every two years (or earlier if circumstances require). Approved changes will be distributed to affected organizations and user community via change transmittal correspondence.

Any additions or changes in levels of classification (new classification entries, reclassification or declassification) shall be coordinated through the affected organizations and user community prior to inclusion in the SCG and subsequent submittal and approval by the OCA. Information submitted for re-grading should be protected at its current level of classification until re-grading is approved or denied by the OCA. If approved, any change in classification of GBS information will be distributed to the applicable/affected organizations and user community through a revised/updated SCG or through interim change pages.

Minor interim changes will be handled as "pen and ink" changes with the change annotated within the document next to the affected information. The margin shall be annotated with both the change number and the date of the change notice transmittal correspondence. More complex changes (either removal, replacement or new page insertions) will be handled according to instructions provided in the change notice transmittal correspondence. The change transmittal correspondence shall be filed immediately beneath the CNR in reverse chronological order (most recent on top) until revised or updated SCG incorporating changes is received.

6.0 CLASSIFICATION CHALLENGES AND RECOMMENDATIONS

Any authorized holder of GBS unclassified or classified information which has substantial reason to believe that information is not classified at the appropriate level or is incorrectly, improperly or unnecessarily classified is encouraged to challenge that classification and bring about corrective action. The challenge may be initiated either informally or formally. Informal questioning regarding classification is encouraged before resorting to a formal challenge. Classification challenges and recommendations should include a sufficient description of information being challenged, the reason or justification the holder believes the information is improperly classified, and the relevant classification policy. Formal classification challenges and/or recommendations should be submitted to the OPR and SMC/PIP (call each for appropriate means of transmission). Clearly identify what the current classification is, recommended classification, and rationale for the change.

7.0 REASON FOR PROTECTING NATIONAL SECURITY SPACE (NSS) INFORMATION

While AFPEO/SP is committed to keeping fundamental research unclassified and available to a broad community where possible, it must also protect certain information. Within the research, development, testing, and evaluation process related to military space capabilities, performance of planned or developing systems, and unique technologies critical to NSS need to be protected. These protective actions are necessary to deny adversaries information regarding U.S. capabilities and intentions. Compromise of U.S. capabilities or intentions would permit adversaries to modify their military or space systems and plans that lessen the effectiveness of U.S. defense systems and undermine U.S. investments in the acquisition of these systems.

Information related to NSS systems that may require classification includes, but is not limited to:

(1) Information, which if known by an adversary could reduce the time, cost, and risk associated with developing more viable NSS systems;

(2) Vulnerabilities and limitations;

(3) Detailed quantitative and qualitative information, to include performance capabilities, design specifications, parameters, schedules, and dates pertaining to specific applications, the status of developmental efforts and direction of effort in specific NSS system development programs, and resource expenditures;

(4) Information concerning breakthroughs and advances in technology and applications;

(5) Technical information that could significantly aid another country in the development of similar equipment, thus reducing the requirement for commensurate expenditure of resources, as compared to U.S. efforts, and reducing U.S. lead time advantages;

(6) Information that could significantly assist a potential enemy in the quantitative or qualitative assessment of U.S. actual and planned NSS systems (e.g. red/blue team test results);

(7) Quantitative results from simulations and testing (e.g. System Integration and Test Lab results, B/W increase results);

(8) Information concerning the development of countermeasures or counter-countermeasures that reveal NSS systems vulnerability or current U.S. judgment as to their effectiveness or efficiency and possible weapon systems application; and

(9) Intelligence and threat data that drive NSS system research, design, and policy.

(10) Operational vulnerabilities of off-site facilities or agencies that provide GBS Source Material. If vulnerabilities identified by GBS, handle IAW internal GBS Vulnerabilities. If vulnerabilities identified by Source, handle IAW Source markings.

7.1 REASONS FOR CLASSIFYING INFORMATION

In accordance with E. O. 12958, as amended, provided below are reasons for classifying GBS information:

1.4 (a): Military plans, weapon systems, or operations;

1.4 (b): Foreign government information;

1.4 (c): Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

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

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

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

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

1.4 (h) weapons of mass destruction

8.0 COMPILATION OF INFORMATION

The determination of the appropriate classification of information or material, in any form, is to be based on consideration of all applicable information; to include but is not limited to GBS information. Individual items of information when standing alone may be unclassified or warrant a lower classification level than when the information is combined with other informational elements. However, these same individual items of information may become classified when compiled with other elements of information. Security classification in each specific case must be determined by the OCA for this SCG. Also, if an authorized holder of classified information believes that compilation of information has resulted in classified information that is not covered in this SCG, the holder is requested to submit to the OPR a

classification recommendation or challenge. The holder of the information must protect the information in question at the possible highest classification level that they have recommended until a resolution is reached.

9.0 DERIVATIVE CLASSIFICATION

Derivative classification occurs when an individual incorporates, paraphrases, restates, or generates originally classified information from another document or security classification guide in a new form. When information is derivatively classified, individuals must use diligence in identifying and documenting the exact original classification and declassification of that information. Information that derives its classification from this SCG or other classified documents will be marked in accordance with DoD 5200.1-R, "Information Security Program".

10.0 DECLASSIFYING INFORMATION

Pursuant to E. O. 12958 as amended, Section 3.1, classified information shall be declassified when it no longer meets the standards for classification as specified in Section 1.1 and 1.4 of the E. O. At the time of original classification, an OCA shall attempt to establish the duration of classification based on a specific date or event.

10.1 DURATION OF CLASSIFICATION

The following declassification instructions will be applied when establishing the duration of classification:

A date or event less than 10 years from date of original classification; or
A date 10 years from the date of original classification; or
A date greater than 10 years but less than 25 years from the date of original classification; or
A date 25 years from the date of the original classification.

Classified information should be reviewed at least 6 months prior to declassification date or event to determine if classification of information should be extended. Otherwise, information will be automatically declassified upon reaching declassification date or event without notification to the Program office or affected organizations. Pursuant to E. O. 12958 as amended, Section 1.5(c), the OCA is the only authority that can extend classification.

10.2 DECLASSIFICATION METHODS

10.2.1 Automatic Declassification

In accordance with E.O. 12958, as amended, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under Title 44, U. S. Code, shall be automatically declassified on December 31, 2006, whether or not the records have been reviewed unless a request to extend classification beyond automatic declassification date has been submitted. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification.

At the time of original classification, the OCA may request an exemption from automatic declassification information which could reasonably be expected to cause damage to national security. All SCGs containing automatic declassification exemption categories that extend classification of any elements of information beyond 25 years must receive final approval from the Interagency Security Classification Appeals Panel (ISCAP). Provided below are exemption categories:

25X1 -- Reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

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

25X3 -- Reveal information that would impair U.S. cryptologic systems or activities;

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

25X5 -- Reveal actual U.S. military war plans that remain in effect;

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

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

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

25X9 -- Violate a statute, treaty, or international agreement.

10.2.2 Mandatory Declassification Review

This method of declassification occurs when a review of classified information is accomplished in response to a request for declassification of the information.

10.2.3 Systematic Declassification Review

This method involves the establishment of a program to conduct a systematic review of classified information contained in records that have been determined to have permanent historical value for declassification IAW Title 44, USC. This also applies to information exempt from automatic declassification and information contained in permanently historical valuable records that are less than 25 years.

11.0 RELEASE OF INFORMATION

The fact that this SCG shows certain details of information to be unclassified does not allow automatic public release of the information. DoD 5400.7-R, "DoD Freedom of Information Act Program" authorizes the withholding of certain information from public release based on applicable FOIA exemptions.

11.1 Public Release of Information

Unclassified GBS Program information must be submitted to and approved by the GBS Joint Program Office and the Public Affairs office prior to release. Classified GBS Program information is not releasable at any time. Once classified information is declassified, it must be submitted and approved by the GBS Joint Program Office and the MCSW Public Affairs. Refer to AFI 35-101, "Public Affairs."

"Policies and Procedures" for submittal and approval process: The term "information" includes, but is not limited to, news articles, contract announcements, advertisements, brochures, photographs, motion picture films, scripts, technical papers, speeches, displays, briefings, etc., on any aspect of the GBS Program. Public release includes meetings, symposiums, seminars, conferences, internet, etc.

11.2 Release of Program Data on World Wide Web (WWW)

The release of GBS Program information on the World Wide Web is also considered public release. Consequently, extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. GBS Program information intended for publication on publicly accessible or unprotected web sites must be approved by the GBS Joint Program Office and the MCSW Public Affairs Office prior to placing on the World Wide Web. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. If there are any doubts, do not release the information. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate.

11.3 Foreign Disclosure - Release of Classified and Unclassified Info to Foreign Government or Their Representatives

In accordance with National Disclosure Policy (NDP-1), National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations; AFI 16-201, Air Force Foreign Disclosure and Technology Transfer Program; and DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, request for and release of GBS Program unclassified, classified and unclassified controlled information to a foreign government, their representative or international organization must be submitted to and approved by Foreign Disclosure Office (FDO), SMC/PIP. This also includes releasing or distributing information at meetings (i.e. symposiums, seminars, conferences, etc.) where attendance by foreign nationals is

anticipated or expected. One final copy of the material proposed for disclosure/release must be submitted to FDO, SMC/PIP a minimum of 30 days prior to the proposed disclosure/release date.

12.0 REPRODUCTION AND DISSEMINATION

Local reproduction of this SCG is authorized only in its entirety for use by activities involved or associated with the GBS Program.

Distribution A applies to this SCG and dissemination is approved for public release; distribution unlimited.

13.0 PROGRAM PROTECTION PLAN (PPP)

The GBS Program does not require a PPP because the system does not contain critical technology.

13.1 Critical Program Information (CPI)

Critical Program Information or CPI, is defined as that "key" information about the program, technologies, and/or systems that if compromised would degrade combat effectiveness or shorten the expected life of the system. CPI may also provide insight into program vulnerabilities, countermeasures, and limitations. Unauthorized access to this information or systems could allow someone to kill, counter, clone, negate, or degrade the system before or near the scheduled deployment, forcing a major design change to maintain the same level of effectiveness and capability. CPI may be classified or unclassified information. Given the potentially grave consequences that can result from the compromise of CPI, everyone who uses this sensitive information must ensure it is adequately identified and protected.

Section II of this SCG, the Classification Matrix Tables, detail guidance for the protection of GBS information. Any further questions regarding CPI and its handling should be referred to the GBS Program Security Office.

14.0 SPECIAL ACCESS PROGRAMS (SAPs)

The GBS Program is Unclassified and does not require Special Access.

15.0 CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Controlled unclassified information is unclassified information that requires applications of controls and protective measures to prevent damage to national security. This type of information on the GBS Program includes For Official Use Only (FOUO) and Sensitive Information (SI) as defined in the Computer Security Act of 1987. Refer to DoD 5200.1-R, Information Security Program, Appendix 3, Controlled Unclassified Information for policy guidance regarding CUI. In general, the SBM's only ingest content information and broadcast that information to the receive suites. The receive suite end users, when opening the information shall handle the unclassified information as annotated (i.e. if it is marked FOUO, follow that guidance and if it is marked Sensitive Information, follow that guidance).

15.1 For Official Use Only (FOUO)

FOUO is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act. For policy guidance refer to DoD 5400.7-R, DoD Freedom of Information Act (FOIA) Program.

15.2 Sensitive Information (SI) (Computer Security Act of 1987)

The Computer Security Act of 1987 (reference (j)), established requirements for protection of certain information in Federal Government automated information system (AIS). This information is referred to as "sensitive information", defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act) (reference (h)), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

16.0 CLASSIFICATION MATRIX AND GUIDANCE

The classification matrix tables provide specific details regarding the GBS Program information to aid users in assigning or determining the classification and protection level of GBS information.

The classification matrix tables in Section II contain the following information: Identification of GBS program information (topic/information revealing), classification level, the reason for classifying the information, the source of original classification if other than the GBS Program SCG; declassification instructions and explanatory remarks, if applicable. Also provided is the classified information original classification date to assist with determining the declassification date based on the 25 year declassification policy.

16.1 Elements of Classification Matrix

Provided is a brief description of the information contained in the Classification Matrix Tables.

Topic/Information Revealing - Identifies and lists GBS Program information that requires protection in the interest of national security. This information protection or classification level can range from FOUO to Top Secret. Whenever possible, information which would require different or ranges of classification or protection levels has not been included in one topic. However, where unavoidable, the "Remarks" column provides additional information in order to distinguish the Classification Level.

Class. Level (Classification Level) - Identifies the classification or protection level of the information listed. Classification levels that apply to the GBS Program are designated with a TS for TOP SECRET, S for SECRET, Secret ROKUS (Republic of Korea United States) for S-ROKUS, C for CONFIDENTIAL, and U for UNCLASSIFIED. Additional protection level designators include CRYPTO, CUI and FOUO (For Official Use Only). Whenever possible, ranges of classification/protection levels (example: FOUO - S) have not been used. If

unavoidable and a range is used, an explanation has been provided in the "Remarks" column delineating the information and the applicable classification or protection level.

Reason for Class. (Reason for Classification) - E. O. 12958 as amended, Sec 1.4, identifies the reason why information is classified. **In all cases for GBS, the only reason that applies is Sec 1.4 (g) and is annotated in the tables.**

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

Orig. Class. Date/Source (Original Classification Date/Source) - This information is required in order to assist with the declassification process in conjunction with E. O. 12958 as amended. The Order states that all classified information shall be declassified as soon as it no longer meets the standards for classification or that classified information should be declassified 25 years from the date of original classification unless exempted. In order to make this determination, the original classification date is needed.

Declassify On - Consistent with declassification policy, the information in this column is required to identify the date or event upon which classified information relevant to the line item will automatically become declassified. This column may also contain an applicable exemption from automatic declassification category. If an exemption from automatic declassification category is not used, information should be reviewed at least 6 months prior to declassification date or event in order to determine if an extension of classification is required.

Remarks - Provide any remarks that will assist the user in understanding classification information and provide justification for OCA determinations.

Derive Class. From (SCG Name) - If the line item listed attained its classification from another SCG or source, this column should be used to identify the source from which the information obtained its original classification. GBS did not use other SCGs to make any classifications.

16.2 Original Classification Determinations Identification

New information requiring classification determination or re-grading of information (downgrading, declassifying, etc) identified in the SCG Classification Matrix Table requires OCA determination and approval. In order for the OCA to be aware that he is making an OCA decision, this information is highlighted with an explanation provided in the "Remarks" column.

16.2.1 Marking and Handling

Classification designations, time limits, derivative marking procedures, and other requirements of the Controlled Access Program Coordination Office (CAPO) guidance will be applied to information classified pursuant to this guide in accordance with DoD 5200.1-R, Information Security Program, and the DoD 5220.22-M, National Industrial Security Program Operating Manual.

SECTION II - CLASSIFICATION MATRIX TABLES

For this section, the terms Transmit Sites or Transmit Suites include Satellite Broadcast Managers (SBM's) and Transportable SBM's (TSBM's).

1.0 General Information

To facilitate development and fielding of the GBS and connection of its users, basic program protection information has been widely disseminated. Therefore, an effort should be made to keep general descriptions of the program free of sensitive material, so that the descriptions can be publicly released as explained in Section I, paragraph 11.0.

Table 1. General Information

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
1.1 Descriptions of the GBS Program Basic information: mission, architecture, and implementation plan.	U					

2.0 Information about Providers and Subscribers

This category includes information about GBS users, including both sources and subscribers that are stored in the SBM/TSBM). Representative information in this category is organizational identification, geographical location, transmit capabilities, and the type of information handled.

GBS is a transport system that broadcasts US Secret, Secret ROKUS (S-ROKUS) (from Wahiawa only) and Unclassified (including CUI) information from Transmit Sites (contained in the Transmit Suite Client (TSC)) to Receive Suites around the world and as such, both the Transmit Sites and Receive Suites are continually updated with current Secret and Unclassified information. Therefore, the information about the Sources and Subscribers stored in the TSC data base of the SBM Transmit Sites that is Secret will remain Secret until the time they are removed from service.

Table 2. Information about Sources and Subscribers

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
2.1 Information Stored in an Operational Equipment Component of the GBS Information about sources and subscribers that is handled by components of the Broadcast Management Segment and Ground Terminal Segment. Includes user profiles established to manage smart push and other functions.	S	1.4 (g)	19980901/ SPG Annex C of 24 July 1998	25X8, End of Service Life for each Transmit Site	Data/Information in the Secret TSC data base is considered Secret. Data/Information in the Unclassified TSC data base is Unclassified. There is no external access to the Unclassified TSC data base.	
2.2 Source affiliation with GBS shall be handled according to the source's Security Classification Guide (Direct commercial sources into GBS are unclassified (e.g. CNN, ESPN).	TS through U	1.4 (g)	19980901	25X8, End of Service Life for each Transmit Site	Information shall be classified according to the source's SCG.	

3.0 User Broadcast Information and Related Control Information

This category includes information that the GBS broadcasts to end users and information used by the GBS to control the broadcasts.

As in Paragraph 2.0, GBS is a transport system that broadcasts US Secret, Secret ROKUS (from Wahiawa only) and Unclassified (including CUI) information from the three Transmit Sites to Receive Suites around the world and as such, both the Transmit Sites and Receive Suites are continually updated with current Secret and Unclassified information. Therefore, the Transmit Sites and Receive Suites that process Secret information will remain Secret until the time they are removed from service.

Table 3. User Broadcast Information and Related Control Information

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
3.1 User Broadcast Information That Is Received from an Outside Source Limited to security levels at which GBS equipment components operate.	S, S-ROKUS or CUI (FOUO or SI)	1.4 (g)	19980901 for Transmit Sites. At time of fielding and processing information for the Secret Receive Suites./SPG Annex C of 24 July 1998	25X8, End of Service Life for Transmit Sites and as Receive Suites is removed from service.	Cannot be classified higher than operating level of component; GBS components operate either at the Secret Level or at the Unclassified Level. Privacy Act Information is considered to be sensitive information per Section I, para 15.2. The RBM end user shall handle all CUI content delivered by GBS IAW the content marking and established procedures.	
3.2 User Broadcast Information That Is System Information The GBS Program Guide The GBS Tuning Plan	 S or U U	1.4 (g)	19980901 for Transmit Sites. At time of fielding and processing information for the Secret Receive Suites/SPG Annex C of 24 July 1998	25X8, End of Service Life for Transmit Sites and as Receive Suites is removed from service.	The Program Guide for the Secret Broadcast is Secret. The Program Guide and Tuning Plan for the Unclassified Broadcast is Unclassified.	

4.0 Traffic and Performance Data

GBS components and their users generate or collect information about GBS operations and analyze it for purposes of performance management. Protection required for traffic and performance data depends on whether or not it was created or collected in a GBS component that operates at a classified level. Some GBS components operate at a classified level because they handle classified user information. Other components handle only unclassified user information or handle user information that GBS has already encrypted for transmission.

Table 4. Traffic and Performance Data

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From

4.1 Traffic Analysis Data from an RBM or any SBM GBS Component Operating at any Classification level (all SBM/TSBM traffic data/RBM traffic data)	S	1.4 (g)	19980901 for Transmit Sites. At time of fielding and processing information for the Secret Receive Suites/ SPG Annex C of 24 July 1998.	25X8, End of Service Life for Transmit Sites and as Receive Suites are removed from service		
4.2 Past Information Throughput Data from any GBS RBM or any SBM Component Operating at any Classification level (Information Throughput Data only).	U				Past Information Throughput Data is considered to be the number of Bytes of Information broadcast during a time period.	
4.3 Traffic and Information Throughput Data from a GBS Component at Classified or Unclassified						
4.3.1 Reveals performance in a threat environment.	S	1.4 (g)	At time of the identification of the threat.	25X8, After the threat has been eliminated or at the end of the service life.		

5.0 Encryption Information

This category includes encryption devices and their descriptions, doctrine, procedures, support equipment, and key material. This table does not state original classifications for this category of information, except for special items for which guidance is needed in the GBS context. Most of the items in this category are protected in accordance with the following:

- NTISSI 4001, *Controlled Cryptographic Items*, 25 March 1985.
- NSTISSI 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials*, August 1997.

- NSA/CSSM 123-2, *Classification Guidance for COMSEC Devices*

Table 5. Encryption Information

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
5.1 Type I Encryption/Decryption Equipment in SBMs and RBMs shall only be under US control.	S or S-ROKUS	1.4 (g)	When the Equipment contains the Secret Keys	25X8, When the key is removed from the Equipment, it becomes CCI.	Consult NTISSI 4001 and NSTISSI 4005 on how to handle and ship Controlled Cryptographic Items.	NSA/CSSM 123-2
5.2 Type II Advanced Encryption Standard (AES) for unclassified broadcast.	CUI (FOUO or SI)				Type II Encryption device protects CUI information broadcast to users. The RBM end user shall handle all CUI content delivered by GBS IAW the content marking and established procedures.	

6.0 Access Control Information

This category contains information about controlling access to GBS resources. It includes information used to authenticate users and operators, and related functions and procedures.

Table 6. Access Control Information

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
6.1 Access Control Data. Passwords, procedural detail, telephone numbers, and network addresses.	CUI					
6.1.1 Passwords for GBS components that operate at S or S-ROKUS.	S	1.4 (g)	When the password is created.	See Remarks.	Classify at same level as resource that the password protects. Declassify as appropriate to password creation and usage.	
6.1.2 Procedures for GBS components that operate at a classified level.	U				Consider on case-by-case basis unless classified by other areas of Section II.	
6.1.3 Passwords and procedures for GBS components that operate at unclassified level.	CUI				See Section I, paragraph 15.0.	
6.1.4 Network addresses for accessing any GBS component.	U					
6.2 Access Control Technology Descriptions of GBS access control mechanisms, algorithms, and protocols.	U					

7.0 Vulnerability Information

This category contains information about GBS vulnerabilities that might be exploited to (1) gain unauthorized access to GBS services or capabilities, (2) gain unauthorized access to sensitive or classified information, or (3) cause denial of service.

Table 7. Vulnerability Information

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
7.1 Vulnerability Acknowledgment A statement that the GBS or one of its elements has a vulnerability, without identifying or describing the weakness.	U				This does not apply to encryption elements. See Section II, paragraph 5.0 regarding encryption information.	
7.2 Unauthorized Access to Resource Any description of how to gain unauthorized access to a GBS resource.	S	1.4 (g)		25X8 - End of Service Life for Transmit Sites and as Receive Suites are removed from service	Also See Section II, paragraph 6.0 regarding access controls.	

7.3. Unauthorized Access to Classified Information: Description of how to gain access to classified information by someone not cleared to the security level of the data.	S	1.4 (g)		25X8 - End of Service Life for Transmit Sites and as Receive Suites are removed from service	When corrected or the equipment is removed from service.	
7.4 Unauthorized Access to CUI Any identification or description of how to gain unauthorized access to any material that is CUI.	CUI (FOUO)				See Section I, paragraph 15.0.	
7.5 Denial of Service Vulnerabilities: Denial of service is the prevention of authorized access to GBS resources or the delaying of time-critical GBS operations.						
7.5.1 Major denial of service. Any description of how to deny service to many users.	TS thru S	1.4(g)	When the condition has been identified.	25X8 - End of Service Life for Transmit Sites and as Receive Suites are removed from service	This applies to Transmit Sites, which could cause denial of service to all Receive Suites in the SBM/TSBM footprint. The identifier of the condition should classify the condition using their best judgment, but until finalized, initial protection is Top Secret security classification.	
7.5.2 Other denial of service. Any description of how to cause an unauthorized denial of service other than a major one.	S thru CUI FOUO	1.4 (g)	When the condition has been identified.	25X8 - End of Service Life for Transmit Sites and as Receive Suites are removed from service	This applies to Receive Suites, which may cause one or several outages but does not take the entire system down. The identifier of the condition should classify the condition using their best judgment, but until finalized, initial protection is Secret.	

8.0 Equipment Information

This category includes information about hardware, firmware, software, and associated documentation that is owned, leased, or operated by or for the benefit of the GBS Program. The GBS Program utilizes COTS equipment and thus specifications, implementation, maintenance, training and operations are unclassified. Encryption equipment information receives special protection, as specified in Section 5.0, Table 5.

Table 8. Equipment Information

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
8.1 Equipment Vulnerability Assessment	FOUO				See Section II, paragraph 7.0, Table 7.	
8.2 Equipment Testing: This category includes test objectives, test plans, test criteria, test procedures, test results, and test analyses for any kind of GBS test, including acceptance tests, operational tests, stress tests, survivability tests, performance tests, and security tests.						
8.2.1 Security-related testing. Information about tests of security-related system functions and equipment features and their test performance.	S thru CUI (FOUO)	1.4 (g)	To be determined by the test organization	25X8	The test organization that performed the test will classify the information based on test results identifying a system or segment vulnerability and the ability to exploit that vulnerability.	
8.2.2 Other testing.	U					

9.0 Operational Considerations/Limitations

This category includes information about Authorized Service Interruptions, and unscheduled outages caused by failures in the hardware/software.

Table 9. Operational Considerations/Limitations

Topic/Information Revealing	Class Level	Reason for Class	Orig. Class Date/Source	Declassify On	Remarks	Derive Class From
9.1 Authorized Service Interruption (ASI) to perform maintenance, install software, etc.	S	1.4 (g)	At the time the ASI is established.	25X8, After the ASI has been performed.	An ASI shall be protected to ensure that an adversary does not have time to plan for an outage.	
9.2 Notification that an SBM is not currently broadcasting information (an unplanned outage).						
9.2.1 Initial Notification to the JPO/Prime Contractor	FOUO					
9.2.2 Subsequent discussions/communications to resolve the outage.	C	1.4 (g)	After the outage has been identified.	25X8, After the outage has been restored.	Discussions/communications shall be performed using secure channels (STU 3 or SIPRNET or other communications channels).	
9.2.3 Discussion of the projected outage time.	S	1.4 (g)	After the outage has been identified.	25X8, After the outage has been restored.	Discussion about projected outage times may allow for an adversary to plan for an event.	
9.3 Telemetry Information						
9.3.1 Telemetry Information extracted from the EHF Terminal	S	1.4 (g)	19980901 AEHF	25X8, End of Service		

			SCG, 02 Jun 2003	Life for SBMs		
9.3.2 Beam Movement has been accomplished	U					

SECTION III - DECLASSIFICATION INDEX

Provided below is an index/history of the GBS Program and the information that has been declassified. Entries are made into the index after this SCG has been approved by the OCA. This is the initial GBS SCG and there are no entries at this time.

	TOPIC/INFORMATION REVEALING	CLASS.	REASON FOR CLASS.	ORIG. CLASS. DATE/	DECLASS. DATE	REMARKS
1						
2						
3						

SECTION IV – ACRONYMS

AF	AIR FORCE
AFI	AIR FORCE INSTRUCTION
AFPD	AIR FORCE POLICY DIRECTIVE
AFPEO/SP	AIR FORCE PROGRAM EXECUTIVE OFFICER FOR SPACE
AIS	AUTOMATED INFORMATION SYSTEMS
ASM	ACQUISITION SECURITY MANAGER
B/W	BANDWIDTH
C	CONFIDENTIAL
CCI	CONTROLLED CRYPOTOGRAPHIC ITEM
CM	COUNTERMEASURE
CNR	CHANGE NOTICE REGISTER
COMSEC	COMMUNICATIONS SECURITY
CPI	CRITICAL PROGRAM INFORMATION, TECHNOLOGIES AND SYSTEMS
CRYPTO	CRYPTOGRAPHIC DEVICE
CSR	CRITICAL SYSTEM RESOURCE
CUI	CONTROLLED UNCLASSIFIED INFORMATION
DAG	DEFENSE ACQUISITION GUIDEBOOK
DoD	DEPARTMENT OF DEFENSE
E.O.	EXECUTIVE ORDER
FDO	FOREIGN DISCLOSURE OFFICE
FOIA	FREEDOM OF INFORMATION ACT
FOUO	FOR OFFICIAL USE ONLY
GBS	GLOBAL BROADCAST SERVICE
INFOSEC	INFORMATION SECURITY
ISCAP	INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL
MCSW	MILSATCOM SYSTEMS WING
MJPO	MILSATCOM JOINT PROGRAM OFFICE
MTCR	MISSILE TECHNOLOGY CONTROL REGIME
NDP	NATIONAL DISCLOSURE POLICY
NISPOM	NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL
NSA	NATIONAL SECURITY AGENCY
NSS	NATIONAL SECURITY SPACE
NSSAP	NATIONAL SECURITY SPACE ACQUISITION POLICY
OADR	ORIGINATING AGENCY DETERMINATION REQUIRED
OCA	ORIGINAL CLASSIFICATION AUTHORITY
OPR	OFFICE OF PRIMARY RESPONSIBILITY
OPSEC	OPERATIONS SECURITY
ORD	OPERATIONAL REQUIREMENT DOCUMENTS
PM	PROGRAM MANAGER
PPP	PROGRAM PROTECTION PLAN
RBM	RECEIVE BROADCAST MANAGER
RD	RESTRICTED DATA
ROKUS	REPUBLIC OF KOREA UNITED STATES (INFORMATION)
S	SECRET
SAP	SPECIAL ACCESS PROGRAM
SBM	SATELLITE BROADCAST MANAGER

SBU	SENSITIVE BUT UNCLASSIFIED
SCG	SECURITY CLASSIFICATION/DECLASSIFICATION GUIDE
SPG	SYSTEM PROTECTION GUIDE
TS	TOP SECRET
U	UNCLASSIFIED
UCNI	UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
U.S.	UNITED STATES
USC	UNITED STATES CODE
USAF	UNITED STATES AIR FORCE
WMD	WEAPONS OF MASS DESTRUCTION
WWW	WORLD WIDE WEB

SECTION V – DEFINITIONS

Analytical Models: The assemblage of mathematical equations and geometric representations, which reflect physical phenomena or processes and which when solved in a particular order will predict various characteristics of the system or subsystem. Usually, the physical processes involved may have been the subjects of previous research, and analytical models of varying degrees of applicability may have been reported in open literature.

Architecture: A description of all system functional activities to be performed to achieve the desired level of defense, the system components needed to perform the functions, and the allocation of performance levels among those system components.

Authorized Holder/Person: A person who has a need-to-know for classified information in the performance of official duties, and who has been granted clearance for the required level.

Availability: A measure of the degree to which an item is operable and committable at the start of a mission, when the mission is called for at an unknown (random) time.

Basic Research: Research in the physical sciences, except research which meets the definition of Restricted Data under the Atomic Energy Act, which does not imply or state how the results could be used to enhance weaponry. The information is known or within the state-of-the-art of other nations and does not represent a potential or actual scientific breakthrough with national security implications.

Breakthrough: Occurs when a technology development is imminent or is achieved, which constitutes a marked or sudden deviation from a trend or shows unexpected progress in relation to time, and is not predictable qualitatively; or when an increase in performance or capability appears to open a field of application to new military system uses.

Capability: In general, it describes what part of the missions a system can meet against an adversary's attack. In particular, it is a collection of performance indices (e.g. defended area, launch area denied, probability of engagement success, raid size capacity) against an attack with specific features.

Category of Countermeasures (CM): Types of countermeasure approaches within a class of CMs. For example, jammers, flares, chaff, and clouds are categories within the masker's class of CMs.

Class of Countermeasures: A top level grouping of countermeasures by the type of effect they attempt to have on defensive systems. Generally accepted classes of countermeasures are simulation, anti-simulation, maskers, traffic, signature reduction, aim point denial, and tactics.

Classification by Compilation: Compilations of information that individually are unclassified but may be classified if combined.

Classified Defense Information: Official information which requires protection against unauthorized disclosure in the interests of national security of the United States, and which has

been so designated in accordance with the provisions of Executive Order 12958 as amended as Confidential, Secret and Top Secret.

Classifier: An individual who makes classification determinations and applies a security classification to information. A classifier may be an original classification authority or someone who derivatively classifies information based on properly classified source information or security classification guides.

Communications Intelligence: Technical and intelligence information derived from the intercept of communications by other than the intended recipients.

Communications Security (COMSEC): The protection resulting from any measures taken to deny unauthorized persons information of value that might be derived from telecommunications. Measures taken to ensure the authenticity of such telecommunications.

Component: Hardware and software with NSS functionality.

CONFIDENTIAL (C): Information that 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.

Compromise: An unauthorized disclosure of classified information.

Controlled Unclassified Information (CUI): Applies to unclassified information to which access or distribution limitations are applied. It includes program-related or other information marked, or that is eligible for marking, as "For Official Use Only" (FOUO) in accordance with (IAW) DoD 5400.7; technical information as defined in DoD 5230.24 and 5230.25; information that is subject to export controls in accordance with the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulation (EAR); sensitive information as defined in the Computer Security Act of 1987; or other qualifying information as identified in DoD 5200.1-R, Appendix C.

Cooperative Programs: Any program conducted concurrently at the same location or uses the same range assets, targets, or data. A cooperative program scenario implies a classification review of each participating program. Cooperative programs can also include international cooperative programs between the U.S. and Allies. International cooperative programs require additional security procedures.

Counter-Countermeasure: Measure taken by the defense to defeat offensive countermeasures. Includes techniques, tactics, procedures, algorithms, technologies, hardware, and software applied to counter offensive countermeasures.

Countermeasure: The employment of devices and/or techniques by an adversary, which have the objective of impairing the operational effectiveness of the system, or elements or components thereof.

Critical Program Information: Critical program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter the program direction. This includes classified military information or unclassified controlled information about such programs, technologies or systems.

Declassification: The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

Declassification Event: An event that eliminates the need for the continued classification of specific information.

Derivative Classification: A determination that specific information is the same as information currently classified in source material or as directed by a classification guide. The application of the classified markings to information confirmed to be already classified.

Derivative Classifier: A person who uses classified information or classification guidance as the basis to classify information.

Description: Include designs, performance, plans, methods, and technologies.

Design: Includes parameters and characteristics such as shape dimensions, mass and mass properties, wavebands (to include observed and emitted), schematics, photographs, and other graphical depictions.

Development: The life cycle of a technical effort from conceptualization, design, and test, up to but not including procurement. Applies to digital, physical, and descriptive instantiations.

Element: A collection of components that may independently execute NSS system tasks.

Feasibility: A measure used to describe the difficulty of implementing a part or function of a system.

Feature: An aspect of an object used to describe that object or to distinguish the type of that object from other objects. Example features are length, radar cross-section, tumble rate.

Foreign Disclosure: The transfer of classified military information through approved channels to an authorized representative of a foreign government or international organization.

FOR OFFICIAL USE ONLY: A protective status and marking for information that has not been given a defense security classification, but which may be withheld from public disclosure under criteria specified in the Freedom of Information Act, Title 5, USC, Section 552. DoD guidance is specified in DoD Directive 5400.7-R, DoD Freedom Of Information Act Program, and DoD Directive 5200.1-R, Information Security Program, Appendix C.

Formerly Restricted Data: Information removed from the Restricted Data (RD) category upon a joint determination by the Department of Energy (DOE) (or antecedent Agencies) and the Department of Defense (DoD) that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination this information is treated in the same manner as Restricted Data (RD). See Restricted Data (RD).

Global Broadcast Service: The Global Broadcast Service (GBS) description is provided in the Forward of this SCG.

Hardness: Level to which a component, subsystem, or system is able to withstand a given space environment without the use of external operational constraints or procedures.

Information: Any knowledge that may be communicated, or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of, the Department of Defense.

Information Security (NISPOM): The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

Information Security (DoD 5200.1-R): The system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information Security (Joint Pub 1-02): Information security is the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC.

Likelihood: (1) A ratio of the probability for one thing to the probability of the collection of things to which it belongs. (2) The probability that a countermeasure will be employed against the defense system being assessed. Includes such factors as technical feasibility and adversary preference. (3) How much more probable it is that an observed signature belongs to one class of objects than to another.

Life-Cycle Cost: The total cost to the Government of acquisition and ownership of that NSS system over its useful life. It includes the cost of development, acquisition, support, testing, sustainment and where applicable, disposal.

Limitation: An inability to achieve a required or desired level of performance or standard.

Limiting Factor: A factor or condition that, either temporarily or permanently impedes mission accomplishment. Illustrative examples are transportation network deficiencies, lack of in-place

facilities, misplaced forces or materiel, extreme climatic conditions, distance, transit or over flight rights, political conditions, etc.

Maintainability: The ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill, and using prescribed procedures and resources, at each prescribed level of maintenance and repair.

Mission Reliability: The probability the system will perform mission essential functions for a period of time under the conditions stated in the mission profile.

Mitigation: Any feature, either physical or operational, that is specifically included in order to survive a threat.

National Security: The national defense or relations of the United States.
Need-to-Know: A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a User Agency.

Operational: Any software, hardware, or other program activity that has the same performance fidelity of the deployed system and would reveal performance parameters or vulnerabilities/limitations of the system it represents.

Operational Capability: The attainment by the system of the capability to perform its intended mission.

Operational Concept: Described purpose, employment, deployment and support of a specific system. It assists in identifying the quantitative and qualitative performance and support specifications needed to satisfy the operational need and provides initial guidance to operating forces for employing the new or improved system.

Operational Effectiveness: The overall degree of mission accomplishment of the system when used by representative personnel in the environment planned or expected (e.g., natural, electronic, threat, etc.) for operational employment of the system considering organization, doctrine, tactics, survivability, vulnerability, and threat.
Operational Suitability: The degree to which a system can be placed satisfactorily in field use with consideration given the availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, man power supportability, logistics supportability, natural environment effects and impacts, documentation, and training requirements.

Operations: The tactics, deployment plans, and operational effectiveness of a strategic defense system and the safety hazards associated with the use thereof.

Original Classification Authority: The authority delegated through the Secretary of Defense allowing a government official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

Parameter: Any of a set of physical properties whose values determine the characteristics or behavior of the system.

Performance: The operational and support characteristics of the system that allow it to effectively and efficiently perform its assigned mission over time. The support characteristics of the system include both supportability aspects of the design and the support elements necessary for system operations.

Performance Characteristics: The operational and support characteristics of the system that allow it to effectively and efficiently perform its assigned mission over time. The support characteristics of the system include both supportability aspects of the design and the support components necessary for the system operations.

Performance Data. Observations and measurements of broadcast and application throughput, delay, error rates, reliability, availability, and other aspects of GBS operation.

Program Baseline: This is a NSS System-level program management document, similar to APBs. It is a formal agreement between SAF/US, AFPEO/SP and PM that reflects a vision of where NSS system expects to be, in terms of cost, schedule, and capability. System-level performance objectives, schedule of key events/activities, and cost objectives tailored to a Capability-based Acquisition approach. It also provides the standard for regular measurement, assessment and reporting of NSS program progress against these stated objectives and goals, which represent ranges of values.

Public Disclosure: The passing of information and/or material to the public, or any member of the public, by any means of communication.

Receive Broadcast Manager: The hardware, software and firmware at the Receive Suite that allows the broadcast information available to the end user.

Reliability: The ability of a system and/or its components to perform its mission without failure, degradation, or demand of the support system.

Research and Development: Effort directed toward achieving advances in technology areas relevant to strategic defense.

Restricted Data: All data concerning the: design, manufacture or utilization of atomic weapons; Production of special nuclear material; or Use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data (RD) category under Section 142 of the Atomic Energy Act of 1954, as amended.

Satellite Broadcast Manager: The hardware, software and firmware at the Transmit Sites that is used to process the incoming information from data sources and broadcasts the information to receive suites. Technicians are also located at the SBM sites.

Significant Technical Advance: An advance of sufficient magnitude to have potential use on an operational or advanced system, which results in a definite military advantage.

SECRET: Information that 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.

Single Point Failure: Any single function, element, component, or node that when not fully operational will cause the system to be inoperable.

Source Document: A document, other than a classification guide, from which information is extracted for inclusion in another document. The classification of the information extracted is determined by the classification markings shown in/on the source document.

System Limits: The outer boundaries of system performance.

System Limitation: An actual performance limit in a system that fails to meet the defined mission requirement, required performance standard, or desired performance standard.

System Resource: Information service provided by the system; a system capability or item of system equipment, such as software, firmware, or hardware; or a facility that houses system operations and equipment.

Systems: Operational weapons, demonstration devices with weapon level parameters, studies of military applications, weapon performance, vulnerability, lethality, and countermeasures.

Survivability: The capability of a system to avoid or withstand man-made hostile environments without suffering abortive impairment of its ability to accomplish its designated mission.

Tactics: The strategy, procedure, maneuvers, or timing by which the system attains its objectives.

Technical Data: Information directly related to the design, engineering, development, production, processing, manufacture, use, operation, overhaul, repair, maintenance, and modification of information in the form of blueprints, drawings, photographs, plans, instructions, computer software and documentation regarding military or space equipment. This also includes information (technology), which advances the state-of-the-art of articles on the United States Munitions List. It does not include information concerning general scientific, mathematical or engineering principles.

Technology Baseline: Documents content of all approved technology efforts and reflects the expectation for the maturation of new capabilities to support NSS system development. It includes basic and advanced research, advanced development, risk reduction, critical experiments, and concept definition.

Technology Breakthrough: An R&D discovery with system application potential that shows unexpected and significant progress in relation to time, performance, capability, or cost savings

that constitutes a sudden deviation from a trend unpredictable by persons trained in the appropriate technical discipline.

TEMPEST: TEMPEST is the UNCLASSIFIED short name referring to investigation and study of compromising emanations.

Test Data: Empirical data obtained from ground or flight-testing of models or full-scale vehicles. A collection of data is known as a record, regardless of the physical form in which the data appears. The data records may be distinguished as three types: raw, processed, and analyzed. These types differ in the extent of the added commentary or annotations revealing the identity and significance of the record.

- Raw data: Data as recorded by a sensor, where no significant effort has been made to reduce, edit, select or interpret.

- Processed data: Raw data records plus commentary or annotations revealing the identity and significance of the record or as information computed from raw data and presented in a revealing and intelligent format.

- Analyzed data: Processed data accompanied by textual material which comments in detail on the significance of the information presented. Conclusions are drawn or implied, and the reader's attention is directed to peculiarities or characteristic phenomena.

TOP SECRET: Information that 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.

Traffic Data: Broadcast control information, protocol header information, and information about the length, frequency, and time of broadcast transmissions.

Vulnerability: A Definitive, Significant Reduction in capability of a NSS system architecture, element, or component to perform a designated mission when subjected to a defined level of adversary effects

- Definitive Reduction: Decrease in Performance based on information generated by analytical models.

- Significant Reduction: Decrease in performance to a level where it is unlikely the system, element, or component can perform its designated mission. It is generally accepted that values for mission performance metrics below 50% indicate a vulnerability.

- Defined level of Adversary Effects: Sufficient information to describe how an adversary causes a NSS system vulnerability. The minimum required information is key design parameters with the parameter values required to achieve levels of significant reductions in capability. NOTE: The term vulnerability only applies to NSS system, element, or component architectures under configuration management. It does not apply to advanced or alternate capabilities that are not yet part of the NSS Program baseline.

SECTION VI – REFERENCES

APPLICABLE POLICY DOCUMENTS AND REFERENCES

AFI 31-401, Information Security Program Management, 1 November 2005

Defense Acquisition Guide (DAG)

Executive Order 12958, Classified National Security Information, as amended by E. O. 13292, dated 25 March 2003

National Security Agency Document NSA/CSSM 123-2, Classification Guidance for COMSEC Devices

NSTISSI 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997

NTISSI 4001, Controlled Cryptographic Items, 25 March 1985

Title 5, United States Code, Section 552, "Freedom of Information Act, (1994) as amended

United Nations Command/ROK-US Combined Forces Command Regulation 380-1, dated 1 April 1998

SECTION VII - DISTRIBUTION LIST

Office of the Assistant Secretary of
Defense (Public Affairs)
Director of Freedom of Information
And Security Review
Pentagon Rm 2C757
Washington DC 20301

NGA, Office of Security
2600 Sangamere Rd
Bethesda MD 20816

OASD/NII
Pentagon, Rm 3D174
Washington DC 20301

Director, Program Analysis and Evaluation
Pentagon, Rm 3E836
Washington DC 20301

Administrator
Defense Technical Information Center (DTIC-OCP)
8725 Kingman Rd, Ste 944
Ft. Belvoir, VA 22304

Director, National Security Agency
Attn: V4
9800 Savage Rd
Ft. Meade MD 20755

Joint Staff (J6S)
Pentagon, Rm 1C826
Washington, DC 20318

Undersecretary of Defense for Intelligence (USD/I)
Pentagon, Rm 1E245
Washington DC 20301

DTIC-DE
Cameron Station
Alexandria, VA 22304

National Reconnaissance Office
Office of Security
14675 Lee Road
Chantilly VA 20150

SAF/AQX/AQL
1500 Wilson Blvd
Rosslyn VA 20305

Central Intelligence Agency
Office of Scientific & Weapons
Washington, DC 20505

US Strategic Command
Director of Security
901 SAC Blvd, Ste 1A1
Offutt AFB NE 68113

Aerospace Corporation
Attn: Facility Security Officer
P.O. Box 92957
El Segundo, CA 90245

Director of Industrial Security
HQ DSS (V0410)
1900 Half Street
Washington, DC 20324

US Army Space & Missile Command
P.O. Box 1500
Huntsville AL 35807

SMC/PIP/IN/PA/JA
Los Angeles AFB CA 90245

MCSW/MCI
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

SAF/USA/USI
1500 Wilson Blvd
Rosslyn VA 20305

HQ AFSPC/DR/XO/PA/IN
150 Vandenberg St, Ste 1105
Peterson AFB CO 80914

ESC/INP
Hanscom, AFB MA 20430

Naval Network Warfare Command
Building 1265, 2465 Guadalcanal Road
Norfolk, VA 23521-3228
Attn: N3312

SAF/PAS
1690 Air Force Pentagon
Washington, DC 20330

HQ AFDO/CC
1720 Air Force Pentagon
Washington DC 20330

HQ AFHRA/RSA
600 Chennault Circle
Maxwell AFB, AL 3

HQ USAF/XOSFI
1340 Air Force Pentagon
Washington, DC 20330

SECTION VIII – GBS Service Representatives

Terminals Program Office
Hanscom Air Force Base
Bedford, MA 01730
(981) 271-2311

Marine Corps Systems Command
Program Manager Communications Network Systems, GBS Project Office
2200 Lester St.
Quantico, VA 22134
(703) 432-4322

SPAWAR PEO C4I, PMW-170
San Diego, CA 92152
(619) 524-7619

PM WIN-T
Building 916
Fort Monmouth
Fort Monmouth, NJ 07703
(732) 532-5179