~~SECRET~~

USCSB 3-12
Copy 7

#18

NATIONAL POLICY ON THE SECURITY OF METEOROLOGICAL SATELLITE INFORMATION (S)

United States
Communications Security Board

Office of the Secretary of Defense
Chief, RDD, ESD, WHS
Date: 27 Jun 2016 Authority: EO 13526 5 U.S.C. 552
Declassify: X Deny in Full: _____
Declassify in Part: _____
Reason: _____
MDR: 13 -M- 4617

DECLASSIFIED
E.O. 13526, Sec. 3.3 (a)
NASA Declassification Guide
September 2009
Reviewer: 5197 Date: 2-12-16

~~Special Handling Required Not Releasable to Foreign Nationals~~

~~GROUP 1 Excluded from automatic downgrading and declassification~~

DECLASSIFIED IN FULL
Authority: EO 13526
Chief, Records & Declass Div, WHS
Date:
JUN 27 2016

~~SECRET~~

R6
13-M-4617

TAB B

USCSB
UNITED STATES
COMMUNICATIONS
SECURITY BOARD

15 April 1970

FOREWORD

On 15 April 1970, the United States Communications Security Board approved a revision to the National Policy on the Security of Meteorological Satellite Information(S), dated 25 March 1968. The revision provided system managers with increased flexibility in meeting the national objective by authorizing the option of selective control as an alternative to control through cryptographic measures. Also the scope of consultation required between the Secretary of Defense, the Secretary of Commerce, and the Administrator, National Aeronautics and Space Administration has been expanded to include operational as well as quasi-operational subsystems.

This policy is effective immediately and supersedes the National Policy on the Security of Meteorological Satellite Information(S), dated 25 March 1968.

Robert F. Froehlke
Chairman

~~SECRET—NOFORN~~

USCSB
UNITED STATES
COMMUNICATIONS
SECURITY BOARD

15 April 1970

NATIONAL POLICY

ON THE

SECURITY OF METEOROLOGICAL SATELLITE INFORMATION

Section I—Purpose and Scope

1. This document establishes the National Policy for meteorological satellite communications security to (a) prevent a hostile nation from gaining control of the satellites and (b) deny a hostile nation direct access to data transmitted from the satellites, when such actions are determined to be in the interest of national security. All operational, quasi-operational, and research and development (R&D) meteorological satellite systems are subject to the provisions of this policy. Furthermore, multipurpose satellite systems in any of the above categories which carry a meteorological sensor will be governed by this policy insofar as the meteorological mission is concerned. The applicability of this policy to other than meteorological sensors/missions aboard multipurpose spacecraft will be determined on a case-by-case basis. Meteorological satellite systems, as used in this policy, consist of the spacecraft, passive data acquisition stations, command and data acquisition (CDA) terminals and associated communications links including communications terminal equipment. A quasi-operational system is defined as one which has a demonstrated operational capability though the primary mission is R&D. This policy is binding on all Departments and Agencies of the Federal Government which develop, launch, and operate satellite systems to obtain meteorological data.

Section II—Background

2. Comprehensive and timely weather information is essential for the effective use of military power. A hostile nation can deny access to weather information from conventional sources within the territory it controls. The weather satellite provides a means to circumvent these controls and obtain useful data from otherwise silent or data sparse areas. In order to exploit this potential operational advantage, it is essential that the National Command Authority have the capability to (a) prevent a hostile nation from taking control of the system

and (b) selectively deny access to the meteorological data to any hostile nation without decreasing the usability of the data to U. S. or friendly forces. A requirement for this capability was stated by the JCS in 1961 and reiterated in 1964 and 1966. The potential operational advantage is presently mitigated by two factors: (a) The satellite command and control subsystems are not secure. A hostile nation can, with relative ease, assume control of U. S. weather satellites presently in operation. (b) Data from present weather satellites is transmitted in clear text. Specifications for ground receiver and processing equipment compatible with the National Operational Meteorological Satellite System (NOAMSS) are unclassified and readily available. Similar specifications pertinent to military systems can be deduced from an analysis of telemetry.

Section III—Objective

3. The objective of this policy is to assure that each Department or Agency of the Federal Government which develops, launches and operates meteorological satellite systems, takes action as a matter of urgency to insure that the National Command Authority is able to (a) maintain control of U. S. meteorological satellite systems in the face of a determined effort by a hostile nation to assume control and (b) control direct access to data transmitted from these systems when such action is considered to be in the interest of national security.

Section IV—Guidelines

4. The following guidelines shall be used in complying with the intent of this policy:

a. Provisions will be made to either encrypt both the command and data links of meteorological satellite systems or to positively silence the useful data.

b. When other means of exercising positive, selective control which provide a level of security equivalent to encryption are developed, these may be considered in lieu of encryption.

c. Options listed in 4*a* above apply as follows:

(1) Operational meteorological satellite systems, their component subsystems, meteorological subsystems on multipurpose satellites and military R&D meteorological satellite systems will be:

(a) Equipped with cryptographic devices, or NSA approved equivalent, and be designed to operate in clear text or under communications security control on command; or

(b) Designed so that useful data transmission from the satellite can be selectively silenced by secure means over designated geographic areas or at specific times.

The Secretary of Defense will determine the option to be used in each case.

(2) All non-military R&D meteorological satellite systems will:

(a) Comply with 4*c*(1)(a) above, or

(b) Comply with 4*c*(1)(b) above, or

(c) Be designed so that useful data transmission from the spacecraft can be positively silenced.

The Administrator, NASA, will determine the option to be used in each case.

(3) In general, the sponsoring agency may select either option for application to non-military, quasi-operational meteorological systems. However, the option for use with those subsystems which could augment operational systems (example: APT on Nimbus II) should be decided by the sponsoring agency on a case by case basis, in consultation with the Secretary of Defense.

d. Initial compliance may not be deferred solely on the basis that no acceptable alternative to encryption exists.

e. Spacecraft systems must be adequately shielded to prevent inadvertent transmission of data in clear text while the satellite is operating in the encrypted mode.

f. The recommendation to impose security procedures on meteorological satellites over specified areas will originate with the Joint Chiefs of Staff. Upon such a recommendation, the Secretary of Defense will obtain the concurrence of the Secretary of State to ensure that foreign policy implications are fully considered prior to requesting the Secretary of Commerce and the Administrator, NASA, to implement appropriate weather satellite communications security measures. Military systems will operate in the secure mode upon direction of the Secretary of Defense.

g. The National Meteorological Satellite Program of the U. S. has been specifically identified as an instrument of international cooperation for the benefit of all mankind. It is imperative, therefore, that the Policy outlined herein be conducted under security safeguards and in a manner which will provide reasonable assurance that the National Meteorological Satellite Program will continue to be so identified. Pending the development of the security plan pertaining to the Policy established herein and its application to the National Meteorological Satellite Program, all information pertaining to the Policy and its existence as it relates to non-military meteorological satellite systems will be classified SECRET – NOT RELEASABLE TO FOREIGN NATIONALS.

h. The explicit reference to military R&D meteorological satellite programs and implicit reference to operational military meteorological satellite programs in paragraph 4*c* (1) is classified SECRET.

i. Any technical information concerning the security techniques or equipment employed shall be classified SECRET – NOFORN; its release is governed by existing security regulations.

Section V—Responsibilities

5. Heads of all Departments and Agencies of the government involved in the development and operation of meteorological satellite systems are responsible for compliance with provisions of this policy at the earliest practicable date. Details of implementation schedules and procedures, operating procedures, and funding responsibilities will be negotiated among DOD, DOC and NASA. Specific Departmental and Agency responsibilities follow:

a. The Secretary of Defense is responsible for:

(1) Insuring that all military meteorological satellite systems are equipped with cryptographic or equivalent security devices or procedures at the earliest practicable date.

(2) Providing cryptographic or equivalent security devices or procedures to the Department of Commerce and NASA.

(3) Consulting with the Secretary of Commerce and the Administrator, NASA, to identify those operational and quasi-operational subsystems to which communications security procedures other than positive silencing should apply.

(4) Initiating discussions with the Secretary of Commerce and the Administrator, NASA on details of implementation, operation and funding.

(5) Consulting with the Secretary of Commerce, the Administrator, NASA, and the JCS to consider application of this policy to subsystems flown on multi-purpose spacecraft which are devoted to missions other than meteorology.

(6) Providing crypto-custodial support to non-military command and data acquisition terminals and associated communications terminal facilities to include installation, periodic check and maintenance, physical security and, during periods when communications security measures are in effect, operating assistance at these facilities.

(7) On the recommendation of the Joint Chiefs of Staff and with the concurrence of the Secretary of State, requesting that the Secretary of Commerce and Administrator, NASA, implement appropriate meteorological satellite communications security procedures.

(8) Developing jointly, in coordination with the Secretary of State, the Secretary of Commerce and the Administrator, NASA:

(a) An overall security plan pertaining to the Policy established herein and its application to the National Meteorological Satellite Program.

(b) A public information plan for handling (1) the impact of the sudden denial of satellite weather information to foreign nations, and (2) the premature disclosure of this Policy.

b. The Secretary of Commerce is responsible for:

(1) Notifying the Secretary of Defense of the numbers of communications security devices needed to equip the operational satellites, CDA terminals, and associated communications terminal facilities operated by the National Environmental Satellite Center of the Environmental Science Services Administration.

(2) Establishing in consultation with the Secretary of Defense, internal operating procedures to be followed during periods when communications security is imposed.

(3) Assisting the designated DOD agent in the installation of the communications security devices.

c. The Administrator, NASA, is responsible for:

(1) Advising the Secretary of Defense of those meteorological satellite systems and meteorological subsystems on multi-purpose satellites which are affected by this policy.

(2) In consultation with the Secretary of Defense, determining which subsystems on quasi-operational satellites should be equipped with communications security devices rather than a positive silencing device.

(3) Advising the Secretary of Defense of the numbers of communications security devices required to equip quasi-operational satellite and associated ground receiver and communications terminal facilities operated by NASA.

(4) Redesigning existing operational spacecraft system(s) to accommodate the communications security devices provided by the Department of Defense.

(5) Coordinating with the Director, NSA, on spacecraft power, weight, and space constraints and other system characteristics which may be pertinent to the development of suitable communications security devices.

(6) Coordinating with the designated DOD agent concerning integration of communications security devices in the satellite.

d. The Chairman of the Joint Chiefs of Staff is responsible for:

(1) Determining the military advantage to be gained by selective denial of weather satellite data.

(2) Recommending to the Secretary of Defense that communications security procedures provided for in this policy be imposed over specific regions and periods of time.

e. The Director of NSA is responsible for:

(1) Designing and developing communications security devices suitable for use with meteorological satellite systems—satellite components and ground receiving and communications terminal facilities.

(2) Evaluating the security of communications devices/procedures proposed for use in lieu of crypto devices in meteorological satellite systems.

(3) Providing necessary directives relative to installation, operation, and physical security of the communications security devices.

(4) Providing technical assistance to NASA and its contractors during the redesign of the operational meteorological satellite system(s) to integrate communication security devices.

NSA