

UNCLASSIFIED

DRAFT

Revision 10/9/87

National Security Decision
Directive Number _____

ATTACHMENT

2NATIONAL OPERATIONS SECURITY PROGRAMOBJECTIVE

Security programs and procedures already exist to protect classified matters. However, unclassified information generally available to the public as well as certain detectable activities exist that provide indications concerning classified or sensitive information or undertakings. Such indicators may be exploited by those seeking to neutralize or to take advantage of US Government actions that affect national security. Application of the Operations Security (OPSEC) process promotes operational effectiveness by guarding against the inadvertent compromise of sensitive or classified US Government activities, capabilities, or intentions.

BACKGROUND

The operations security process involves five steps: identification of critical information, analysis of the threat, analysis of the vulnerabilities, assessment of the risks, and application of appropriate countermeasures. It begins with an examination of the totality of an activity to determine what exploitable but essentially unclassified indicators could be acquired in light of the known collection capabilities of potential adversaries. Indicators usually evolve from openly available data and other detectable actions. Certain of these indicators may be pieced together or interpreted to

UNCLASSIFIED

discern critical information. Indicators most often stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once the indicators are identified, they are analyzed against the threat to determine the extent to which they could reveal critical information.

Commanders and managers then use these threat and vulnerability analyses in their risk assessment to assist in selecting and applying practical countermeasures to mitigate or nullify selected indicators. Indicators may be controlled or protected, as appropriate, using the full range of OPSEC measures. These OPSEC measures may include, but are not limited to: counterimagery; cover, concealment, and deception; and physical, information, personnel, signals, computer, communications, and electronic security.

OPSEC is, thus, a systematic and proved process by which the US Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified indicators associated with the planning and execution of sensitive government activities.

APPLICATION

Indicators and vulnerabilities are best identified before activities start through detailed OPSEC planning. They may also be identified during or after the conduct of routine functional activities by analyzing how functions are

actually performed and what procedures are used. Planning and analysis proceed from the adversaries' perspectives. To assist in OPSEC planning and analysis, OPSEC planning guidance must be developed jointly by those most familiar with the operational aspects of a particular activity together with their supporting intelligence elements.

OPSEC planning guidance should consider those critical aspects of an activity that should be protected in light of US and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence threats, as well as an outline of projected OPSEC measures.

In the OPSEC process, it is important to distinguish between the threat and vulnerability analysis phases and the phase in which OPSEC measures are applied. Recommendations on the use of OPSEC measures are based on the joint operational-intelligence analyses, but ultimate decisions on their implementation are made by commanders, supervisors, or program managers who determine what aspects will be protected. The decisionmaker with ultimate responsibility for mission accomplishment and resource management must have total authority for determining where and how OPSEC will be applied.

POLICY

A National Operations Security Program is hereby established. Each department and agency assigned or supporting national security missions with

classified or sensitive activities shall establish a formal OPSEC program with the following common features:

- o Specific assignment of responsibility for OPSEC direction and implementation.
- o Specific requirements to plan for and implement OPSEC in anticipation of, and where appropriate during, department or agency activity.
- o Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.
- o Institution of positive measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.
- o Instructions to conduct an internal annual OPSEC review that will outline the current OPSEC program of a department or agency and highlight successes or problem areas that may aid other OPSEC programs.
- o Provisions for support of and cooperation with other departments and agencies in their OPSEC programs.

UNCLASSIFIED

Agencies with minimal activities that could impact on national security need not establish a formal OPSEC program; however, they must cooperate with other departments and agencies to minimize damage to national security when OPSEC problems arise.

RESPONSIBILITIES

Heads of departments and agencies assigned or supporting national security missions. Establish organizational OPSEC programs; issue, as appropriate, OPSEC policies, procedures, and planning guidance; and designate departmental and agency planners for OPSEC. Advise the NSC on OPSEC measures required of other departments and agencies in order to achieve and maintain effectiveness in operations or activities. JCS should advise the NSC of the impact of nonmilitary US policies on the effectiveness of OPSEC measures taken by the US military and recommend to the NSC policies that would minimize any adverse effects.

Chairman, Senior Interagency Group for Intelligence (SIG-I)

The SIG-I is designated as the NSC's instrumentality for national OPSEC policy formulation, resolution of conflicting interagency OPSEC issues, guidance on national-level OPSEC training, technical OPSEC support, and advice to individual agencies. The National Operations Security Advisory Committee (NOAC), as part of the SIG-I structure and functioning under the aegis of the Interagency Group for Countermeasures (Policy), will:

- o Provide the SIG-I structure with advice and recommendations concerning measures and methods for reducing OPSEC vulnerabilities and propose corrective measures.
- o As requested, consult with and provide advice and recommendations to the various departments and agencies concerning OPSEC vulnerabilities and corrective measures.
- o On an ad hoc basis, chair forums for two or more agencies having competing interests or responsibilities with OPSEC implications that may affect national security interests. Analyze the issues and prepare advisory memorandums and recommendations for the competing agencies. In the event of an impasse, make appropriate recommendations to the SIG-I structure for resolution of the dispute.
- o Bring to the attention of the SIG-I those major unresolved OPSEC vulnerabilities and deficiencies that may arise within designated programs and activities of the executive branch.
- o Articulate to the SIG-I national-level requirements for intelligence and counterintelligence support to OPSEC.

Nothing in this Directive:

- o Is intended to impinge on the authorities and responsibilities of the DCI to protect intelligence sources and methods, nor those of any authorized agency or department to conduct intelligence-related activities.

- o Implies any authority on the part of the SIG-I, Interagency Group/Countermeasures (Policy), or the NOAC to examine the facilities or operations of any department or agency without the approval of the head of such department or agency.



THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

ATTACHMENT 3

13 NOV 1986

POLICY

MEMORANDUM FOR THE CHAIRMAN, NATIONAL OPERATIONS SECURITY ADVISORY COMMITTEE (NOAC)

SUBJECT: Civil Satellite Remote Sensing Programs

Under section 101 of the Land Remote-Sensing Commercialization Act of 1984, (Tab A), the Congress declared that, among other things, the national interest of the US lies in maintaining international leadership in civil remote sensing and in broadly promoting the beneficial use of remote-sensing data. The Congress declared, also, that land remote sensing by...private parties of the US affects...national security concerns of the US.

Section 402 of the Act prohibits any US person from operating any private remote-sensing system without a license (issued by the Secretary of Commerce).

Section 607 of the Act requires the Secretary of Commerce to consult with the Secretary of Defense on all matters under the Act affecting national security (including the issuance of the requisite license); and, the Secretary of Defense shall determine the conditions necessary to meet national security concerns.

The National Oceanic and Atmospheric Administration (NOAA), under the Department of Commerce, issued a Notice of Proposed Rulemaking (51 Fed. Reg. 9971, March 24, 1986) (Tab B) which, according to the Radio-Television News Directors Association (RTNDA), would violate the First Amendment. The thrust of RTNDA objections to the Notice is that the rules are unconstitutionally vague and would authorize NOAA to impose impermissible prior restraint. According to RTNDA, the question is not whether NOAA can take action to protect national security, but what standards must it use when doing so.


Given that commercial multispectral imaging resolution of other countries, such as France and Japan, is at least as good now as the US, and over the years along with US commercial satellites, will achieve even better resolution, the question becomes, "How does the US accommodate necessary and inevitable commercial growth in space and still protect US sensitive information?"

It seems to me that,

(1) The Department of Defense needs to develop and publish clear, defensible standards for the guidance of the Secretary of Commerce in applying the national security concerns of the Secretary of Defense to his licensing criteria. Without these standards, there is a possibility that, on the grounds of vagueness, the plea "national security" would not, in and of itself, be sufficient to forestall issuance of a license.

(2) As the department with the greatest equity in overflight security, the DOD nevertheless should develop its standards in coordination with the entire counterintelligence community. (In this connection, all departments and agencies should recognize that their sensitive outdoor activities, at least, are vulnerable now to overhead collection and will become more so as technology advances.)

Accordingly, I ask that your committee undertake an interagency review of the subject and recommend to the Secretary of Defense standards for the guidance of the Secretary of Commerce in meeting the necessary national security concerns in the licensing process.


Craig Alderman, Jr.
Deputy

Page Denied

UNCLASSIFIED

2

(U) Satellites could be used extensively to "monitor" status of US developmental efforts in controversial areas of research and development. Much is published in open sources which indicates where (in general terms) such research is done. This initial targeting data could be used for the periodic "looks" by the media's overhead systems. Consequently, if not already in place, steps would have to be taken routinely at these locations to avoid observation by the systems.

(U) There are very significant dollar/time costs associated with avoiding overhead platforms at research and development locations. Some tests can be conducted only under certain weather or atmospheric conditions. It is misleading to assume that the use of avoidance countermeasures will always work because the costs of postponement may be prohibitive and test preparations cannot always be hidden.

(U) The difficulty of hiding a large-scale military operation would be complicated by adding to the list of potential intelligence collectors. Large numbers of troops, equipment, and supplies must be massed at the decisive time and place. Barring the availability of ground, ship, or airplane observation posts, satellites provide the best means of verification. Low resolution systems are sufficient for detecting mass buildup.

Indirect Threats

(U) Media publication of "facts" they gather about their targets' (military, economic, or political) capabilities, problems, or intentions might give hostile intelligence services an insight into true US intelligence assessments.

(U) Friendly intelligence collection could be affected by foreign efforts to accelerate their counterimagery programs based upon the added threat to their operations posed by increased US satellite activity.

(U) Target antisatellite efforts could be accelerated to the detriment of US military capabilities since media satellites would also have to be taken out in early stages of war or preparation for war. (On the other hand, a US-licensed commercial system could augment US capabilities.)

MEASURES AVAILABLE TO PROTECT NATIONAL SECURITY

Notification

(U) The key ingredient to achievement of protection from any overhead threat, including that of a postulated MEDIASAT, is notification, the necessary elements of which are tracking and reporting.

UNCLASSIFIED

Page Denied

UNCLASSIFIED

4

Licensing Provisions

(U) The Land Remote-Sensing Commercialization Act of 1984 (15 USC 4277) requires the Secretary of Defense to determine the conditions necessary to meet national security concerns with respect to issuance by the Secretary of Commerce of the requisite license for a remote sensing system in space, such as a MEDIASAT.

(U) The NOAC recognizes that the conditions of licensing under 15 USC 4277 of the act are for the sole determination of the Secretary of Defense; and, the NOAC understands that the current DoD position on the subject is that the DoD must have the "widest possible latitude" in determining the national security concerns. The NOAC, therefore, merely suggests the following possibilities for consideration of the cognizant DoD officials:

(U) When the Secretary of Defense, after conferring with the Chairman of the Joint Chiefs of Staff, declares that the disclosure of data collected from particular orbits during a particular time frame would pose a serious and immediate threat to distinct and compelling national security, that data shall be withheld from public distribution or disclosure for so long as the threat exists or until the same data can no longer be held undisclosed because of actual public disclosure by other means, e.g., a military action has been launched and reported.

(U) Discussion: There are two principal methods for imposing ad hoc limitations as suggested above:

- a. Imposing constraints on the timeliness of data dissemination in specific situations or specific geographic areas where directed for national security reasons. In peacetime such constraints should be in writing and limited to specific periods of time, or to the specific situation.
- b. Imposing constraints on the collection of imagery in such specific situations or specific geographic areas.

(U) Either method will probably be subject to legal challenges by an applicant for a MEDIASAT license as a violation of the First Amendment of the Constitution, and specifically as an imposition of impermissible prior restraint. Should the MEDIASAT concept become a reality, this issue could be expected ultimately to go to the Supreme Court for resolution.

(U) (Our initial advice is that the second method may be more defensible because, i) it does not involve the prior restraint

UNCLASSIFIED

Page Denied

UNCLASSIFIED

6

equipment which is available today, some of which is approved by the Government. The prevention of loss may well be worth the price of protection to the applicants who may consider incorporation of protection in any satellite system.

ADDITIONAL CONSIDERATIONS

(U) In the preceding sections the NOAC working group has addressed the narrow issue of protecting sensitive Defense information from reconnaissance by overhead satellites. There remain two different kinds of problems that, in the view of the working group, need to be considered by the Department of Defense: i) Guidelines for review of license applications and, ii) Guidelines for determination as to the need for imposition of controls on an operating system.

Guidelines for Review of License Applications.

(U) A primary concern should be the completeness of the information provided according to the Rules, including,

The date of intended commencement of operations and the expected duration of such operations;

The method of launch, and the name and location of the operator of the launch vehicle and the launch site;

The range of orbits and altitudes requested for authorized operation;

The range of spatial resolution or instantaneous field of view requested;

The spectral bands requested for authorized operation; and

Timeliness of reporting.

(U) (Whether or not a resolution limitation is to be imposed will be determined by National Space Policy, revision of which is under White House study.)

(U) In deciding later whether national security interests are involved, timeliness of dissemination of the imagery will be a factor.

Guidelines for Determination of the Need for Imposition of Controls on an Operating System.

UNCLASSIFIED

UNCLASSIFIED

7

(U) Once a license has been granted and the system is operational, consideration of what spatial resolution "ought to be" is no longer pertinent. The problem now is the determination of how, when, and in what manner any controls that the national security requires may be imposed.

(U) As has been indicated, control may be either i) prior restraint on the release of information already obtained or ii) constraints on collection so that the sensitive imagery is not obtained in the first instance. Both of these methods raise constitutional questions but the latter course seems to be the more reasonable. The obvious OPSEC problem with the latter course, however, is "tipping one's hand" since the media--and, through them, the whole world--could be warned both as to the geographic area and the timing in which something the Department of Defense considers very important is about to occur.

OVERSIGHT

(U) Notwithstanding the availability of remedies other than license conditions as discussed above (notification, concealment, and deception), the working group perceives the need to establish in the Department of Defense a single operational entity--an executive agent--with oversight responsibility for all matters arising from US media-controlled satellite imaging. The terms of reference for the executive agent should be established well ahead of the first application for a license and may include the following elements:

a. (U) Who, specifically, is to be responsible for following the situation so continuously and so carefully as to be able to identify situations in which a MEDIASAT could endanger the national security?

(U) (Note: Knowledgeable DoD working group members suggest the possibility of designating the Chairman of the Joint Chiefs of Staff as executive agent with the day to day responsibility--perhaps through a special group in the NMCC/NMIC--of advising the Secretary of Defense when the Secretary of Commerce needs to be notified of the application of predetermined controls. It is believed that an OSD staff element is too far out of the operational environment to fulfill this role.)

b. (U) How is the determination by the Secretary of Defense that action is needed to be conveyed to the responsible official in the Department of Commerce, the official who will actually impose the controls? Procedures in this area need

UNCLASSIFIED

UNCLASSIFIED

8

to be quite carefully spelled out since there could be situations in which time would be of the essence; delays of as little as 1 hour in initiating the proper reaction might make the whole exercise one of futility.

c. (U) What policy decisions need to be addressed for handling of applications for licensing of remote sensing systems?

d. (U) What policy decisions must be addressed as a basis for recommendations as to how and under what circumstances imaging controls would be imposed on a MEDIASAT because the Secretary of Defense had "determined" that the national security required those controls?

SUMMARY

(U) The NOAC working group believes that the following three statements summarize the thrust of this report:

a. Realistic protection from overhead imagery is through notification and OPSEC measures.

b. Given the current commercial imaging capabilities, constraints on spatial resolution by the US Government are not an effective control.

c. The Department of Defense should consider the designation of an executive agent to be responsible for all matters arising from US media-controlled satellite imaging.

UNCLASSIFIED

TERMS OF REFERENCE FOR NATIONAL OPERATIONS

SECURITY ADVISORY COMMITTEE

MEDIASAT WORKING GROUP

Review of Security Implications of Civil

Satellite Remote Sensing Programs

- I. TASK The Department of Defense has asked the NOAC to review the US Civil Satellite Remote Sensing Program and recommend to the Secretary of Defense standards for the guidance of the Secretary of Commerce in meeting the necessary national security concerns in the licensing process.
- II. BACKGROUND
- Under section 101 of the Land Remote-Sensing Commercialization Act of 1984, the Congress declared that, among other things, the national interest of the US lies in maintaining international leadership in civil remote sensing and in broadly promoting the beneficial use of remote-sensing data. The Congress declared, also, that land remote sensing by... private parties of the US affects...national security concerns of the US.
 - Section 402 of the Act prohibits any US person from operating any private remote-sensing system without a license (issued by the Secretary of Commerce).
 - Section 607 of the Act requires the Secretary of Commerce to consult with the Secretary of Defense on all matters under the Act affecting national security (including the issuance of the requisite license); and, the Secretary of Defense shall determine the conditions necessary to meet national security concerns.
 - The National Oceanic and Atmospheric Administration (NOAA), under the Department of Commerce, issued a Notice of Proposed Rulemaking (51 Fed. Reg. 9971, March 24, 1986) which, according to the Radio-Television News Directors Association (RTNDA), would violate the First Amendment. The thrust of RTNDA objections to the Notice is that the rules are unconstitutionally vague and would authorize NOAA to impose impermissible prior restraint. According to RTNDA, the question is not whether NOAA can take action to protect national security, but what standards must it use when doing so. NOAA has responded to the comments and has issued Final Regulations effective August 10, 1987, (52 Fed. Reg. 25970, July 10, 1987)

- Given that commercial multispectral imaging resolution of other countries, such as France and Japan, is at least as good now as the US, and over the years along with US, commercial satellites will achieve even better resolution, the question becomes, "How does the US accommodate necessary and inevitable commercial growth in space and still protect US sensitive information?"

III SCOPE OF REVIEW

- What are the national security implications of an extensive media use of high-resolution satellite imaging capabilities?

- What measures are available to protect national security concerns relative to media use of civil satellite imaging systems, both US and foreign? (Responds to first bullet, above.)

+ Notification à la SATRAN (Satellite Reconnaissance Advanced Notice) and FRNDSAT

+ Concealment and military deception

+ Licensing provisions under section 607 of the Act.

IV REPORT

a. Scope Consistent with the NOAC charter, paragraph 2.c., the mediasat working group should limit its report to discussion of the national security implications, that is, the OPSEC vulnerabilities, and to corrective measures to overcome those vulnerabilities.

b. Disposition. The report should be forwarded to the Chairman, NOAC, who will decide its further disposition. That is, if he concurs in the report, provide its advice and recommendations concerning OPSEC vulnerabilities and corrective measures to the Secretary of Defense, ATTN: DUSD/P, Washington, D.C. 20301-2200.

TAB B

National Operations Security Advisory Committee
MEDIASAT Working Group and Advisers*

John Hoover, ODUSD/P, Chair	697-7641	
Major General Jack Thomas, USAF-Ret. C ³ I*	697-2720	
A. R. Cinquegrana, DoJ-OIPR*	633-5604	
Mark Evans, DoJ-OIPR	633-5607	
		STAT
Peter Modley, State, INR*	647-8651	
Alan Brown, Commerce	377-1722	
		STAT
MAJ Bill Puddy, Army/DAMO-OD	694-8199	
LCDR Bob Golding, JCS/J33	695-1653	
		STAT
CPT Mary Moffitt, ODUSD/P/CI&IP	697-9586	

Page Denied

Next 5 Page(s) In Document Denied

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
FOR COMMAND, CONTROL, COMMUNICATIONS
AND INTELLIGENCE

Date June 5, 1987

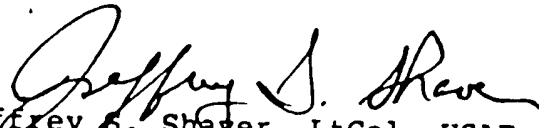
Memo for Mr. Latham

Attached is the background paper you asked for in preparation for your TV interview with Hodding Carter on "Use of imaging satellites by news media."

All pertinent information in the tabs has been summarized in the paper itself. The only real, written policy of the U.S. Government on this topic is Public Law 98-365, "Land Remote-Sensing Commercialization Act of 1984," and NSDD-42, "National Space Policy," from 1982. DoD's only written position on this is a DUSD(P) letter to NOAA commenting on their proposed rules for implementing PL 98-365.

I have included some other information on current activities, some discussion of possible national security concerns, and some potential pitfalls that might come your way during the interview. Your staff expert on this issue is MGEN Jack Thomas, X72720, in DASD(I). He provided most of the information here.

Jan Bodanyi sent me an audio tape of Mr. Carter's interview with Mr. Sims, done on 2 June 1987. It might be good preparation, if you are interested.


Jeffrey S. Shaver, LtCol, USAF
Military Assistant for Space
Policy Development

Background Paper
for
MacNeil-Lehrer Interview on
"Use of Imaging Satellites by News Media (MEDIASAT)"

INTERVIEW SPECIFICS

ASD(C3I) to do interview (tentatively 1630, June 5, 1987) with Mr. Hodding Carter for MacNeil-Lehrer Newshour.

They want DoD/Administration spokesman to discuss DoD concerns over possible security problems when media uses remote sensing satellites (i.e., SPOT).

What is potential for abuse when media uses remote sensing satellite information?

Are there legitimate national security concerns?

If so, what are they?

Examples?

OUTLINE

Paper is structured as follows:

- I. Current Policy Framework
 - o General Observations
 - o Public Law
 - o Presidential Directives/Policies
 - o Department of Defense Directives/Policies
- II. Current Activities/Ongoing Actions
 - o NOAA Licensing Rule Development
- III. National Security Concerns/Issues
 - o Specific Interview Questions (as above)
- IV. Cautions/Potential Pitfalls
- V. Classified Addendum

PREPARED BY: LtCol Shaver/X50210/4 Jun 87

I. CURRENT POLICY FRAMEWORK

o General Observations

- Current policy framework appears limited in scope.
 - Public law (PL 98-365, "Land Remote Sensing Commercialization Act of 1984") really only aimed at getting U.S.G. out of funding LANDSAT system; recognized potential national security implications, but did not really anticipate MEDIASAT type developments (i.e., use of satellite remote-sensing for collection of "intelligence-like" information for rapid dissemination to the public through the media).
 - Presidential policy (NSDD-42, "National Space Policy") establishes goal of expanding private-sector involvement in space and space-related activities, and requires U.S.G. to provide climate conducive to this expanded private-sector involvement, with due regard for national security; not very clear on how resolution is achieved when commercial interests, first amendment rights and national security interests collide.
 - DoD Space Policy, February 4, 1987, concentrates on military space program policies, but recognizes as a contributory goal the need for a strong technology base and a healthy space industry; policy requires DoD to cooperate with civil and commercial sectors for mutual benefit.
 - Only official DoD written position specific to issue of land remote sensing is DUSD(P) letter of January 22, 1987, to NOAA commenting on NOAA's proposed rules for licensing private remote sensing space systems; rules have not been finalized, so we do not know if contents of this letter have been accepted by NOAA (i.e., do not know if this position will become U.S.G. policy).
- Current policy framework (PL 98-365, NSDD-42) does not appear to have kept pace with new issues in satellite remote sensing; policy apparently did not anticipate:
 - Speed of technology developments related to civil/commercial remote sensing systems and capabilities;
 - Extent of growth of commercial media interest in exploiting capabilities of such systems;

I. CURRENT POLICY FRAMEWORK (Continued)

- Significant growth of foreign remote sensing satellite capabilities beyond the reach of potential U.S. regulatory constraints

o Public Law

- Public Law 98-365, "Land Remote-Sensing Commercialization Act of 1984", July 17, 1984 (Tab A)
 - Lawmakers recognized value of commercial remote sensing capabilities, but also recognized existence of impacts on national security and expressly required protections for preservation of national security.

"TITLE I-DECLARATION OF FINDINGS, PURPOSES AND POLICIES

FINDINGS

Sec. 101. The Congress finds and declares that--...

(1) the continuous civilian collection and utilization of land remote-sensing data from space are of major benefit in managing the Earth's natural resources and in planning and conducting many other activities of economic importance;...

(4) land remote sensing by the Government or private parties of the United States affects international commitments and policies and national security concerns of the United States;...

(13) certain Government oversight must be maintained to assure that private sector activities are in the national interest and that the international commitments and policies of the United States are honored;....

PURPOSES

Sec. 102. The purposes of this act are to--...

(2) maintain the United States worldwide leadership in civil remote sensing, preserve its national security, and fulfill its international obligations;....

I. CURRENT POLICY FRAMEWORK (Continued)

POLICIES

Sec. 103. ... (c) It shall be the policy of the United States both to commercialize those remote-sensing space systems that properly lend themselves to private sector operation and to avoid competition by the Government with such commercial operations, while continuing to preserve our national security, to honor our international obligations, and to retain in the Government those remote-sensing functions that are essentially of a public service nature."
[Underlines added]

- Law establishes Secretary of Commerce as manager of commercialization program; gives Secretary licensing authority for private remote-sensing space systems; establishes conditions for operation of such systems.

"TITLE IV-LICENSING OF PRIVATE REMOTE SENSING SPACE SYSTEMS

GENERAL AUTHORITY

Sec. 401. (a)(1) In consultation with other appropriate Federal agencies, the Secretary is authorized to license private sector parties to operate private remote-sensing space systems for such period as the Secretary may specify and in accordance with the provisions of this title.

CONDITIONS FOR OPERATION

Sec. 402. (a) No person who is subject to the jurisdiction or control of the United States may, directly or through any subsidiary or affiliate, operate any private remote-sensing space system without license pursuant to section 401.

(b) Any license issued pursuant to this title shall specify, at a minimum, that the licensee shall comply with all of the requirements of this Act and shall--

(1) operate the system in such manner as to preserve and promote the national security of the United States and to observe and implement the international obligations of the United States in accordance with section 607;...."

[Underlines added]

ATTACHMENT - 4

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)
WASHINGTON, D.C. 20505

(ISCOM)

9 November 1987

ANNUAL REPORT
OF THE
INFORMATION SECURITY COMMITTEE (ISCOM)

SECTION I

A. This section of the annual report of the ISCOM is based on the ISCOM charter, minutes, and special reports of the ISCOM.

1. The ISCOM charter was approved by the Chairman of the Interagency Group/Countermeasures (Policy) (IG/CM(P)) on 2 December 1986. The charter provides an authoritative basis for the ISCOM, and sets forth its mission, functions, responsibilities, composition and organization.

2. In its first year of operation, the ISCOM met four times; the meeting dates were 21 August 1986, 13 November 1986, 3 February 1987, and 22 July 1987. (The next meeting is set for 18 November 1987.)

3. Some of the activities of the first year were devoted to establishing a charter document that would be acceptable to the many diverse interests represented by ISCOM departments and agencies, namely:

- Department of Defense
- Department of Army
- Department of Navy
- Department of Air Force
- Defense Intelligence Agency
- National Security Agency
- Federal Bureau of Investigation
- Department of State
- National Security Council Staff
- Central Intelligence Agency
- Department of Justice
- Department of Commerce
- Department of Energy
- Department of Treasury
- Information Security Oversight Office
- Intelligence Community Staff

However, most of the ISCOM's first-year effort was devoted to the task of determining the disposition of the many significant recommendations contained in the so-called IG/CM(P) "collated list of action items" dated 24 October 1986. Of the 95 action items, the

ISCOM initially was assigned 38 for action. In the process of disposing of most of those, the ISCOM made contributions to the solution of other recommendations, including input to the Personnel Security Committee for the recommendations on government-wide training objectives, use of the polygraph for counterintelligence purposes within the Department of Defense, and reimbursement to the government for personnel security investigations based on false information. The ISCOM reported its progress on the collated list of action items on 30 March 1987, 7 April 1987, and 9 October 1987; only a few of the action items remain to be addressed.

SECTION II

B. This section of the annual report pertains to the ISCOM's projected activities for its second year of operation.

1. The ISCOM's course for its second year of operations has been set to some extent by past events. It is clear that the following will have to be addressed:

a. Disposition of the remaining action items from the collated listing cited above. (Included are the recommendations to ensure that plans are developed to maintain the security awareness of the public at large and the possible significance of foreign contacts, and closing out action on other recommendations such as welcoming the opportunity for joint discussions between Congress and the Executive Branch to examine various approaches to legislation regarding unauthorized disclosure of classified information.)

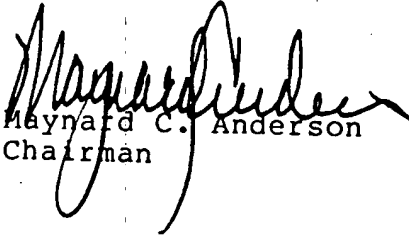
b. Address the many information security questions concerning the STU-III that is about to be placed in wide-spread use. (It is likely that this will become a tasking derived from the "1987 National Assessment of the Hostile Intelligence Threat and U.S. Countermeasures.")

c. Ways and means to stimulate and provide better classification management. (The initial decision to classify information drives all other classified information security countermeasure programs.)

d. Support and guide implementation of the 13 initiatives of the Information Security Oversight Office. (Approval of these by the President is anticipated soon.)

2. The ISCOM can and should play a larger role as a forum where department and agency representatives can exchange views, problems, and solutions that impact both interagency and internal settings. The cumulative expertise represented in the ISCOM is enormous and this national resource should be used to the fullest extent, and in harmony with, the Information Security Oversight

Office. The ISCOM should be more active in its second year. It is anticipated that the ISCOM will meet six times, at least, and may form working subcommittees to address particular matters such as the STU-III.


Maynard C. Anderson
Chairman

ATTACHMENT - 5

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)
WASHINGTON, D.C. 20505

Physical Security Committee Report

November 10, 1987

MEMORANDUM FOR: Chairman,
Interagency Group/Countermeasures (Policy)

VIA: Director,
Community Counterintelligence and Security
Countermeasures Staff/IC Staff

FROM:
Chairman,
Physical Security Committee

25X1

SUBJECT: Status of the Physical Security Committee
Efforts

The attached synthesizes the current status of this Committee's activities in regard to the initiatives raised by the President's and SSCI reports on counterintelligence and security countermeasures. A summary of our other efforts and planned action is also discussed.

Attachment:
As stated.

Regraded Unclassified when
Separated from the
Classified Attachment

Doc. 43 Brandt

SECRET/NOFORN
DECL:OADR

SECRET/NOFORN

November 10, 1987

Physical Security Committee Progress Report

1. Synopsis:

The Committee's Charter was approved by the sitting membership at its third meeting, on May 22, 1987, and forwarded to the IG/CM (P) for approval and dissemination. The Committee has held seven meetings since its inception and has gathered consensus in establishing direction and priorities. Currently we are actively involved in the combination lock initiative, determining existing centers of excellence, and reviewing the GSA Interagency Committee on Security Equipment (IACSE) master plan. Action initiatives from the President's Report may soon become an active issue for the Committee to address because of the budget's impact on certain of the recommendations. A summary of our progress in each of these areas follows.

2. The President's and SSCI Reports:

Enclosure 1 is the most recent report of the Physical Security Committee's efforts on implementation of the initiatives stemming from the President's and the SSCI Reports. To summarize our efforts:

- The SSCI recommended in item 103 of their report that intelligence agencies be given the opportunity to participate in the planning and oversight of new office building construction efforts, the CIA should strive for timely involvement in this endeavor, and long-range security plans for East Bloc missions should be accelerated. CIA and other interested intelligence agencies have personnel assigned to the Foreign Buildings Office. These elements continue to participate in the planning, design and construction phases of new building work. The CIA has taken the lead role to ensure timely participation and response by the intelligence community. Current initiatives in this arena are focusing on the need for the long-range plans of the intelligence community to be vetted early by the Foreign Buildings Office.
- The President's Report stressed the need for the community to sustain Congressional funding of programs developed from the Advisory Panel on Overseas Security (The Inman Report). The current fiscal restraints required to meet

SECRET/NOFORN
DECL:OADR

SECRET/NOFORN

-2-

reduced funding level projections will impact continuance of security enhancement work in the physical security area. Without an increased Base in FY 1989, the Department of State will only be able to sustain a base program and maintain security postures at a portion of the missions overseas requiring service and support. No new enhancements will be fundable. We will fall short by roughly 60 posts from meeting the Secretary of State's goal of a standard level of security for all our Missions, world-wide.

This matter will be raised at the next Physical Security Committee meeting to determine what support may be solicited from others who have involvement in the foreign arena and would stand to benefit from maintaining the enhancement program to completion.

- The most recent action by the Congress to use Diplomatic Security Capital Funding for temporary off-setting of reduced S&E funding levels may impact compliance with the SSCI Report item 1020, implementation of the Inman Panel recommendations for relocation of our most vulnerable overseas facilities. The Panel's original listing has already been payed back for budget as well as real estate reasons. We can not predict the impact of further reductions until the Congress produces an FY 1988 appropriation. At that time the Department of State will reopen and review the list.

3. Combination Lock Initiative:

Development of new specifications and test criteria for dial combination locks is underway. GSA has received an adequate level of commitment to funding from other agencies to fund the NCEL lock program. The Committee will request quarterly status from NCEL on this project.

The Department of State, working with the CIA, has initiated a contract with Sargent & Greenleaf (S&G) Locks Company to produce a modified S&G 8500 series combination lock unit that will address the vulnerability to technically assisted manipulation. S&G is evaluating several different approaches and will be reporting their findings shortly.

SECRET/NOFORN
DECL:OADR

SECRET/NOFORN

-3-

The Lock Initiative Subcommittee of this Committee is responsible for the lock initiatives effort. Their next agenda will involve determining the need for criteria and standards and certification of a testing facility, commercial or government, and the process for support, qualification and certification of commercial vendor security equipment.

4. The Master Plan:

A representative of GSA briefed this Committee in September on that agency's efforts to develop and implement a Master Plan to standardize security equipment terminology, and testing and certification standards and processes in meeting the common needs of the Government. To this end, the GSA formed the Interagency Advisory Committee on Security Equipment (IACSE). The IACSE prepared a Master Program Plan of 13 taskings and contracted for support of the effort to Dynatrend, Inc. Enclosure 2 is a background and status report on the IACSE.

According to the GSA brief to this Committee:

- The Master Program Plan was projected as a \$3.4 million three-year effort but only partially funded for start-up. Full funding was never budgeted by GSA.
- The Contractor had completed some of the taskings and reported their findings to IACSE.
- GSA would maintain its responsibility for specification and standards but did not have the expertise required to manage such a technically specific program. GSA would have to remain dependent on user agencies to fund and drive such efforts.

The Physical Security Committee is currently reviewing the IACSE initiated Master Program Plan to determine the need and feasibility of continuing the Plan. The general consensus of this Committee is to continue the Master Plan. In the next meeting we will be determining the taskings and priorities, and the contract support required to continue the plan or portions of the plan considered applicable to the Committee's Charter.

Doc. 44 Brandt

SECRET/NOFORN
DECL:OADR