

HANDLE VIA
BYEMAN
CONTROL SYSTEM



RAK-Y5-16
POL-A-4
myn

~~TOP SECRET~~
(S) NATIONAL RECONNAISSANCE OFFICE
WASHINGTON, D.C.

THE NRO STAFF

February 1, 1968

MEMORANDUM FOR DR. FLAX

VIA: General Berg and Mr. Reber

SUBJECT: Recommendation G, of a Report forwarded by DCI to the NSAM 156 Ad Hoc Committee, 19 September 1967

I have been addressing the matter of Dr. Seamans' request for clarification related to Recommendation G of the special study panel's report prepared as DCI security policy in response to the NSAM 156 Committee's Recommendation #7.

I find myself at grips with a very difficult problem. My initial approach was to prepare a draft study (see attached, which I forward to you at this time for exemplifying purposes only). The study attempts to define sensitive technology in terms of OAO-Voyager activities, and then proceeds to outline the elements of a NASA instituted and managed security system (distinct from, yet complimentary to BYEMAN) designed to provide the appropriate level of security protection. I am now convinced that this is not the answer, that any system of strict security for this purpose within NASA would be as an oasis in the desert. Particularly so, unless we can devise a good reason for the special security, appropriate for unclassified consumption.

Upon re-examination, I have concluded, that the inconsistencies which presently exist between NASA and DOD methods of security operation, cannot be adequately dealt with on the basis of DCI security policy guidance alone (competent only as it relates to protection of intelligence sources and methods). Although I presently have no detailed evidence to support such a conclusion, I am convinced that these inconsistencies exist across the board and are by no means limited to matter of satellite, reconnaissance-like sensor activity. It is just a case where attempt is being made to apply the grease to the noisiest wheel.

HANDLE VIA
BYEMAN
CONTROL SYSTEM

~~TOP SECRET~~
EXCLUDED FROM AUTOMATIC REGRADING
DOD DIRECTIVE 5200.10 DOES NOT APPLY

CONTROL NO INTERNAL
COPY _____ OF _____ COPIES
PAGE 1 OF 3 PAGES

It is unfortunate that DOD and NASA have placed so much singular emphasis upon the subject of the security of reconnaissance-like sensors, because anything we do to attempt to correct the situation, is doomed to self-defeat. The reason for our corrective devices becomes immediately apparent; in some circles they are viewed as being DOD interest serving. The result is controversy and controversy is a deadly enemy of security. Furthermore, it is far easier to define what technology should be behind the special security fence in DOD, where the alternative is special access required or at least normal security classification, than in NASA, where the alternative is no security at all. In the case of satellite reconnaissance, all elements of technology, whether spacecraft, hardware or software, contribute in some measure to our degree of success.

I now feel that the matter of the security of overall NASA-DOD space technology should be addressed first. This is long overdue. With the U.S. Government spending close to six billion dollars per annum on space activities, and with the ratio favoring NASA between 4 or 5 to 1, it is not in the national interest to permit NASA and DOD to continue with such a stark difference in basic security philosophies. Certainly with the U.S. Government providing such substantial funding for the advancement of space and related technology, it is within its rights to insure that a process exists for a review of the resulting technology to ascertain if it itself does not have some other application for the technology, i.e. some defense or intelligence application. If some defense or intelligence application exists, then an appropriate level of security classification and/or control should follow - regardless of what government organization was responsible for the initial effort.

Yes, I am talking about a form of 5200.13 to cover both DOD and NASA space activities. But that would be the policy, first we would need to define the objective and then the mechanism. The objective, I think, would be clear: to insure adequate consideration of potential military applications for U.S. Government sponsored space research and development, with appropriate security controls to follow. The mechanism, I feel, would of necessity have to involve something revolutionary - possibly the establishment of a JSTCO (Joint Space Technology Coordinating Office) however, it may be that the matter could be explored initially within the framework of existing organization such as the MSFPC, the Space Council or PSAC.

RECOMMENDATION:

That you authorize this subject to be pursued from the standpoint of overall DOD-NASA security inconsistencies, rather than attempting to solve the problem based solely upon the requirements for intelligence sources and methods protection. Once we have dealt with the former, the latter will surely come into sharper focus.

Atch


LOUIS F. MAZZA
Assistant for Security
NRO Staff

A STUDY

Recommendation G, Section XIV
of a Report forwarded by DCI
to the NSAM 156 Ad Hoc Committee,
19 September 1967, Examined.

I. BACKGROUND:

Included in a report of a special study panel convened to consider the matter of Recommendation #7 of the NSAM 156 Ad Hoc Committee's report of 11 July 1966 "Political and Security Aspects of Non-military Applications of Satellite Earth Sensing", was the following recommendation:

"G. NASA systems intended to produce better than the prescribed .LMR limiting criterion, such as might be required for purposes of lunar or extra-planetary exploration or astronomical observation from earth orbit, should be developed utilizing security procedures presently prescribed under project UPWARD."

Whereas recommendation G of the special study panel's report deals with a subject not considered by the NSAM 156 ad hoc Committee, the panel, after developing rationale supporting the need for special security controls for image forming, satellite borne equipment producing better than the .LMR limiting criterion, opined, "that optical and spacecraft technology and technical requirements for telescopes for stellar and solar observations, are of a degree of significant ^{similarity} with NRP high resolution optical systems, as to warrant the development of a security guide for such activities similar to that prescribed under project UPWARD."

On 19 September 1967, the DCI approved the findings and recommendations of the special study panel and forwarded its report to the NSAM 156 ad hoc Committee.

At the Manned Space Flight Policy Committee meeting of 28 November 1967, the Deputy Administrator, NASA asked: "What are the relationships between these potentially restrictive considerations and what is likely to happen to the technology?" He exemplified OAO, NASA's planned efforts for an astronomical telescope and the VOYAGER program as areas of possible conflict resulting from recommendation G. The Director, National Reconnaissance Office agreed to prepare a position paper and to consult with the DCI regarding the matter.

II. PURPOSE:

The purpose of this study is threefold:

(1) To attempt to differentiate, in the sense of the degree of security protection required, between NASA systems designed for purposes of astronomical observation from earth orbit or space exploration and those designed to observe the earth's surface.

(2) To attempt to identify sensitive technology related to such activities, as would require special security controls in order to insure continued protection to the NRP as a vital U.S. intelligence source.

(3) To recommend an appropriate system of security for such activities.

III. INTRODUCTORY RATIONALE:

Prepared as DCI security policy guidance, this study is competent to speak only to the subject of the degree of security protection required to protect a vital intelligence source. This requires an estimate as to the impact of various public or international exposures in terms of bringing about various levels of counteraction, which would prejudice the end effectiveness of the NRP, the intelligence source - in short, an estimate of the provocation.

There is a very fundamental difference between security requirements related to NRO and NASA activities involving the use of spacecraft borne optical sensors. This is the requirement under NRP to conceal the on-board presence of the optical sensor, a requirement which does not exist in regard to NASA activities. In considering the present subject, this fundamental difference effects the conclusions related to what technology should be provided special security protection as well as the character and composition of the system of security controls to be imposed, as will be shown later.

IV. SECURITY REQUIREMENTS FOR NASA, OAO/VOYAGER TYPE AND EARTH SURVEY ACTIVITIES DISTINGUISHED:

The provocation value of imagery resulting from NASA astronomical observations from earth orbit or resulting from survey of other planets, in terms of causing prejudice to the NRP, would in all probability be minimal regardless of the resolution produced. This is because the imagery will be

of unfamiliar surfaces and will include none of the usual landmarks which are characteristic of reconnaissance photography.

The provocation value of research, development and fabrication activities related to such activities however, will in all probability be significant, inasmuch as the equipments produced will be comparable in most respects to ^{those} high performance equipments used for satellite reconnaissance purposes. If conducted without benefit of strict security controls, this would provide to those who are interested, a convenient corollary to U.S. satellite reconnaissance systems, which would serve as excellent data base to those adversaries considering counteraction, particularly if they lean toward more sophisticated techniques to inhibit the program, least apt to involve themselves in international confrontation as a result of their acts.

This leads to the conclusion that, whereas research, development, and fabrication activities related to such programs should be subject to strict security controls in deference to the vital intelligence source, some allowance can and in all probability should be made with respect to data reduction, compilation and analysis activities associated with the resulting imagery, even to the extent of providing the basic geometry related to the optical sensor (eg: focal length, swath width etc) necessary to those engaged in such activities. This would allow for the

full and open exploitation of the resulting imagery, uninhibited by special security controls.

V. SENSITIVE TECHNOLOGY IDENTIFIED:

An important point to be considered in identifying that technology associated with NASA OAO/VOYAGER type activities requiring special security controls, is that not all of the items to be listed, currently require BYEMAN security controls within the NRP. This seeming enigma stems from the previously referred to fundamental difference between security requirements related to NRO and NASA activities involving use of spacecraft borne optical equipments. It is not the first time that it has had to be considered with respect to NRO V/A/V NASA activities, for whereas a NASA image forming sensor for earth application, designed to produce no better than .1MR, would not require special security controls, NRO systems of similar capability do.

Because covert or semi-covert activities, if they are to remain such, must compartment the sensitive portions of the activity into the smallest possible nuclei, much fringe technology (not directly involving the optical sensor, but critical nevertheless to the complete spacecraft/sensor reconnaissance system) are within NRP, handled under normal security classification and controls, however, the application to a satellite reconnaissance system is "fuzzed" through the use of cover explanations and/or "cut-outs," appropriate to the particular situation. If the same degree of security protection were to be afforded this fringe technology within

NASA activities, where the concealment of the on-board presence of the optical device is not a security requirement, an easy corollary could be drawn.

The following technological items are therefore recommended for special security controls in association with NASA OAO/VOYAGER type activities where they are intended to include image forming sensors designed to operate at better than the prescribed criterion:

(1) All data related to the internal composition of the image forming sensor, not essential to data reduction, compilation and analysis of the resulting imagery.

(2) All processes related to image forming sensor fabrication, related lens grinding and polishing, mirror construction and film manufacture to be either researched or developed under NASA contract.

(3) Those command and control processes which reveal data described in item #1 above to include indications of cycle time limitations, image motion compensation techniques, focus, filter, and exposure controls.

(4) That data related to the spacecraft, external to the image forming sensor, but which have a direct bearing upon sensor targeting, timing, and attitude controls, temperature and other environmental requirements critical to sensor functioning.

VI. RECOMMENDED SYSTEM OF SECURITY:

The system of security recommended is one which would be instituted and managed by NASA, subject to review by the Offices of the DCI to insure compliance with DCI security policy guidance. The system would not involve semi-covert security procedures such as those used under the NRP, because it is only the technology which is being protected and because semi-covert procedures do/^{not}lend themselves well to NASA activities and organization. It is intended to be distinct from, yet complimentary to the NRP system of security (BYEMAN). The system recommended is one which is adaptable to implementation within the framework of the existing NASA organization and those agreements into which NASA has entered with other U.S. Government organizations related to the subject of security.

The basic elements of the recommended system of security are as follows:

- (1) Implementation and management by NASA.
- (2) Review by the Offices of the DCI to insure compliance with DCI security policy guidance.
- (3) Prerequisite TOP SECRET security clearance for all individuals provided access to controlled information (Recommended in preference to DCID 1/14 personnel security requirements, because access to actual intelligence activities is not being authorized and because TOP SECRET security clearance standards are more compatible with NASA's organization and existing

agreements with other U.S. Government organizations related to the subject of security).

(4) Physical security protection consistent with BYEMAN standards.

(5) Strict, formal review of need-to-know for all individuals provided access to controlled information, consistent with the requirements of the activity.

(6) Special control of documents, equipments, and associated data designed to insure that access to controlled information is limited to only authorized individuals.

(7) Prior coordination with the NRO through the SACC before entering into negotiations with contractors involving activities requiring access to controlled information, in order to insure compatibility with any NRP instituted security procedures which may be applicable to the particular contractor's facility.

VII. SUMMARY RECOMMENDATION:

That NASA, in consideration of a vital U.S. intelligence source, institute a system of special security controls, the basic elements of which are described in Section VI of this study, to be applied to technology related to the use of image forming sensors for purposes of space exploration or astronomical observation from spacecraft. The technological data recommended for special security control ~~is~~^{are} listed in Section V.

DEPARTMENT OF THE AIR FORCE
OFFICE OF THE SECRETARY

MEMORANDUM

April 16, 1968

Paul:

Please note Gen. Berg's comments. In all honesty, I'd like to comply with Russ' request, but I've about run dry on this subject.

My problem is - "D/NRO agreed to prepare a position paper and consult with the DCI regarding the matter" and there is no question but that that is my action.

General Berg wants SACC to try it on for size - and I don't even know how to go about introducing the subject to that group.

How's about SS-5 taking this one on? No kidding - I'm not crying - but I just know that this will get no further action if it stays with me.



Mr. Mezza -

I've been thru one long
enough and now wish to move
out. I'll not go thru the documents
in fine detail - I only wish to
say - Let's not rock the boat.
We have a system working now
let's continue to use it.

Another point for consideration
Introduce the subject to the
SACC and see how it goes. see
what the feelings are in this group.

Frankly, get together with
Paul, Ron, such as you did on ETR
problem and let's get a single
position on this one -

Russ

MEMORANDUM

FOR MR MAZZA

I visualize one page - or a page and a half.

1. We set rules on pecc sensors in 1965.
2. We were really thinking of earth-sensors
3. Here you all are in the astronomy business
4. We don't mean to inhibit that...
5. However, whenever you use NRP-
derived technology for astronomical
purposes, we are involved and
want to be in on the deal.
6. So - continue to send your astronomy
program to SACC for coordination,
pre-initiation. This is mandatory
7. SACC knows the problem and can
help you handle it.

Duce

MEMORANDUM February 2, 1968

General Berg:

I've discussed the attached with Col Worthman. Although he understands my philosophy, recognizes that I have a tough problem and respects my integrity - he disagrees with my staff work (the manner in which I have gone about responding to Dr. Floss).

See also attached some of Col W's earlier comments. Col W agrees that I forward this matter as is to you.

L. Maggs