~~TOP SECRET NOFORN~~

NRO PROTECTION REVIEW

"WHAT IS [redacted]

6 November 1992

Handle via [redacted]
~~TALENT-KEYHOLE-COMINT~~
Control Channels Jointly

~~TOP SECRET NOFORN~~

INTRODUCTION

The DDCI directed this comprehensive review of the content of [redacted] and other security systems interfaces. A joint NRO/CIA IG report noted and added the need to determine what must remain [redacted] This report outlines the approach to the study as approved by the NRO Board of Directors; the top down protection review reflected in updated classification guides; specific ground station location issues; contractual and industrial concerns; and specific recommendations to the DNRO.

REVIEW APPROACH

This review of [redacted] was conducted in response to the DDCI's concern that there is a "lack of good definition in the interfaces [redacted] TALENT-KEYHOLE, and the other security systems' interfaces . . . ." Our starting point was the DDCI's categorization of the "program's original purpose: To protect key, specific, and fragile details of reconnaissance satellite design and operation." These "key, specific, and fragile details" are the intelligence sources and methods which the DCI has the charter to protect. For the purposes of this paper, those sources and methods are defined as the means by which the U.S. gathers intelligence using reconnaissance satellites (the mission sensitive aspects of each collector.) [redacted]

Using that as the ultimate criterion, we can identify six areas of information which have traditionally been considered to be exclusively [redacted] and apply the test. They include 1) system vulnerability and survivability information, 2) system development and key design information, 3) industrial and contracting relationships, 4) funding and budget, 5) sensitive launch integration and operations, and 6) command and control operations.

Based on direction from the DNRO, the NRO Program Directors tasked each satellite system program manager to conduct the "top

down" review to determine what requires [redacted] The goal was to severely reduce the amount of information [redacted] and then provide guidance in revised classification guides.

For an in-depth technical and security analysis, the review activity would require the expertise of program managers, system engineers, and security officers within the NRO. In order to disseminate information on the purpose and objectives of the activity, briefings were given to each of the Program Offices, internal NRO elements, selected CIA and DIA offices, Intelligence Community Staff representatives and [redacted] (See Pages 16-17 for those briefed on the review.)

The survey findings and study approach were briefed to the NRO Board of Directors on 10 May 91. The DDNRO requested a status report on 25 Sep 91. In September, the Program Office Directors questioned the initial results and requested additional time to ensure a comprehensive in-depth review as envisioned by the Board of Directors.

During review preparations and the initial survey, several important observations were provided to the various program elements to help set the stage for their work. First, the relationship between [redacted] TALENT-KEYHOLE is often misunderstood by those who work primarily in only one of the control systems. This, together with large numbers of personnel untrained in classification, resulted in erroneous judgments over time in compartmenting NRO information. For a manufacturing activity, the initial rationale for classification/compartmentation was often lost with the rotation of personnel; the security judgement requirement was handed down often unquestioned. Second, there has been a tendency to simply classify [redacted] for ease of handling and cost savings. The definition and breakout of sensitive information diverted engineers from other tasks, and in the 1960s-70s, there was much less interaction with the user community. Third, a general belief prevails that system capabilities exist solely at [redacted] the TALENT-KEYHOLE level. The individual system capabilities descriptions at the TALENT-KEYHOLE level were

closely held and not often updated, especially after Kampiles sold a KH-11 manual to the Soviets in 1978. When the Joint-Service Tactical Exploitation of National Systems (J-TENS) Manuals were disseminated at the TALENT-KEYHOLE level in the early 1980's, they were incorrectly used as a classification guide. These TALENT-KEYHOLE descriptions relieved pressure on the program offices to update their earlier guidance.

RESULTS OF CLASSIFICATION GUIDE REVISIONS

Each program office, following their top down review, provided revisions of classification guides. A key issue was the clear identification of capability and tasking information [redacted] Each of the classification guides was reviewed for content, format, and clarity. The long term goal is the formulation of system-level classification guides which follow a generalized format, address relevant facts concerning the classification of specific systems, and are "user friendly." The draft guides were evaluated both individually and collectively for correlation and uniformity.

The major areas that were reviewed across all programs encompassed mission ground station locations, targeting/collection by each system, launch dates/activity, relay satellite information, ephemeris data, and system vulnerabilities. In addition, each classification guide was reviewed for consistent classification determinations. Of the above areas, mission ground stations are addressed separately in this report because of recommended changes in classification.

While all program classification guides addressed major subject areas and appear appropriate, several significant points surfaced during the review. First, each office presented classification details in differing formats. Secondly, additional detail is necessary to ensure consistency in the information addressed across NRO programs. These two points derive in part from the involvement of different system integration contractors and also in part from different Program Office perspectives concerning security issues in their unique environment. Such variation complicates rapid research to

address classification questions and answers. NRO classification and security guidance on subjects common to all programs was revised and expanded to resolve inconsistencies where possible.

OD&E/CIA recommended that its organization be acknowledged as part of the NRO at the SECRET/TALENT-KEYHOLE [redacted] level. This will require coordination and approval within CIA.

As technology and communications automate the tasking process of NRO systems, additional interfaces across the Intelligence Community underscore the requirement for consistency in system classification guides. In the past, NRO operations [redacted] however, operational information is needed by the user community for tasking purposes on a daily basis [redacted] This trend will continue in the future with the Requirements Management System (RMS) for imagery and in the Overhead Collection Management Center (OCMC) for SIGINT. In addition to classification guide changes, dictated by the review, a number of immediate and significant TALENT-KEYHOLE solutions were developed for tasking information [redacted] required by RMS and OCMC.

[redacted]

[redacted]

[redacted]

[redacted]

Handle via [redacted]
~~TALENT KEYHOLE/COMINT~~
Control Channels Jointly

[redacted]

Handle via [redacted]
TALENT-KEYHOLE/COMINT
Control Channels Jointly

[redacted]

[redacted]

Senior corporate leaders and security officers recognize the need for continuous security review to validate activities at the lowest classification level. They clearly understand the resource savings that accrue if they can reduce certification levels for facilities, computers or personnel to less than those required by DCI directives.

[redacted]

Handle via [redacted]
~~TALENT-KEYHOLE/COMINT~~
Control Channels Jointly

[redacted]

[redacted]

[redacted]

[redacted]

CONTRACTING AND INDUSTRY CONCERNS

Contracting and government security officers must review deliverable lists more closely to ensure that classification determinations are appropriate. Over the years, certain misperceptions resulted in deliverables of higher classification than necessary for the full scope of users. Program Office Contracting Officer's Technical Representatives (COTR's) [redacted] However, with proper security planning, deliverables [redacted] can be appropriately classified at the TALENT-KEYHOLE, collateral SECRET, or even unclassified levels. [redacted]

The senior contracting and security personnel of OD&E, SP and SPAWAR have agreed to a statement that accompanies certain efforts which indicates that deliverables lists have been reviewed by the COTR's and the project security officer with a full consideration of users. This check should result in lower classification determinations or a combination of deliverables such as a TALENT-KEYHOLE report with [redacted] In the current review, program offices were asked to examine existing deliverable lists, as well as those in planned requests for proposals.

Independent Research and Development (IR&D) presents similar security challenges and opportunities. Companies were found to frequently classify work at higher levels to obtain reviews by government technology engineers who would be knowledgeable of potential space reconnaissance applications. In the future, such work should be classified according to actual content, including a compartmented annex, if necessary. This approach would facilitate a "knowledgeable" review and technology transfer in US and potentially foreign efforts where appropriate.

Questions arose from industry concerning technology transfer. Contract provisions provide for release of information with contracting program office approval. With new economic pressures, procedures need to be re-examined, updated and

reissued. Such provisions were essential to avoid duplication of effort and provide a framework for interaction with [redacted] Contractors must provide a plan for security review and Program Office approval, if they desire to share facilities, show past performance or capabilities to government source selection panels, or bring out technology at equivalent, lower, or unclassified levels.

Contractors also expressed a desire that we continue to allow flexibility to tailor security to the particular company and its approach to protection. Thus, a TRW might have a different approach with a matrix structure than a LMSC or Martin Marietta.

NATIONAL SECURITY AGENCY

Issues affecting the relationship of NSA and the NRO center on delegation authority, differences [redacted]

[redacted]

Significant issues have arisen from the fact NSA [redacted] facilities were directed to follow NSA implementation rules which often conflict with DCI/NRO security provisions incorporated in NRO contracts. Discussions were held with those NSA personnel resident in our program offices and ground stations as well as personnel from M-5, G, P, Q, and R groups and the OCMC. Our main emphasis was to determine what [redacted] required by NSA and their contractors given the fact that the amount of information [redacted] was being

reduced. As a result of these meetings, the NRO recommendation was to place specific, [redacted] into NSA's Very Restricted Knowledge (VRK) COMINT compartments, and thus protect such information within TALENT-KEYHOLE and COMINT control. This would prevent conflicting operational security administration and control [redacted] as VRK offers an equivalent level of protection. However, NSA felt that such a separate access system would be too restrictive in that their contractors could not attend meetings and interface with NRO contractors.

SUMMARY

Information [redacted] has expanded over the years with the increased number of NRO satellite systems and a larger contractor base that supports the development, acquisition, and operation of satellites. The result has been a significant increase in numbers of people briefed [redacted] as TALENT-KEYHOLE.

This review and analysis of [redacted] is the first major zero base review undertaken by the NRO [redacted] involving program managers, engineers, security officers, and contractors. The effort has resulted in judgements that [redacted] To enhance classification management, program classification guides should be of a standardized format that adequately addresses all appropriate subject areas and are easily understood by the reader.

The need to articulate the rationale [redacted] is a 'lesson learned' essential for ongoing "top down" revisions. Those responsible for protection determinations need a litmus test or threshold approach to identify the specific damage [redacted] For example, technological lead time, surprise, uniqueness or capability need to be assessed as sources and methods protection issues for satellite reconnaissance development and operations. Computer data bases provide an excellent tool to look across NRO

satellites as well as DOD, civil and commercial capabilities. Such a tool enables a far more informed and accurate assessment of sources and methods concerns.

Inherent [redacted] is the ability to protect the indicators, and when necessary, the existence of activity. The tailored sources [redacted] enable a range of protection when applied to acquisition and operational activities. This flexibility, when required, provides an especially cost effective and powerful element of protection not readily available under other standard security control systems.

This security protection review must be an ongoing effort to refine, revise, and educate. This is due to the dynamic nature of the needs of the user community, new opportunities for tasking and dissemination, changing sensitivity of information and pressures on the industrial base in a time of austere and decreasing resources. Further, certain adjustments will be made as we revise classification/compartmentation of the NRO. NRO elements need to work closely with the CIO and SIGINT and MASINT committees as they refine their classification guidance. NRO has membership on the DCI Classification Standards Task Force headed by [redacted] representation on the National Industrial Security Program and input to Gen Scowcroft's (Ret) National Operations Security Review. As these activities converge, there will be opportunities to simplify, streamline, reduce classification, and educate, yet protect sources and methods necessary for the collection success of our systems.

ISSUES SUMMARY AND RECOMMENDATIONS

ISSUE: Maintain and Update Classification and Security Guidance.

This exhaustive security review has witnessed the formulation and update of program classification guides and the establishment of a technology data base that identifies specific satellite system components and activities and levels of protection. This effort must be kept current to protect essential technology and activities but also to recognize those areas where lower classification levels may apply. Updated security policy guidance and a current technology data base will aid program managers and security officers as they balance the costs and benefits of security with security risks.

RECOMMENDATION ONE: Annually or upon significant program change, each system program manager will update security and classification guidance. This will be maintained under a configuration control system. To facilitate usage, these guides should correspond to the general format of major subject categories that will be provided by the NRO Director of Security.

APPROVE [signature] DISAPPROVE _____

ISSUE: Classification/Protection Training

The review has highlighted the complexities of protecting NRO activities across the spectrum of research and development, acquisition, launch, and operations. Personnel engaged in NRO activities represent diverse communities, disciplines, and backgrounds with a wide variance in security training and experience.

RECOMMENDATION TWO: Within 90 days, the NRO Security Center, Training Staff will establish a classification/protection training program to educate members of the NRO community. The objective is for individuals to understand and apply the range of

protection measures required for NRO activities, [redacted]

[redacted]

APPROVE M. Jaya DISAPPROVE _____

ISSUE: Overclassification of Contract Deliverables.

The deliverables which result from our contracted efforts [redacted] when in fact, they could be protected at a TALENT-KEYHOLE, COMINT or non-compartmented level.

RECOMMENDATION THREE: For contracted deliverables of benefit to the user community, a certification procedure will be used by contracting officers technical representatives and program security officers to review deliverables lists and validate the appropriate level of classification. These procedures shall be implemented within 90 days.

APPROVE M Jaya DISAPPROVE _____

ISSUE: Overclassification of Contractor Independent Research and Development (IR&D).

This overclassification often results from the perception to obtain a "knowledgeable" government review of such effort. However, the higher classification may limit the audience and technology transfer considerations. Further, technology security reviews are later required to evaluate subsequent decompartmentation and declassification alternatives.

RECOMMENDATION FOUR: Formal security guidance will be issued by program contracting offices to all NRO contractors within 60 days, requiring that IR&D be conducted and documentedat the actual security level of the activity. When required,

annexes shall be for higher levels of classified applications.

APPROVE M Doyle DISAPPROVE _____

ISSUE: Precise Access Determination.

The increased use of [redacted] classification of NRO related activities should result in a reduced requirement for [redacted]

RECOMMENDATION FIVE: Within 90 days, the Director of Security, NRO in conjunction with the program offices, the DSPO, and the NRO Security Center Training staff, shall provide the user community with updated TALENT-KEYHOLE briefing materials and the NRO Classification and Security Guidance manual. This information will be used by government security officers and managers in formulating "must know" recommendations [redacted]

APPROVE M Doyle DISAPPROVE _____

ISSUE: [redacted]

[redacted]

[redacted]

APPROVE M Fuga DISAPPROVE _____

ISSUE: NSA Relationships

NSA requires selective national security space program information to accomplish its mission. However, major differences with NSA arise over whether such information for NSA-contracted efforts must [redacted] This highlights the need for resolving authorities and responsibilities for access determination [redacted]

RECOMMENDATION SEVEN: Within 60 days, the Director of Security, NRO, on-behalf of the DNRO, shall request that the NSA Office of Security identify the specific information [redacted] appropriate level of access.

APPROVE M Fuga DISAPPROVE _____

ORGANIZATIONS AND PERSONS BRIEFED ON REVIEW

U. S. Government

NRO Elements

NRO Board of Directors
Director, Program A
Director, Program B
Director, Program C
Director, P&A
Program A Elements - Program Offices, Contractors, and Security Staffs to include NSA members
Program B Elements [redacted] to include NSA member, [redacted]
Program C Elements - Senior Staff
P&A - Senior Management Group
[redacted] Panel
[redacted]
NRO Government Conference Working Group
[redacted]
NRO Staff to include members of COMIREX, SORS/SIGINT, and MASINT committees

CIA Elements

Director of Security
Collection Requirements and Evaluation Staff (CRES/DI)
NPIC Security and Policy Staff
Security Policy Division (O/S)

NSA Elements

Director of Security
M-5
R-3
G-3
Q-4
PO-5