~~TOP SECRET~~

4 August 1970

(b)(3)

MEMORANDUM FOR: Charles Roth

VIA :

SUBJECT : Security

The heavy expenditures associated with the privacy of returning image data from the NOI Imaging Satellites has lead to the following:

In the present budget environment, this writer believes a simple, workable scheme of obtaining images with minimum initial emphasis on image privacy is a legitimate goal. The frequency, data rate and type of modulation all give an interceptor a great deal of problems in extracting a bit stream from an intercepted signal. To tape record the signal after demodulation is a risky process (probably) even for much less an interceptor station. Serious expenditures must be undertaken to even attempt this process and this, in itself, is something of a security barrier.

The establishment of a single facility within 30-50 miles of D.C. to perform the functions of R/F, O/F and P/F with a single 85-foot antenna would yield the following advantages:

-Minimum initial expenditure

-System outputs available to be used for "marketing" (to EXCOM-NRO) of improvement programs to NOI.

-Simpler physical security

-Only one site and building to plan, construct and maintain.

-No 200 mile ground link to design, build and maintain.

-No family (if (wave) intercepted signals being used.

~~TOP SECRET~~

-No R/T-C/F interface (over 200 miles to be worked out).

-No image data encryption on I/S.

-Growth in several dimensions available.

-Much higher reliability.

-Fewer recorders and computers.

Inherent in this approach are the following disadvantages. Possible growth plans for alleviating these disadvantages are presented later.

-High signal strength for a interceptor located at Embassy of USSR.

-Moderate signal strength for a shipborne interceptor. Good strength in bad weather for us (and not for him).

-Large antenna (or radome) in a location that would be seen by more people (denser population) than at 200 miles from D.C. This shortens discovery time and could lead to penetration during construction.

-No back-up if antenna fails.

-No weather diversity.

-Suitable EMI-free site may be difficult to locate; URBAN R/F NOISE

-No fall back capability (except for TT&C) if single site or antenna is damaged.

As further financial commitments are made, the ROI system can be "beefed-up" (for data security purposes) as time goes on. This activity should be moderated by knowledge (or estimate) of the interception threat as that threat (presumably) grows. Detection of a regular ship-borne threat should be a relatively reliable process. An Embassy or Canadian threat would probably be more difficult to detect. Temporarily (or permanently) aiming the satellite antenna away from a threat is one very quickly accomplished action that will increase the interceptor's problem. It is free of financial impact. Other actions that should be considered are:

-Installation of image data encryption equipment on each I/S launched after the equipment is developed. Decryption gear then required at the receiver.

-Jamming of the interceptor by a plane over CONUS or a fixed clandestine station in downtown D.C.

-Construction of an R/F further from the threat which would become the primary receiving station when complete. Requires ground link, then. Now have back-up site for other considerations.

-Construction of an R/F just a few miles from the co-located facility to gain weather diversity. This then denies the shipborne threat the weather advantage. Also have back-up now.

(b)(1)
(b)(3)

(b)(3)