

~~SECRET~~

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON 25, D.C.



REPLY TO
ATTN OF:

AFOAC-S/O

SUBJECT:

Satellite to Ground Encryption

12 APR 1960

TO:

AFDRD-ER

1. The attached correspondence has been held in AFDAT without action. Confirming conversations between Major White of this office and Major Giraud, AFCIN, and between Major Giraud and Major Bensey of your office, it appears that if action is to be taken on this correspondence, it should come from your office.

2. Major Floyd, AFDAT Project Officer, is not available for consultation at this time, but he has expressed the fact that AFDAT does not want to establish a file on this subject.

3. This letter is unclassified when removed from attachments.

for Robert W. Paulson

ROBERT W. PAULSON
Colonel, USAF
Chief, Communications Systems Division
Directorate of Communications-Electronics

10 Atchs:

- 1. AF IN 50209 fm USAFSS (S)
- 2. AF OUT 64224 fm AFCIN-1C1 (S)
- 3. AF IN 15720 fm USAFSS (S)
- 4. AF IN 1414 fm AFBMD (U)
- 5. Ltr fm AFORQ-RN to AFDAT (S)
- 6. Ltr fm AFORQ-RN to AFCIN (S)
- 7. 1st Ind fm AFCIN-1C (S)
- 8. Ltr fm ECD to AFDRQ (S)
- 9. Ltr fm AFCIN-1C1 to AFORQ (S)
- 10. Ltr fm Sys Eng to W. Fromm (S)

5129

#8

~~SECRET~~

AT 7-352

~~CONFIDENTIAL~~

DEPARTMENT OF THE AIR FORCE
STAFF MESSAGE DIVISION

AF IN : 50209 (22 Jan 60) T/R/hph

ACTION: ORQ CHANGED TO (DAT) (Maj Floyd)(5 Feb 60)

INFO : OAC

AC - PARAPHRASE NOT REQUIRED EXCEPT PRIOR TO CATEGORY B ENCRYPTION
PHYSICALLY REMOVE ALL INTERNAL REFERENCES BY DATE TIME GROUP PRIOR
TO DECLASSIFICATION-NO UNCLASSIFIED REFERENCE IF THE DTG IS QUOTED
DE RJWFKW

R 212304Z

FM USAFSS

TO COFS USAF

BT

~~C O N F I D E N T I A L~~ FROM ECD/21-1-0212.

ACTION AFDRQ. PLEASE PASS TO AFOAC-S/C FOR INFO. REFERENCE

USAFSS LETTER, SUBJECT: ~~(C)~~ QUALITATIVE OPERATIONAL

REQUIREMENT FOR A SATELLITE-TO-GROUND ENCRYPTING DEVICE,

DATED 10 SEPTEMBER 1959. REQUEST THIS HEADQUARTERS BE

ADVISED OF STATUS OF ABOVE REFERENCED LTR.

BT

AFHQ 22 FORM JUN 56 0-309a

PREVIOUS EDITIONS OF THIS FORM
MAY BE USED. REPLACES AFHQ FORM
0-309F, 19 JAN 51, WHICH IS OB-
SOLETE.

~~CONFIDENTIAL~~

5129

~~2007~~ AT7-352
ATCH 1

JOINT MESSAGEFORM

SECURITY CLASSIFICATION

SECRET

SPACE BELONGS TO COMMUNICATION CENTER

Reproduction of this message in whole or in part is prohibited without approval of the office of primary interest. (See ROI 10-6)

PRECEDENCE	TYPE MSG (Check)			ACCOUNTING SYMBOL	ORIG. OR REFERS TO	CLASSIFICATION OF REFERENCE
ACTION	ROUTINE	BOOK	MULTI	SINGLE		
INFO				X	AF	

FROM: HQ USAF

SPECIAL INSTRUCTIONS

TO: AFEMD, LOS ANGELES, CALIF. INFO: COMUSAFSS

INT DISTRIBUTION

AFSS FT MEADE, MD. AFDAT (Maj Floyd)

~~SECRET~~ FROM AFCIN-1C. **64224**

AFEMD FOR WDZYD. AFSS FOR OOD. USAFSS PROVIDES CERTAIN RADINT SUPPORT FOR DISCOVERER. ASSUMING OTHER AFEMD SATELLITE PROJECTS FOR 1960 WILL ENTAIL SIMILAR REQUIREMENTS FOR AFSS RADINT SUPPORT, THE FOLLOWING INFORMATION IS REQUESTED: (A) PROJECTED SCHEDULE OF SATELLITE LAUNCHES. (B) FREQUENCIES FOR MONITORING INTEREST. (C) PROJECTED ORBITS. (D) ADDRESSEES FOR REPORTING AND REPORTING PRECEDENCE. (E) TYPE OF DATA REQUIRED FROM RADINT. RECEIPT OF THIS INFO WILL PERMIT ADVANCE PLANNING FOR SEARCH AND REPORTING PROCEDURES, PREPARING NECESSARY DIRECTIVES AND ESTIMATING ACTUAL SUPPORT AFSS CAN PROVIDE.

AC - PARAPHRASE NOT REQUIRED EXCEPT PRIOR TO CATEGORY B ENCRYPTION - PHYSICALLY REMOVE ALL INTERNAL REFERENCES BY DATE-TIME GROUP PRIOR TO DECLASSIFICATION - NO UNCLASSIFIED REFERENCE IF THE DATE-TIME GROUP IS QUOTED

2016 57 2

DATE	TIME
19	1545
MONTH	YEAR

5123

Floyd

WRITER	SYMBOL		SIGNATURE	
	AFCIN-1C1		<i>[Signature]</i>	
	TYPED NAME AND TITLE (Signature, if required)		TYPED (or stamped) NAME AND TITLE	
	GILBERT L. BRANDON, CAPT, USAF/med		JOHN M. FOW 1st Col, USAF Directorate of Collection AFSS/AF/10000000	
PHONE	PAGE NR.	NR. OF PAGES	5 3308 <i>Atch 1/2</i>	
75756	1	1		
SECURITY CLASSIFICATION		RELEASER		
SECRET		COPY 2 OF 5 CYS		

STAFF MESSAGE DIVISION
UNCLASSIFIED MESSAGE

AF IN

(1 Dec 59)

I N C O M I N G

X/W

ACTION: DAT

INFO : CIN CGM
SMD A 061

HQDD 6ZCQJB167

PP RJEZHQ

DE RJWZBK 14

P 302326Z

FM AFBMD LOSA CALIF

TO COFS HQUSAF

BT

UNCLAS FROM WDZYO 11-6-E FOR AFDAT AND AFCIN BASED ON THE VICE CHIEF OF STAFF LETTER CMM DATED 5 AUG 59 CMM SUBJECT CLN ASSIGNMENT OF OPERATIONAL PLANNING RESPONSIBILITY WE HAVE DETERMINED THAT CMM WITH THE FOLLOWING EXCEPTIONS CMM ALL SAMOS INFORMATION IS SECRET. THESE EXCEPTIONS CMM WHICH WOULD CONTINUE TO BE TOP SECRET ARE /1/ SPECIFIC DATE OF LAUNCH/SPECIFIC PAYLOAD CONFIGURATION AND MISSION ASSIGNMENT CMM WHEN IDENTIFIED TOGETHER /2/ RESULTS AND EFFECTIVENESS OF RECONNAISSANCE SATELLITE DATA WHEN PROCESSED AND REDUCED TO USEABLE FORMAT. REQUEST CONFIRMATION OR CORRECTION TO THIS INTERPRETATION

BT

01/0042Z DEC RJWZBK

DEPARTMENT OF THE AIR FORCE
STAFF MESSAGE DIVISION
UNCLASSIFIED MESSAGE

I N C O M I N G

CIN

M G

SA

D

Z C

100

BT

6

6 Q

~~SECRET~~

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON 25, D.C.



REPLY TO: AFORQ-RN
ATTN OF:

OCT 28 1959

SUBJECT: (U) SAMOS

TO: AFDAT

1. References:

- a. GOR 80-2, paragraph K.l.a.
- b. QOR for Satellite-to-Ground Encrypting Device, USAFSS, dtd 11 Sep 59, with indorsement by AFCIN, dtd 16 Oct 59. (Atch #1)
- c. Letter from AFCIN, Encryption Device for SAMOS, dtd 16 Oct 59, with attachment. (Atch #2)

2. The requirement for secure transmission of data from the electro-magnetic version of SAMOS is concurred in by this office and was included in paragraph K.l.a. of GOR 80-2 on 26 Sep 58.

3. Since the GOR already states the basic requirement covered by USAFSS in their QOR, no amendment to the GOR is deemed necessary.

4. Recommend developmental action to insure compliance with the QOR be initiated by your office.

Fred W. Dyer

FRED W. DYER
Colonel, USAF
Chief, Reconnaissance Division
D/Operational Requirements

- 2 Atchs
- 1. Ltr to AFCIN, 17 Sep 59, QOR for a Satellite-to-Ground Encrypting Device, and 1st Ind fr AFCIN, 16 Oct 59, same subj (SS: 8271) Orig & 1 cc, 1 pg ea; w/USAFSS Ltr, 11 Sep 59, same subj, Orig & 1 cc, 2 pgs ea (SS: 7172)
- 2. Ltr fr AFCIN-1C1, 16 Oct 59, Encryption Device for SAMOS, Orig & 1 cc, 1 pg ea; w/Memo dtd 14 Oct 59, Orig & 1 cc, 3 pgs ea (SS: 8272)

Copy to: AFCIN-1C

~~SECRET~~

5180

5510 477-352
Atch 5

SECRET

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON 25, D.C.



2 Oct 59

X3

SEP 17 1959

REPLY TO
ATTN OF: AFORQ-RN

SUBJECT: (C) Qualitative Operational Requirement for a Satellite-to-Ground Encrypting Device

TO: AFCIN

Request your comments on the attached letter per routing by originator.

James A. Shannon
JAMES A. SHANNON
Lt Col, USAF

Deputy Chief, Reconnaissance Group
D/of Operational Requirements

1 Atch
USAFSS Ltr, dtd 11 Sep 59,
subj as abv, Orig & 2 cc,
2 pgs (S)

5120

SECRET

Atch 6
91368 AT7-352 5900

~~SECRET~~

Ltr, AFOAC-S/O, Subject: (U) Satellite to Ground Encryption

JUL 14 1960

1st Ind (AFDRT-ER)

TO: AFORQ-RN

The requirement expressed in the Security QOR for SAMOS has been overtaken by events. Specifically, there are no known plans for operation beyond vehicles containing the F-2 sub-system. The program for vehicles containing sub-systems F-1 and F-2 could not be delayed to satisfy the security requirement.

Cloyd H. Drey
CLOYD H. DREY, Colonel, USAF
Directorate of Research & Technology

10 Atchs
n/c

*Any further correspondence on
this matter should be addressed to AFDSD.
—CHD*

*RW
SS 5751*

~~CONFIDENTIAL~~
When separated from
classified enclosures

~~SECRET~~

Doc - 7-298

1A77-352

~~SECRET~~

Ltr, AFOAG-S/O, Subject: (U) Satellite to Ground Encryption

1st Ind (AFDRT-ER)

001 14 1960

TO: AFORQ-RN

The requirement expressed in the Security QOR for SAMDS has been overtaken by events. Specifically, there are no known plans for operation beyond vehicles containing the F-2 sub-system. The program for vehicles containing sub-systems F-1 and F-2 could not be delayed to satisfy the security requirement.

CLOYD H. DEREY, Colonel, USAF
Directorate of Research & Technology

10 Atchs
n/c

REGRADED ~~CONFIDENTIAL~~
when separated from
classified enclosures

~~SECRET~~

AT 7-352

Ltr fr. AFORQ-RN dtd 17 Sep 59, subj: (C) Qualitative Operational Requirement for a Satellite-to-Ground Encrypting Device.

1st Ind (AFCIN-1C)

Headquarters USAF, Washington 25, D.C.

16 OCT 1959

TO: AFORQ-RN

1. The QOR set forth in basic communication is supported and concurred in. The developments of the capability identified in this QOR in relation to SAMOS should not, however, delay or impede programmed flights of vehicles containing the F-1, F-2, F-3 or F-3a sub-systems. Development of this QOR should be programmed into F-4 and follow-on vehicles. Satisfaction of this QOR might also have some applicability in securing the man-in-space program.
2. It is believed that this device should be incorporated into the requirements for sub-system H.
3. AFBMD is being queried as to bit-rate of both digital and analog data to be transmitted from satellite to ground in all sub-system F vehicles. Your office will be furnished the information immediately upon receipt. This information will furnish guidance and realistic requirements for the development of encryption devices.



50X1

Harold Watson

1 Atch
n/c except 1 cy w/d

HAROLD E. WATSON
MAJOR GENERAL, USAF
DEPUTY ASSISTANT CHIEF OF STAFF,
INTELLIGENCE

RN
SS 8271

5129

~~SECRET~~

CIN 1235

Atch 7
AJ 7-352

~~SECRET~~

R-0-1888-3

ST-J-1-331

MEMO TO: W. Fromm

FROM: Systems Engineering

DATE: 14 October 1959

SUBJECT: F-1, F-2, and F-3 Vehicle Output Data Characteristics

This memo documents the characteristics of the output digital word from the F-1, F-2, and F-3 vehicles.

F-1 Vehicle Digital Word Data

Bit Rate:	8Kc $\pm 5\%$ (from recorder) 4Kc nominal (real time readout)
Word Length:	48 bits
Spacing between Words:	24 bit minimum
Bit Width:	62 ± 12 microseconds
Amplitude:	"one" bit level $\pm 6V$ to $\pm 12V$. (8V nominal) "zero" bit level $-6V$ to $-12V$ ($-8V$ nominal)
Signal form:	Three level return to zero.

F-2A and F-2B Vehicle Digital Word Data

Bit Rate:	10Kc $\pm 20\%$
Word Length:	50 bits and 5 milliseconds $\pm 20\%$
Spacing between Words:	3.8 to 10 milliseconds
Bit Length:	100 microsecond $\pm 20\%$ from the leading edge of one bit to the leading edge of the following bit.
Duty Cycle per Bit:	40 to 65%
Amplitude:	"one" bit level, $\pm 6V$ $\pm 10\%$ "zero" bit level, $-6V$ $\pm 10\%$

F-3A and F-3B Vehicle Digital Data Output of Digital Recorder

Bit Rate:	10Kc $\pm 20\%$
Word Length:	68 bits and 6.8 milliseconds $\pm 20\%$
Spacing between Words:	3.8 to 10 milliseconds

5129

~~SECRET~~

AT 7-352 ALCh 10

~~SECRET~~

Bit Length: 100 microseconds $\pm 20\%$ from the leading edge of one bit to the leading edge of the following bit.

Duty Cycle per Bit: 40 to 65%

Amplitude: "one" bit level, +6V $\pm 10\%$
"zero" bit level, -6V $\pm 10\%$

Signal Form: Three level return to zero.

F-3A Vehicle Digital Track Output of Analogue Recorder (double speed readout only)

Bit Rate: 20Kc $\pm 1\%$

Word Length: 68 bit and 3.4 milliseconds nominal

Spacing between Words: 4 milliseconds minimum

Bit Width: 20 to 30 microseconds

Amplitude: "one" bit level, +6V $\pm 10\%$
"zero" bit level, -6V $\pm 10\%$

Signal Form: Three level return to zero

F-3B Vehicle Digital Track Output of Analogue Recorder (single speed readout)

Bit Rate: 10Kc $\pm 1\%$

Word Length: 68 bit and 6.8 milliseconds nominal

Spacing between Words: 8 milliseconds minimum

Bit Width: 40 to 60 microseconds

Amplitude: "one" bit level +6V $\pm 10\%$
"zero" bit level -6V $\pm 10\%$

Signal Form: Three level return to zero

F-3A Vehicle Analogue Output of Analogue Recorder (double speed readout)

Performance figures are not available for the vehicle recorder only. Data below is for a vehicle-ground recording system. Since the vehicle recorder is read out at double speed, the frequency characteristics are at least double those stated below:

System Frequency Response: The overall frequency response of the system is such that for an input signal flat from 30 cps to 100Kc, the reproduced output signal is flat within ± 0.5 db to -1.5 db with respect to the response obtained at 30 Kc.

~~SECRET~~

ATD-350

~~SECRET~~

Signal to Noise Ratio: The signal to noise ratio of the airborne unit is less than 40 db peak to peak signal to RMS noise measured over the full reproduced band width.

Output Signal Amplitude: 1.2V peak to peak maximum

Outputs: Two analogue tracks are read out simultaneously.

F-3B Analogue Output of Analogue Recorder (single speed readout)

Frequency Response: 12 Mc wide from 1 to 13 Mc

Signal to Noise Ratio: The signal to noise ratio of recording system consisting of the vehicle recorder and its complementary ground recorder is no less than 35 db peak to peak signal to RMS noise measured over the full specified bandwidth.

Output signal Amplitude: 2V peak-to-peak, nominal

F-3B Signal Characteristics

The signal played back by the airborne unit is a composite and compounded signal requiring two channels each 12 Mc wide for transmission to the ground unit. The output from two alternate heads on the scanning wheel of the recorder are switched to one transmission channel; that from the other two alternate heads on the scanning wheel are switched to the other channel. In other words, the output from heads 1 and 3 is carried by channel A and that from 2 and 4 is on channel B. This gives a time sequence of 1-A, 2-B, 3-A, 4B, 1-A, 2-B, etc. There are overlap periods between the channels corresponding to the overlap periods on the tape. These overlap periods accommodate the time reference bursts. The time reference consists of 25 usec bursts of a 4 Mc time at the start and end of each segment of data. The data is frequency modulated with a center frequency of 8 Mc and sidebands extending from 1 Mc to 13 Mc. Each segment of data plus time reference lasts approximately 725 usec. The black period between segment is approximately 525 usec.

F. Tenenbaum

FT/GS/jhs

cc: F. Tenenbaum (6 copies)
J. P. Thompson

~~SECRET~~

AT 7-352

AFDSD-AT/ J. Howard sas 71791/8 Aug 60

AFDSD-AT

AUG 10 1960

Encryption Device for SAMOS

Commander, ARDC, Andrews AFB, Maryland

1. Reference USAFSS QOR, dated 11 September 1959, USAFSS message ECD 19-7-241, dated 20 July 1960, and related correspondence (attached).
2. It is requested that ARDC analyze these requirements and inform this headquarters as soon as practicable the scope of the development effort required, schedule, and estimate of the cost to provide this capability in the SAMOS program.

FOR THE CHIEF OF STAFF

- 4 Atch
1. QOR, dtd 11 Sept 59
 2. Ltr fr AFCIN to AFORQ, dtd 16 Oct 59
 3. AF IN 15720, dtd 15 Dec 59
 4. AF IN 53464, dtd 20 Jul 60

JOHN D. MARTIN, JR.
 Colonel, USAF
 Deputy Assistant for Advanced
 Technology, DCS/Development

COORDINATION: AFDSD-AT
 Mr. Howard

AFORQ-RN

AFCIN-1C1

SEP 6

9 JAN 1

AB

Howard a

AFDSD-AT
19 0 0

~~SECRET~~

HEADQUARTERS
UNITED STATES AIR FORCE SECURITY SERVICE
SAN ANTONIO, TEXAS



11 September 1959

REPLY TO
ATTN OF: 4 CD

SUBJECT:

~~(CONFIDENTIAL)~~ Qualitative Operational Requirement for a Satellite-to-Ground Encrypting Device

Hq USAF (AFDRQ)
Wash, D. C.

THRU: Hq USAF (AFCIN)

1. ~~(CONFIDENTIAL)~~ Introduction: This qualitative operational requirement pertains to the operational support of WS-117L and is being submitted in accordance with Air Force Regulation 57-3, dated 15 May 1956.
2. ~~(SECRET)~~ Activity of Originating Organization Affected by the Proposed Equipment: In support of this headquarters' intelligence gathering mission, a requirement exists for a satellite-to-ground encrypting device(s) to be used on proposed modification of SAMOS (previously BENTRY) Subsystem F. The proposed modifications were discussed at a meeting on 13 August 1959 at Wright-Patterson AFB by Hq USAF (AFCIN), ATIC, SAC, and USAFSS. Subject of the meeting was redirection of the SAMOS program to include a COMINT collection capability. It was agreed by all parties that a satellite COMINT collection capability would be highly desirable, however, a definite decision as to when the COMINT integration will be accomplished or the degree of the integration has not been reached as of the date of this QOR.
3. ~~(CONFIDENTIAL)~~ Present Capability to Accomplish the Function: This headquarters is not aware of any existing device which can accomplish a satellite-to-ground encrypting function. To our knowledge, no formal requirements have been placed on the National Security Agency to develop such a device, however, available information indicates NSA is working on the development of a satellite encrypting device as an internal NSA project. It is not known whether or not the National Security Agency device will fulfill the WS-117L requirement.
4. ~~(SECRET)~~ Effect of Equipment Deficiency: An operational capability of a satellite-ground encrypting device is desired by October 1960. Integration of COMINT capability into the SAMOS program is totally dependent upon the ability to secure transmission of the intelligence information from the satellite to the ground tracking and acquisition stations. Until an encryption capability is obtained, the COMINT function cannot be integrated into the Subsystem F program.
5. ~~(SECRET)~~ Employment: If such a device can be developed by October 1960, it is probable that the device or modifications thereof would be used on all F series vehicles launched after that date. Present

~~SECRET~~

3310

ATTN-352

Atch 1²

~~SECRET~~

Intentions are to integrate a COMINT function into the SAMOS program gradually, so it appears that the COMINT system will utilize the existing ELINT collection and transmission system with minor modifications. Under such conditions, the encryption device would serve a dual purpose in that it would be able to encrypt the ELINT information from the vehicle also. To date, no provisions have been made to encrypt the ELINT information for transmission from satellite to ground.

6. ~~(SECRET)~~ Performance Capabilities Required: The encryption device must be compatible with the existing WS-117L SAMOS Subsystem F collection-transmission system. It must also be compatible with the eventual modifications induced by integration of a COMINT collection capability. Since a decision on the degree of integration to be performed on any specific SAMOS vehicle has not yet been reached, USAFSS will supply NSA with information on specific performance capabilities required of the encryption device as the project develops and exact requirements become known.

7. ~~(SECRET)~~ Additional Performance Capabilities Desired: To provide maximum flexibility, the encryption device should be developed on a modular construction basis and be multipurpose rather than specialized, if such versatility can be obtained without a serious time sacrifice. The modular construction characteristic is desirable as the SAMOS program will have an encryption requirement for different rates of signal encryption as the program progresses and additional reconnaissance capabilities are developed. Although the initial encryption requirement is for a digital type signal, an eventual analog encryption capability is also desired.

FOR THE COMMANDER:

CORNELIUS E. McBRAYER
Colonel, USAF
DCS/Communications-Electronics

~~SECRET~~

~~SECRET~~

16 OCT 1959

AFCIN-1C1

Encryption Device for SAMOS

AFORQ (Maj Spence)

1. In accordance with telephone conversation of 14 October, forwarded herewith is Digital and Analogous Output for Subsystem F SAMOS.
2. It is believed that this information will be valuable in determining the definitive requirements for the QOR submitted by USAFSS for an encryption device for Subsystem F. SAMOS.

JOHN E. POE
Lt Colonel, USAF
Directorate of Collections
ACS/Intelligence

1 Atch
Ref paper (2 cys)

~~SECRET~~

AT 7-352

Ack 92

Ltr, AFOAC-S/O, 12 Apr 60, (U) Satellite to Ground Encryption

27 JUL 1960

2nd Ind (AFORQ-RN)

TO: AFDSO-AT

1. Do not concur that this requirement has been overtaken by events. Although the F system launch schedule has been reduced, this office knows of no current guidance which implies cessation of R&D to meet the specified (SOR 80-2) ELINT and COMINT objectives.
2. Request you proceed to include the capability covered in the USAFSS QOR in the development program, since this capability is already stated as a requirement in SOR 80-2.
3. Your attention is invited to the attached secret message from USAFSS, cite 19-7-241, dated 20 July. Request you take action on this message for the reasons stated in paragraph 2 above.

Fred W. Dyer
 FRED W. DYER
 Colonel, USAF
 Chief, Reconnaissance Division
 D/Operational Requirements

11 Atch
 1 - 10 n/c
 Added 1 atch
 11. AF IN 53464 USAFSS 20 Jul 60

Mr Dave Welford 188 X 7557
H/c Charles Reynolds X 7181

Info by Dir NSA

SS 5751

~~SECRET~~

~~SECRET~~DEPARTMENT OF THE AIR FORCE
STAFF MESSAGE DIVISION

AF IN : 53464 (20 Jul 60) D/aly

ACTION: ORQ

INFO : OAC, CIN

DE RJWFKW 188
R M 192243Z ZEX
FM USAFSS SAN ANTONIO TEX
TO RJEZHQ/COFS USAF WASH D C
INFO RJEZFF/ARDC ANDREWS AFB MD
RJWZBK/AFBMD INGLEWOOD CALIF
BT~~SECRET~~ FROM ECD; 19-7-241.

ACTION FOR USEF (AFORQ), INFO FOR USAF (AFOAC-5/C) AND

(AFCIN 1-C), ARDC, AFBMD FOR MAJOR COPLEY AND NSA (CSEC).

SUBJECT: SAMOS F-2 ENCRYPTION. THIS MESSAGE IN THREE PARTS.

PART 1. THIS HEADQUARTERS HAS DEVELOPED A PROPOSAL FOR A COMMUNICATION SECURITY SYSTEM FOR SAMOS F-2 DIGITAL TRANSMISSIONS WHICH WOULD ALLEVIATE SAMOS COMSEC PROBLEMS UNTIL SATELLITE KEY GENERATORS CAN BE DEVELOPED. BASICALLY, THE SYSTEM CONSISTS OF USING TWO CHANNELS OF THE EXISTING SAMOS F-2 TAPE RECORDER TO STORE AND GENERATE KEY STREAM INFORMATION. KEY WORDS THE SAME LENGTH AS THE DATA WORDS WOULD BE STORED ON THE KEY CHANNELS IN TAPE SPACE SYNCHRONIZATION WITH THE INTERCEPT WORDS ON THE DATA CHANNEL. THE TWO CHANNELS WOULD THEN BE ADDED TOGETHER PRIOR TO TRANSMISSION TO PROVIDE COMMUNICATION SECURITY. THE MAIN ADVANTAGE OF SUCH A SYSTEM IS

(Reproduction of this Message in whole or in part is prohibited without approval of
THE OFFICE OF PRIMARY INTEREST.)

AFHQ FORM 0-309b

PREVIOUS EDITIONS OF THIS FORM MAY BE USED

~~SECRET~~

COPY NO.

atol #4

~~SECRET~~DEPARTMENT OF THE AIR FORCE
STAFF MESSAGE DIVISION

AF IN 53464 (20 Jul 60)

THAT THE ONLY ADDITIONAL SYSTEM CIRCUITRY REQUIRED IN THE SATELLITE WOULD BE THAT NECESSARY TO ADD THE KEY STREAM WORDS TO THE INTERCEPT WORDS AND THAT NECESSARY TO GENERATE NEW KEY WORDS FROM THE OLD KEY WORDS BETWEEN VEHICLE READOUTSM IT WOULD ALSO BE HIGHLY DESIRABLE TO INCLUDE A SWITCH-OUT CAPABILITY ON THE COMSEC SYSTEM IN ORDER TO MINIMIZE ITS EFFECT ON THE OVERALL SAMOS RELIABILITYM PART II. BOTH NSA AND LOCKHEED WHO IS THE SAMOS PRIME CONTRACTOR HAVE BEEN APPROACHED FOR OPINIONS AND COMMENTS ON THE ABOVE PROPOSALM LOCKHEED, AFTER MAKING A PRELIMINARY ANALYSIS OF THE MODIFICATIONS INVOLVED, STATED THAT THERE WOULD BE NO PROHIBITIVE TECHNICAL DIFFICULTIES IN IMPLEMENTING THE RECORDED KEY STREAM SYSTEMM NSA, IN A MESSAGE TO THIS HEADQUARTERS, CSEC 222, DATED 14 JULY 1960, STATED THAT THE PROPOSAL - QUOTE "APPEARS TO HAVE SOME MERIT AS AN INTERIM PROPOSAL" UNQUOTE. HOWEVER, THEY ALSO STATED THAT THEY HAD RECEIVED NO OFFICIAL STATEMENT OF REQUIREMENT FOR PROTECTION OF SAMOS DATXAM PART III. AFCIN, IN A MESSAGE TO THIS HEADQUARTERS, WINIC 0019, DATED 5 JAN 60, CONCURRED WITH DIRNSA LETTER, 14 OCT 1959, TO AGS/I RECOMMENDING THAT - QUOTE "WE SHOULD NOT RETARD INTEGRATION OF COMINT INTO SUBSYSTEM F THROUGH ANY INITIAL REQUIREMENTS FOR ENCRYPTION" UNQUOTE. THIS HEADQ ARTERS

(Reproduction of this message in whole or in part is prohibited without approval of
THE OFFICE OF PRIMARY INTEREST.)

Page 2 of 3

AFHQ FORM 0-309b

PREVIOUS EDITIONS OF THIS FORM MAY BE USED.

~~SECRET~~

COPY NO.

~~SECRET~~DEPARTMENT OF THE AIR FORCE
STAFF MESSAGE DIVISION

AF IN : 53464 (20 Jul 60)

STILL CONCURS WITH THIS POLICY, HOWEVER, WE ARE OF THE OPINION THAT SAMOS F-2 DATA TRANSMISSIONS SHOULD BE SECURED IF A PRACTICAL ENCRYPTION CAPABILITY EXISTS. IT IS RECOGNIZED THAT A FACT BASED DECISION AS TO WHETHER OR NOT A COMSEC SYSTEM SHOULD BE INCLUDED ON FAW FLIGHTS CANNOT BE MADE AT THIS TIME. THEREFORE, IT IS RECOMMENDED THAT NSA BE REQUESTED TO TECHNICALLY ASSIST LOCKHEED MISSILE SYSTEMS DIVISION IN DETERMINING EXACTLY WHAT ADDITIONAL CIRCUITRY WOULD BE REQUIRED IN THE SATELLITE AND AT THE GROUND STATION TO INCLUDE THE ABOVE PROPOSED ENCRYPTION SYSTEM. THIS WOULD ALSO INCLUDE A DETERMINATION OF SPECIFIC SIZE, WEIGHT, POWER REQUIREMENT, AND RELIABILITY AS IT AFFECTS THE OVERALL SAMOS SYSTEM. THE FINAL DECISION ON IMPLEMENTATION COULD THEN BE DRAWN FROM THE RESULTS OF THE EVALUATION UNDER IDEAL CONDITIONS, IT WOULD BE DESIRABLE TO INCLUDE COMSEC

SYSTEM ON THE SECOND FAW FLIGHT IN OCTOBER 1961; HOWEVER, IMPLEMENTATION BY THAT DATE WILL REQUIRE IMMEDIATE DEVELOPMENT ACTION. REQUEST YOUR COMMENTS AND/OR CONCURRENCE

BT

19/2322Z JUL RJWFKW

(Reproduction of this message in whole or in part is prohibited without approval of
THE OFFICE OF PRIMARY INTEREST.)

Page 3 of 3

AFHQ FORM 0-309b
22 JUN 56

PREVIOUS EDITIONS OF THIS FORM MAY BE USED.

~~SECRET~~

COPY NO.

NNNN