Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

CONFIDENTIAL

OCC-M-78- 166

MEMORANDUM FOR: Director of Data Processing

25X1A FROM : [redacted]
Chairman, OS/OC Security Review Committee

SUBJECT : Security Review of SAFE Proposals (U)

1. (U/AIUO) Attached are the findings of the Security Committee Review for the SAFE proposals submitted by [redacted] 25X1A
25X1A [redacted] It is the recommendation of the Security Working Group that the BLACK system bus architecture be selected for the SAFE program.

2. (C) The three key factors which impact the conclusions and recommendations for the report are:

a. The totality of sensitive data on a RED bus,

b. The budgetary constraints for a labor intensive on-going line surveillance program deemed essential for a RED bus,

c. The advancement of the state-of-the-art anticipated in the field of microminiature technical collection equipment.

3. (U/AIUO) We, ODP/OC/OS, are entering the next generation of information handling within the Agency and within the Intelligence Community. It is imperative that crucial decisions be made at the entry point to obviate the recognized expense of retrofits.

25X1A
[redacted]

Attachment:
As Stated

E2, IMPDET CL BY: 390969

CONFIDENTIAL

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

25X1A
Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Next 3 Page(s) In Document Exempt

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

SECURITY EVALUATION:

SAFE Communications

Architecture Reports

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

STATINTL
Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Next 3 Page(s) In Document Exempt

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

SECURITY EVALUATION:

SAFE Communications

Architecture Reports

31 MAR 1978

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

EXECUTIVE SUMMARY

25X1A

The Security Review Committee, comprised of Office of Security and Office of Communications representatives, have reviewed [redacted] studies for the SAFE program. The multi-discipline background of the members of this committee run the gambit of Office of Security officers with intimate experience and responsibilities for protecting the Agency's Information Systems and Classified Information, with expertise in technical countermeasures for wireline protection; and Communications Security officers who have the prime responsibility for protecting the data flow of Agency information.

It is the position of this committee that the BLACK communications architecture is necessary to protect the information currently anticipated to be flowing within this system.

This is based on an appraisal of the threat/risk to the information. The classification level of information and its sensitivity mandates the highest level of protection. The difficulty of providing a high level of security in a RED system, its estimated resource costs both financial and human, long and short, further support this position.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

TABLE OF CONTENTS

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

I. INTRODUCTION

This report provides a security evaluation of the SAFE RED and BLACK communications architectures provided 25X1A by [redacted] It contains recommendations for selection of an adequately secure architecture.

A. BACKGROUND

To fulfill the requirements of SAFE, an unprecedented volume of data including Top Secret, Sensitive Compartmented Information (SCI) and Community proprietary material will be distributed 25X1A via a data communication system to approximately [redacted] users. A system which from the start appeared able to handle SAFE's complex communication system was the RF Bus Wide Band Communication System (WBCS). 25X1A This system was investigated by [redacted] under an ORD Feasibility Study, and has been adopted as the design for SAFE. Although the WBCS has numerous operational advantages, it requires high level security protection because all data flows to all points on the bus.

The concept of a communication trade-off study was formulated at the time of the SAFE Request For Proposal (RFP) to allow flexibility in providing the required security protection for the SAFE data. Two approaches were proposed: RED and BLACK. A plain text RED system would rely heavily on physical security devices and TEMPEST protection techniques. A BLACK system would derive its security from encryption. The contractors were directed to pursue the design of both a RED and a BLACK architecture to a point where meaningful comparisons could be made by the Government and a preferred architecture chosen. This point in time has now been reached.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

B. OBJECTIVES

The objectives of the OS/COMSEC Working Group were to evaluate both contractors' proposed systems and their security features for security adequacy and cost. In order to estimate the degree of security required for the SAFE Communications System and then determine how well the proposed systems met these requirements, it was necessary for the Working Group to first assess the threats to which the SAFE Communications System would be subjected. Next, the communications systems were analyzed for vulnerabilities in their designs. Costs included not only one-time costs of designing and implementing the security features, but also the continuing costs and manpower requirements to sustain the required security protection. Finally, security countermeasures had to be identified to correct the weaknesses in an acceptable manner.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

25X1A

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Next 1 Page(s) In Document Exempt

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

III. RED/BLACK COMPARISON

A. PREREQUISITES

There are certain prerequisites that must be considered before addressing the two types of architectures, RED and BLACK. These are minimum standards which must be met by any system which is installed.

1. It is a requirement that high grade cryptographic key generators be used to protect inter-building links.

2. If a RED system is installed, the Security Standards for Classified Plain Text Distribution in the Headquarters Building and the Security Standards for Classified Plain Text Distribution in Outside Buildings must be adhered to. Also, NACSEM 5100 requirements (TEMPEST) must be met for all terminals and the cable distribution system.

3. If a BLACK architecture is implemented a high grade cryptographic algorithm must be used in the cryptographic module (CM) in a cost effective manner. This is feasible by the omission of certain alarms, checks, and security failure analysis. The TEMPEST requirements imposed by Chapter 6 of KAG-30 will be applied to the CM. NACSEM 5100 requirements will be applied to the BLACK terminals. MIL-STANDARD 461 requirements will be applied to the cable distribution system.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

B. RATIONALE

The rationale for the evaluation of the proposals was to determine what security protection is required for various types of installations and then ascertain what approved countermeasures could be used to reduce the degree of risk to an acceptable level. Only those techniques presently employed by the Office of Security were considered since no new physical security techniques were addressed by either contractor.

For the RED installation, all BIU's, amplifiers, splitters and taps must be locked and alarmed. In addition, the terminals must be locked to prevent unauthorized access to the system. The possibility of constructing special purpose vaults to protect the rooms which house terminals vice alarming individual terminals was investigated and the cost was found to be prohibitive. The idea of placing the terminals in safes, as is presently done for some cryptographic systems, was also considered and found to be too expensive in addition to being inconvenient for the operator. We concluded that individual alarms were cost effective and included only the minimum number of alarms necessary to isolate a problem to a reasonably small physical area ensuring an acceptable alarm response time. This approach provides security protection while allowing the SAFE operators to work in a standard office environment.

For the BLACK installation, only the cryptographic module and terminal must be protected. For simplicity of installation it is recommended that the CM be integrated into the terminal or work station. The required protection for the CM and terminal in a BLACK System is a strengthened cabinet and lock.

For a BLACK System, the Automatic Key Distribution Center (AKDC) and the other centralized cryptographic functions must be in a privacy area within the computer center, which will meet the criteria for a Special Purpose Vault. Another requirement on the AKDC is that nobody is allowed in the area alone; also referred to as two-man control.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

IV. COSTS

A. GENERAL

For the purpose of evaluating the costs associated with either a RED or BLACK communications architecture one must look not only at the systems costs presented by the two contractors, but also the added costs of providing the requisite security protection for the system. The following is an analysis of the added security hardware costs and resource impact for meeting requisite security protection.

25X1A

B. [redacted] SYSTEMS COST ESTIMATES

25X1A

The [redacted] System architecture is configured so that the bus runs only as far as the electrical closets where the BIU and cluster units are located. The data is then distributed to each work station via individual twisted pair cabling. It should be noted that only the data to and from an individual terminal is available to an intruder on each pair of twisted wire. The security protection required is, thus, similar to that provided today. Table 1 enumerates the items that require protection, indicates the quantity of devices to be protected, and designates the security measures and the associated costs for both the RED and BLACK systems. Table 2 provides the computation data for the added physical and technical security protection required for the G.E. RED system. Table 3 provides the computation data for similarly protecting the [redacted] BLACK system. It should be noted that the quantities used were based on information provided by the contractor and the experience of the working group. No security costs for outside buildings have been included in this cost estimate. The unit cost of physical and technical security protection in outbuildings may be higher than that required in the Headquarters environment.

25X1A

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

CONFIDENTIAL

TABLE 1

HARDWARE COST OF SECURITY MEASURES FOR 25X1A [redacted] SYSTEM

	ITEM BEING SECURED	QUANTITY	SECURITY MEASURE	UNIT COST RED	UNIT COST BLACK
1.	Single I/O Device SAFE Terminal Regional Printer ADSTAR Terminal	1663 121 900	Cabinet lock and increased strength of cabinet	$ 100	$100
2.	BIU or BIU Extenders	45	Contact switch alarm in existing elect. closet with twisted shielded pair to a monitor	100	
			Cabinet Lock	20	
				120	0
3.	Workstation Cluster	N/A	N/A, since BIU's located in closets	0	0
4.	Splitter Tap	95 18	Contact switch alarm in existing elect. closet with twisted shielded pair to a monitor	100	
			Cabinet Lock	20	0
				120	0
5.	Coaxial Bus Amplifiers enclosure	2	Contact switch alarm in existing elect. closet with twisted shielded pair to a monitor	100	
			Cabinet Lock	20	
				120	0
6.	Coaxial Cable Pullbox	41	Contact switch alarm outside existing elect. elect closet with a twisted shielded pair to a monitor	1350	
			Cabinet Lock	20	
				1370	0
7.	Twisted Pair From BIU to I/O Device	N/A	N/A twisted pair in floor cells will not require additional costs	0	0

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

25X1A

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Next 1 Page(s) In Document Exempt

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

25X1A

C. [redacted] SYSTEMS COST ESTIMATE

25X1A

The [redacted] system architecture is configured so that the bus runs all the way to the BIU which will be located in the work station area. The transmission path is coaxial cable. This necessitates providing protection for the system wherever the bus data is available to an intruder. Table 4 enumerates the items that require protection, indicates the quantity of devices to be protected, and designates the security measures and the associated costs for both the RED and BLACK systems. Table 5 provides the computation data for the added physical and technical security required to protect the [redacted] RED system. Table 6 provides the computation data for similarly protecting the [redacted] BLACK system. It should be noted that the quantities used were based on information provided by the contractor and the experience of the working group. No security costs for outside buildings have been included in this cost estimate. The unit cost of physical and technical security protection in outbuildings may be higher than that required in the Headquarters environment.

25X1A

25X1A

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

CONFIDENTIAL

TABLE 4

HARDWARE COST OF SECURITY MEASURES FOR [redacted] SYSTEM 25X1A

	ITEM BEING SECURED	QUANTITY	SECURITY MEASURE	UNIT COST RED	UNIT COST BLACK
1.	I/O Device SAFE Terminal Regional Printer ADSTAR	 1663 158 900	Cabinet lock & increased cabinet strength	$ 100	$100
2.	Regional Printer + BIU SAFE Terminal + BIU ADSTAR + BIU	158 332 900	Contact switch alarm outside existing elect. closet w/TSP to a monitor Cabinet Lock	1350 20 1370	0 100 100
3.	Workstation Cluster + BIU 60%@4:1RATIO 998/4 = 20%@2:1RATIO 333/2 =	 250 167	Contact switch alarm for each cluster series w/TSP to a monitor Cabinet Lock	1500 20 1520	0 100 100
4.	Splitter Tap	30 1500	Contact switch alarm FM existing elect. closet w/TSP to a monitor Cabinet Lock Contact switch alarm from outside existing elect. closet w/TSP to a monitor Cabinet Lock	100 20 120 1350 20 1370	0 0 0 0 0
5.	Elect. closet IDF and floor cell entry cover	70	Contact switch alarm from existing elect. closet w/TSP to a monitor Cabinet Lock	100 20 120	0 0
6.	Pullbox	41	Contact switch alarm for outside existing elect. closet w/TSP to a monitor Cabinet Lock	1350 20 1370	0 0
7.	Floor cell covers	2000	Buy new covers to replace presently missing covers	40	0

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

25X1A

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Next 1 Page(s) In Document Exempt

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

D. RESOURCE COSTS

The required resource allocation for a security surveillance program can vary widely depending on the level of effort. In order to illustrate the range of costs, the resource costs were divided into two categories - a maximum effort and a minimum effort.

1. Maximum Effort

Technical Inspection - For a RED environment, if the Office of Security inspects every I/O device once a year, it is estimated that it would take 12 man-years of effort to inspect the SAFE system. This is based on an estimated 8 hours to inspect an I/O device and its associated wiring. It is estimated that for a RED scenario, it will take 10 man-years to provide an alarm monitor and response program capability. For a BLACK system, it will take 5 man-years to monitor the security console. In addition, the present annual maintenance costs for alarms and associated wiring is $31.2/alarm per year. It is estimated that these costs for the [redacted] RED system will be $6,300 and the the [redacted] RED system will be $107,600. These costs are not reflected on any table.

25X1A
25X1A

TEMPEST Inspection - If the Office of Communications TEMPEST-inspects every I/O device once a year, it is estimated that it would take 24 man-years of effort to inspect the SAFE system. This is based on a two-man team inspecting one I/O device per day and two electrical closets per day.

2. Minimum Effort

Technical Inspection - For a RED environment, if the Office of Security checks only the conduit runs and maintains alarms it is estimated that 3

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

man-years of effort would be required. It is estimated that for a RED scenario it will take 10 man-years to provide an alarm monitor and response program capability. For a BLACK system it will take 5 man-years to monitor the security console. In addition, the present annual maintenance costs for alarms and associated wiring is $31.2/alarm per year. It is estimated
25X1A that these costs for the [redacted] RED system will be
25X1A $6,300 and the [redacted] RED system will be $107,600. These costs are not reflected on any table.

TEMPEST Inspection - If the Office of Communications TEMPEST-inspects the 70 electrical closets annually and 10% of the I/O devices annually, it is estimated that 2 man-years of effort would be required.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

V. COMSEC SUBSYSTEM DEVELOPMENTAL RISK

The development schedule provided in the architecture document is confirmed as realistic. The schedule could be tightened, exposing the system to a higher degree of risk, but this does not appear necessary or desireable. NSA hopes to begin development of the COMSEC Subsystem in early FY-79. This will allow NSA to develop a CM which could be common to a variety of systems. This has several advantages to the SAFE program: lower unit cost, minimum development cost, security protection, and interoperability with other intelligence networks, and a development schedule approximately 9 months to 1 year earlier than required.

The performance risk is considered low. A significant risk item is the 9600 bps throughput required of the CM. However, this risk is minimized by the following:

A. There is a moderate risk in meeting the requirement with current day technology in microprocessors.

B. If the new higher speed microprocessors announced by manufacturers meet their claims, NSA can meet the requirement with ease.

C. Alternative cryptologic devices exist which can meet the throughput requirement, however, their employment would likely adversely effect potential interoperability with other systems.

D. NSA could use any one of a number of existing LSI cryptologic chips with microprocessor control and easily exceed the system requirements. However, the cost for each CM would probably rise to about $500 and SAFE would likely lose potential interoperability with other systems.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

25X1A

The SAFE COMSEC Architecture is analogous to the [redacted] development program. [redacted] has been in development since April 1977 and an operational testbed should be installed in mid-1979. Most of the detailed design and network protocols and procedures have already been accomplished. The next year involves software coding and equipment fabrication for the test. The only direct fallout from [redacted] to SAFE beyond the design stage, is the high speed Key Generator Unit (KGU). The remaining design and fabrication of this KGU is less than one year from completion. Thus, there are no remaining "prerequisites" from [redacted] except the KGU, and that will be fabricated and demonstrated prior to a SAFE contract award.

25X1A

25X1A

25X1A

The most significant risk item in the COMSEC Subsystem has to do with its interface to the SAFE System components. Changes in the basic SAFE architecture, once defined, must be fully coordinated with NSA to determine their impact on NSA schedules.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

VI. FUTURE UTILIZATION OF THE BUS

Since the analysis of the bus communications system indicates that it will only be 40% utilized when SAFE is fully operational, the remaining 60% capacity will be utilized for other communications requirements. This 150% growth in the number of I/O devices which can be connected to the bus is extremely significant because the same physical and technical security problems that exist for the SAFE system will exist for any system that utilizes the bus. This stems from the requirement to protect the information appearing on the bus.

If a RED bus system is installed, all the security features detailed in the cost section of the report must be applied for each new I/O device.

If a BLACK bus system is installed, a CM and lock will be the only security requirements for each I/O device.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

VII. DEFICIENCIES IN CONTRACTOR REPORTS

As expected, the two contractors made some different assumptions in coming up with their RED/BLACK presentations. Surprisingly, certain costs were excluded in one case and not in the other. Certain system sizing numbers were not consistent throughout. It was therefore difficult to create a common base of comparison for the candidate systems, particularly because the contractors were vague about itemizing security related costs. Although some of the differences could be resolved by assumed quantities to which unit security costs could be applied, other component counts were so imbedded in the contractors' submissions that unit costs could not be assigned. To be specific:

25X1A

A. [redacted] excluded the costs of physical security devices in their RED presentation. Therefore, the RED total cost was unrealistically low. Furthermore, it was difficult to track the distribution of system components so that reasonable physical security unit costs could be applied.

B. Although it was fully understood by the Working Group that the RED/BLACK Security Evaluation was not supposed to be a contractor competition, contractor design comes into play

25X1A

because [redacted] has a BIU associated with each terminal and the coaxial bus extending to the

25X1A

BIU, whereas [redacted] has one BIU for many terminals and terminates its bus in the electrical closets. The Security Working Group recognizes that part of the decision of the contractors for BIU placement was based on individual interpretations of what they were or were not permitted to do by the Government. If operations or security appears to advise a change, either contractor could be instructed to switch to the other's approach.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Although not a part of the contractors' submissions, Combined Project SAFE Office (CSPO) background paper, which included a communication system timetable, suggests an apparent difficulty for the delivery of the BLACK crypto subsystem. NSA confirmed on 23 March 1978 to the CSPO there was no difficulty. The original NSA delivery timetable was based on the dates previously supplied by CSPO. If a new shorter timeframe can truly be achieved by the contractors, then NSA can also advance its delivery. This can be stated with some confidence. Work on the more difficult building blocks of the BLACK COMSEC subsystem is already well underway for other applications, quite independent of SAFE. The SAFE contractors should be directed to work out the integration of the subsystem to their respective BLACK communications architecture.

It was noted as a deficiency of the CSPO timetable and the contractors' reports that no mention of a testbed timetable was made. Although a testbed period would be part of the System Acquisition Phase (SAP), the lack of reference to it in the CSPO timetable made it difficult to determine the necessary delivery date for a BLACK COMSEC Subsystem. The amount of time available to resolve any problems anywhere in the communications system which would first come to light in a functioning system could also not be determined.

25X1A

[redacted] neglected to provide an integration design figure to estimate support for a BLACK subsystem. It is understood that they are working up these figures at the present time.

It should be noted, as was stated by the NSA consultant in the joint meeting with the CSPO Working Group, that the costs of the BLACK COMSEC Subsystem were in part, predicated on the need for a 10 Mbs data rate per frequency slot. Subsequent contractor architecture changes have resulted in a change from the 10 Mbs rate to a 2 Mbs rate. As a result of this change, the costs for the COMSEC Front End (CFE) and the Safe Key Generator (SKG) should be greatly reduced.

It should be pointed out that [redacted] included costs for a conduit in the BLACK Communication System price. This is not a security requirement for a BLACK system. The total should be adjusted accordingly before comparing any total system costs.

25X1A

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

VIII. CONCLUSION AND RECOMMENDATIONS

A. INTRODUCTION

The utilization of a bus communication system introduces a new dimension to the data communication security problem. This dimension is the flow of all system communications on a single cable throughout the bus installation configuration. The potential damage to the Agency and National Security from penetration of this bus for the information flowing, mandates maximum security.

B. CONCLUSION

The two fundamental forms of communications security RED and BLACK were compared. The following conclusions are a result of this comparison:

1. The BLACK system provides absolute security on an end to end basis for each identifiable circuit within the bus; the RED system provides a high degree of physical security at the most vulnerable points only.

2. If Agency management accepts the higher security vulnerability of a RED system then management must recognize and accept:

   a. The Risk

   b. Added security hardware costs

   c. Increased security revalidation and maintenance resource costs

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

3. The security for bus expansion is easily achieved in a BLACK system; security costs are estimated at 50% lower than for a RED system.

4. A factor not directly associated with the SAFE communication system but which is worthy of management consideration is the potential influence on the Intelligence Community of a BLACK selection.

C. RECOMMENDATIONS

It is the recommendation of the Security Working Group that the BLACK system architecture be selected.

It is further recommended that a coordinating group be established to maximize the effectiveness of the security features which are to be implemented in the system.

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2

CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2002/01/30 : CIA-RDP85-00966R000100030001-2