CONFIDENTIAL

85-3169

OC-0848-85 COMPT-85-1050

11 SEP 1985

MEMORANDUM FOR: Executive Director

VIA: Comptroller
Deputy Director for Administration

25X1 FROM: [redacted]
Director of Communications

SUBJECT: Funding for the Network Security
25X1 Initiative Through FY-86 [redacted]

REFERENCE: Computer Security Investment Strategy,
25X1 FY 1985-91 [redacted]

1. In response to the "Computer Security Investment Strategy, FY 1985-91," (Network Security Initiative), the Communications Security Division (CSD) has established a Network Security Test Bed Program that will address the critical security areas of networking as outlined in the Network Security Initiative. The Test Bed Program is projected to continue into the 1990's, with the initial focus through 1986 being concerned with standards development, secure gateway research and development, and multilevel secure operation. A first step in
25X1 this program will be to proceed with a two year effort with [redacted]
25X1 [redacted] for the configuration testing and evaluation of a multilevel secure gateway in several
25X1 Agency network configurations. [redacted]

25X1 [redacted]

25X1

25X1 [redacted] [redacted]

CONFIDENTIAL

DCI EXEC REG

S-103

SUBJECT: Assurance of Funding for the Network
25X1 Security Initiative through FY-86 [redacted]

3. An Executive Summary and a Project Plan are attached for your review and we are attempting to schedule a briefing of this program to the Information Systems Board (ISB) during
25X1 October 1985. The point of contact in CSD [redacted]
25X1 [redacted]

Attachments:
A. Executive Summary
B. Project Plan

CONCUR:

Deputy Director for Administration — Date

25X1 [redacted]

Comptroller — 20 SEP 1985 — Date

ATTACHMENT A

NETWORK SECURITY TEST BED PROGRAM

Executive Summary

I. General

The Computer Security Investment Strategy for FY 1985-91 identifies network security as an Office of Communications (OC) initiative to increase the security, survivability, and interoperability of this Organization's networks.

Pursuant to this strategy, OC has initiated a Network Security Test Bed Program to explore new approaches to secure network connectivities and data communications.

This summary describes the Test Bed Program and the significant potential benefits.

II. Test Bed Program Definition

The Network Security Branch (NSB) will procure hardware and software to support a test bed for exploring state-of-the-art network security technology and concepts, such as multilevel secure gateways, front-end processors, and filter/interface devices.

The test bed will simulate various network environments and interface connections that exist either now or will exist throughout the Agency. This will allow determination of the best solutions to networking security issues. For example, a major issue in network security is where to place the secure access controls to restrict services and data flow: in the host? in the backbone network? in the gateway or interface filter? or in some combination of these? The test bed will allow the Agency to configure a specific network architecture and determine the best techniques and tools for that architecture.

Tremendous cost savings may be realized if such security solutions are tested on a small scale first, prior to investing millions of dollars on a network-wide implementation.

There are numerous other network and interface security issues to be confronted by the 1990's, such as how to maintain security while interconnecting a network operating in multilevel secure mode with a network operating system high. However, we

cannot wait until the 1990's to address these issues. This test bed will serve as an asset to begin studying networks immediately, from a top-down, overall perspective. OC has already identified major security issues confronting networks; we must now identify user interfaces and high level network relationships, then apply the test bed to evaluating devices and techniques to secure these interfaces.

The Test Bed Program will take direct advantage of several studies currently underway at the DOD Computer Security Center:

A. The draft Network Security Criteria;
B. The Internetwork Security Research Study; and
C. The Multinet Gateway Program.
D. The Multilevel Secure Bus Interface Unit

III. Test Bed Program Objectives

The Test Bed Program will serve four long-range objectives:

A. Evaluate Network Components (Products and Concepts)

The test bed will support testing and security evaluation of various network components in order to recommend such components to network architects who must construct secure networks. These components include gateways, front-end processors, and filter/interface devices, as well as state-of-the-art security concepts such as [redacted] end-to-end encryption.

25X1

B. Certify Networks

The test bed will provide a means for certifying existing networks and interfaces as well as those under construction.

C. Develop Certification Criteria

Although the DOD Computer Security Center at NSA has published the "Orange Book" defining criteria for evaluating monolithic computer operating systems, new criteria and techniques must be developed for evaluating networks that present new and complex problems which cannot be addressed wholly from the viewpoint of COMPUSEC, nor wholly from the traditional approaches of ComSec. The test bed will allow evaluation of and input to draft Network Security Criteria that the DOD Computer Security Center is developing for certifying networks.

D. Serve as Training Environment for Agency Certifiers

Certification is the evaluation of an application to see how well it meets security requirements. The test bed will provide security evaluator personnel with evaluation and judgment skills necessary to certify networks and their components.

IV. Test Bed Program Phases - General Description

The Network Security Test Bed Program will be structured in several phases:

A. Phase I - MULTINET Gateway (1985-1987)

In Phase I, the NSB will acquire test bed hardware and software as well as a multilevel secure gateway device, then test and evaluate the product as detailed below.

B. Subsequent Phases (1986-1995)

Subsequent phases of the Test Bed Program will evaluate other applications of the MULTINET Gateway, as well as other secure networking devices and concepts. These may include GEMINI, SCOMP and SCP devices; also [redacted] End-to-End Encryption and secure LAN technology.

25X1

V. Phase I MULTINET Gateway - Detailed Description

A. In the first phase of the Test Bed Program (1985-

25X1

[redacted]

B. In addition to evaluating the MULTINET Device as an internet gateway, Phase I will initiate a study to identify interface requirements and higher level relationships among

[redacted]

25X1

C. Thus, by the end of Phase I, three functional versions of the MULTINET gateway will have been developed, implemented and evaluated in the OC test bed:

1. Internetwork Gateway. A multilevel secure gateway connectivity between many diverse network types.

2. Front-End Processor with End-to-End Encryption. A multilevel secure network front-end processor with end-to-end encryption chips. This front-end device would connect terminal clusters and host systems into a larger network, such as a Local Area Network (LAN) or long-haul network.

3. Front-End Filter/Interface Device. A multilevel secure filter and interface device for connecting smaller systems, such as LANs or host clusters, into a larger network. End-to-end encryption may be optionally available.

D. Although the initial MULTINET product is expected to be certified A1 as a MULTINET Gateway, there is no guarantee that it will be certified in its other functional modes as a front-end processor and filter/interface device. Part of the Phase I effort will be to evaluate the gateway in its functional roles as a front-end processor with end-to-end encryption and as a front-end filter/interface device. Thus, the objective of this first phase of the Test Bed Program is to evaluate how well the MULTINET Gateway product:

1. Satisfies multilevel secure requirements for gateways, filters, and interface devices;

2. Supports the mission to improve interoperability by interconnecting multiple network types; and

3. Supports the mission to increase survivability by the use of public, DOD and other specialized USG-owned or operated data networks.

CONFIDENTIAL

ATTACHMENT B

PROJECT PLAN

NETWORK SECURITY TEST BED PROGRAM

28 JUNE 1985

25X1

Office of Communications

CONFIDENTIAL

TABLE OF CONTENTS

PROJECT PLAN

Network Security Test Bed Program

1.0 Introduction

1.1 Purpose

The document defines the Program and steps to be executed in order to meet program objectives.

1.2 Scope

This document spans the entire projected life cycle of the testbed program, from acquisition of equipment to its use within the Agency as an asset for addressing network security issues. The program will run through 1995 and will address many aspects of network security including:

- test bed procurement
- R & D of multi-level secure internetworking devices
- operational test and evaluation of networks
- development of certification criteria
- certification of networks

1.3 References

25X1

1.3.1 Computer Security Investment Strategy, FY1985-91, [redacted] pp. 12-19, November 1984, CIA Computer Security Working Group, Information Systems Board.

1.3.2 Draft of Network Security Threats, Issues, and Countermeasures, Rev. 13 Jun 85, DDA/OC/CSD/APG/NSB

2.0 Background

The Computer Security Investment Strategy, FY 1985-91, approved by the Executive Director, CIA, identifies Network Security as an Office of Communications (OC) initiative to increase the security, survivability, and interoperability of Agency networks.

Increased security is achieved when hosts processing data at different security classifications and security compartments and accredited at different Automated Data Processing system security modes are allowed to communicate securely. Increased

inter-operability is achieved by allowing hosts on different networks, with different network protocols, to exchange data without resorting to exceptional procedures. Survivability is achieved by providing the capability of using DoD or public networks as transfer mechanisms to reestablish Agency internet connectivity.

Pursuant to this strategy, the OC has initiated a Network Security Test Bed Program to explore new approaches to secure network connectivities and data communications. The Network Security Branch of the OC Communications Security Division (OC/CSD) will procure hardware and software to support a Test Bed for exploring state of the art network security technology and concepts, such as multilevel-secure gateways, front-end processors, and filter/interface devices.

The Test Bed will simulate various network environments and interface connections that either exist now or will exist throughout the Agency. This will allow determination of the best solutions to networking security issues. For example, a major issue in network security is where to place the secure access controls to restrict services and data flow: in the host? in the backbone network? in the gateway or interface filter? or in some combination of these? The Test Bed would allow the Agency to configure a specific network architecture and determine the best techniques and tools for that architecture.

Tremendous cost savings may be realized to the Agency if such security solutions are tested on a small scale first, prior to investing millions of dollars on a network-wide implementation.

There are numerous other network and interface security issues that will confront the Agency by the 1990's, such as how to maintain security while interconnecting a network operating in multilevel-secure mode with a network operating system high. However, we cannot wait until the 1990's to address these issues. This Test Bed will serve as an Agency asset to begin studying networks immediately, from a top-down, overall perspective. OC has already identified major security issues confronting networks; now, working independently and with the Office of Information Technology (OIT), OC must identify user interfaces and highlevel Agency network relationships, then apply the Test Bed to evaluating devices and techniques to secure these interfaces.

The Test Bed Program will take direct advantage of several studies currently underway at the DoD Computer Security Center:

(1) the draft Network Security Criteria,

(2) the Internetwork Security Research Study, and
(3) the MULTINET Gateway Program.
(4) the Multilevel Secure LAN Bus Interface Unit

3.0 Test Bed Program Objectives

The Test Bed Program will serve four long-range objectives:

(1) Evaluating Network Components (Products and Concepts). The test bed will support Agency-wide test and security evaluation of various network components in order to recommend such components to Agency network architects who must construct secure networks. These components include gateways, filters, front-end processors, and interface devices, as well as state-of-the-art security concepts such as [redacted] end-to-end encryption.

25X1

(2) Certifying Networks. The test bed will provide a means for certifying existing networks and interfaces as well as those under construction.

(3) Developing Certification Criteria. Although the DoD Computer Security Center at NSA has published the "Orange Book" defining criteria for evaluating monolithic computer operating systems, new criteria and techniques must be developed for evaluating networks that present new and complex problems which cannot be addressed wholly from the viewpoint of COMPUSEC, nor wholly from the traditional approaches of ComSec. The Test Bed will allow evaluation of and input to draft Network Security Criteria that the DoD Computer Security Center is developing for certifying networks.

(4) Serving as Training Environment for Agency Certifiers. Certification is the evaluation of an application to see how well it meets security requirements. The Test Bed will provide the security evaluator personnel with evaluation and judgement skills necessary to certify networks and their components.

4.0 Test Bed Program Phases.

The Network Security Test Bed Program will be structured in several phases:

(1) Phase I - MULTINET GATEWAY (1985-1987). In Phase I, OC/CSD Network Security Branch (NSB) will acquire Test Bed hardware and software as well as a Multilevel Secure Gateway device,then test and evaluate the product as detailed below.

(2) Subsequent Phases - (1986-1995). Subsequent phases of the Test Bed Program will evaluate other applications of the MULTINET Gateway, as well as other secure networking devices and concepts. These may include GEMINI, SCOMP and SCP devices; also [redacted] End-to-End Encryption and secure LAN technology.

25X1

4.1 PHASE 1 MULTINET GATEWAY - Detailed Description

4.1.1 In the first phase of the Test Bed Program (1985-1987), [redacted] OC/CSD/NSB will obtain and evaluate the MULTINET Gateway.

25X1
25X1

[redacted]

4.1.2 In addition to evaluating the MULTINET Device as an internetwork gateway, Phase I will initiate a study to identify various Agency and Intelligence Community requirements for multi-level secure local area network and major interconnections among CIA, DoS, DOD, and other networks to determine where the Gateway can best support security issues. (See Appendix A for requirements questionnaire.) These requirements will be supplied to FACC under a Phase I contract to develop and help evaluate two additional configurations of the MULTINET device specifically for Agency applications: 1) a generic front-end processor and 2) a front-end filter/interface device.

4.1.3 Thus, by the end of Phase I, three functional versions of the gateway will have been developed, implemented and evaluated in the Test Bed:

(1) Internetwork Gateway. A multilevel-secure gateway connectivity between many diverse network types, such as the CIA MERCURY and the NSA PLATFORM networks, or MERCURY and Defense Data Networks (DDN).

(2) Front-End Processor with End-to-End Encryption. A multi-level secure network front-end processor with end-to-end encryption chips. This front-end device would connect terminal clusters and host systems into a larger network, such as a local area network or long-haul network.

(3) Front-End Filter/Interface Device. A multilevel-secure filter and interface device for connecting smaller systems,

such as the NPIC LAN or host clusters, into a larger network. End-to-end encryption may be optionally available.

4.1.4 Although the initial MULTINET product is expected to be certified A1 as a MULTINET gateway, there is no guarantee that it will be certified in its other functional modes as a front-end processor and filter/interface device. Thus, part of the Phase I effort will be to evaluate the gateway in its functional roles as a Front-end Processor with End-to-End Encryption and as a Front-End Filter/Interface Device.

4.1.5 Specific test objectives include evaluating how well the MULTINET device:

(1) satisfies multilevel secure requirements for gateways, filters, and interface devices,

(2) supports the mission to improve interoperability by interconnecting multiple network types, and

(3) supports the mission to increase survivability by the use of public, DoD and other specialized USG-owned or operated data networks.

4.1.6 Specific security functions of the three MULTINET devices to be tested include:

(1) Multi-level secure switching (isolation of data messages.)
(2) Embedded end-to-end encryption (supports multi-level security)
(3) Network access controls
(4) Interoperability between users of different access protocols.
(5) Data labeling
(6) Auditing (statistics and violations)

5.0 Organization and Responsibility

5.1 Office of Communications (OC)

5.1.1 The Network Security Branch of the Communications Security Division will act as Test Bed Program Office to manage and execute this project.

5.1.2 The Engineering Division will provide technical assistance and guidance through the MERCURY Project Office (MPO). The Test Bed hardware will be procured through the Mercury Project

Office.

5.1.3 The OC Contracting Team will support any contract and dealings with contractors that arise as part of this project.

5.2 Office of Information Technology (OIT)

5.2.1 The Computer Security Group, OIT, will assist OC/CSD in definition of interface requirements and security issues for Phase I MULTILNET Gateway. CSG will also be involved with testing other representative TCB systems (e.g., Gemini, SCOMP, SCP)

5.2.2 The Domestic Network Group, OIT, will participate in definition of interface requirements and security issues for Phase I MULTINET Gateway.

5.2.3 The Processing Systems Group, OIT, will participate in definition of interface requirements and security issues for Phase I MULTINET Gateway.

5.3 Office of Logistics (OL)

5.3.1 The Security Staff, OL, will provide guidance on matters of security as they relate to contracts, personnel, shipping, and external correspondance.

5.3.2 The Supply Division, OL, will provide support for the shipping and receiving of hardware that will arise as part of this project.

5.4 Rome Air Development Center (RADC)

RADC will loan the OC the initial Phase I device to be evaluated in the Test Bed, i.e., The MULTINET Multi-level Secure Gateway. They will also assist OC by writing a high-level Test and Evaluation Plan for the MULTINET gateway.

5.5 Ford Aerospace & Communications Corporation (FACC)

FACC is developing the MULTINET Multi-level Secure Gateway under contract to RADC and will provide hardware/software reconfiguration work on the gateway under contract to OC as a part of the OC Network Security Test Bed Program.

6.0 Management and Technical Controls

6.1 Project Coordination Note (PCN)

A PCN (Appendix B) will be issued to all project personnel prior to the occurrence of an event important to the project. They will be numbered sequentially and in a standard format, (see attached).

6.2 Action Item

As part of a PCN, an Action Item will be issued to those persons who must act on a certain item upcoming in the project.

7.0 Operational Requirements

Networks evolve from the combination of a computer system and a communication system; however, network security concerns are more than just the combination of the security issues of computers and communications. The security concerns are additive to a certain extent, with new concerns arising from the interactions of computer systems with communication systems. The Network Security Test Bed Program will help ensure that our networks can be used to their fullest extent by addressing network security issues and developing appropriate solutions.

8.0 Resources

8.1 Personnel

	CSD	MPO	OIT	OL	Contractor
man years/yr	1.5	.1	.75	.1	1.

8.2 Funding

25X1 Approximately [redacted] will be provided for Network Security through 1991; part of this will be allocated for the Network Security Test Bed Program.

8.3 Equipment

25X1 8.3.1 [redacted] will provide one MULTINET Secure Gateway for this Agency to evaluate for a period of 24 months.

8.3.2 Follow on efforts of the Test Bed Program will require hardware/software from various Agency or external sources.

8.3.3 Test equipment to support the Test Bed will be borrowed,

rented, or procured.

8.4 Procurement Plan

8.4.1 The initial Network Security Test Bed hardware and software will be procured as part of the Mercury contract with funds transferred to the Mercury Project Office (see section 9.0).

8.4.2 Test equipment will be procured independently of testbed hardware.

9.0 Program Schedules

See Milestone Chart (Appendix B)

10.0 Security

The Security Staff, OL, will provide guidance on all matters of security related to the handling of contracts and contractors, as well as other aspects of this program with physical security concerns.

11.0 Training

Members of OC and OIT will undergo training pertaining to the operation of the Test Bed. This will be coordinated through the Mercury Project Office and will occur as part of the MERCURY training contract or separately under NSB cognizance.

12.0 Continuing Efforts

Through 1995, NSB will use the Test Bed to achieve the Network Security Test Bed Program objectives defined in Section 3.0 of this plan.

NETWORK AND INTERFACE REQUIREMENTS QUESTIONNAIRE (DRAFT)

1. Name of Network or Interface: Specify Common User Name of the network or interfacing systems; for Example, COINS, NPIC LAN, CAMS to 4C.

2. User Community Category: Classify network or interface in terms of its users, such as Intelligence Community, CIA, Defense. Thus, an interface may be IC to CIA, or CIA to CIA, or IC to Defense, etc.

3. Classification Category: Classify netowork or interface in terms of the data classification. Thus an interface may be Unclass to Classified, Compartmented, or Unclass to Unclass, etc.

4. Network Category: Classify the network or interface in terms of its networking components; e.g., a LAN, Host Cluster, Long-haul packet-switch network, Terminal Cluster, Switchable Terminal to Host, Host to LAN, Long-Haul to Long-Haul.

5. Overview: Give a brief description of network or interface plus a characterization of user needs. Identify user community(s)

6. Interface Requirements: Specify the networks and systems that must connect with the network or are connected by the interface device.

7. Major Network Components: Specify connections media and processing entities. For example:

a. Connections - communications media to interconnect processing entities. (e.g. leased line, satellite, etc.)

b. Processing entities - those devices attached to the communications media that facilitate, control, monitor, or otherwise participate in the transfer of information across that medium. Such devices may include, but are not limited to:

host computer
network switch
switchable terminal
network front end
gateway
personal computer
encryption device
key distribution center

8. Topology: Describe geometry and physical geographical location of the network components; e.g., star with major nodes located world-wide. Two major structures are:

a. Centralized - consisting of a central computer system with simple communication lines radiating from central computer system (STAR), or may include multiplexors or concentrators serving to fan in still other radial communications lines (HIERARCHICAL TREE).

b. Distributed - ranging from RING to FULLY-CONNECTED depending upon the number of lines joining the nodes.

9. Threats associated with the network or interface.

10. Security Policy to be enforced as it relates to threats. For example, "eliminate risk of spillage." Include following elements:

a. host security policy, if hosts are involved;
b. filter security policy if interfaces are involved;
c. Network security policy, if a network is involved;
d. Levels and compartments of security to be processed
e. Operating Mode (multi-level, uni-level, or unprotected)
f. Physical access limitation
g. Logical access limitations, e.g., on data flow and services

11. Protocols: Specify first 3 protocol layers used in the network. (Layer 1 = physical layer, layer 2 = link layer, layer 3 = network layer).

12. Data Processing Requirements: Specify performance, terminal, and data characteristics:

a. Performance - Thruput and data speeds, channel allocation (fixed or dynamic, I/O (synchronous or asynchronous)

b. Terminal characteristics - Number of terminals, thruput, speed, and response time required.

c. Data Characteristics - Character Set (EBCDIC, ASCII, BAUDOT); Parity (odd, even, or none)

13. Transmission Control Specify:

a. Terminal control, such as clear to send or data terminal ready.

b. Error control, such CRC or data recovery.

1. Name of Network or Interface.

2. User Community Category.

3. Classification Category.

4. Network Category.

5. Overview.

6. Interface Requirements.

7. Major Network Components.

8. Topology.

9. Threats associated with the network or interface.

10. Security Policy to be enforced as it relates to threats.

11. Protocols.

12. Data Processing Requirements.

13. Transmission Control.

PROJECT COORDINATION NOTE:

Project : PCN#

Author : Date

Approval : File

Subject :

Distribution:

Text

Action Items

Appendix B

MILESTONE CHART

MILESTONES	COMPLETION YEAR 85	86	87	88	89	90
1.0 Phase I: Multinet Gateway	x----------x					
1.1 Front end processor with end-to-end encryption	x-------x					
1.2 Internet Gateway	x----------x					
1.3 Front end filter/ Interface Device	x----------x					
2.0 Phase II: Subsequent Phases		x----------x				
25X1 2.1 The [redacted] Program		x--------x				
2.2 Secure voice gateway systems			x---------x			
2.3 Packet voice systems				x----------x		
2.4 Other applications					x----------x	

Appendix C