22 AUG 1984

5 July 1984

MEMORANDUM FOR THE RECORD

STAT FROM : [redacted]
Computer/Systems Analyst-Programmer, IAB

SUBJECT: Production Version of the RECON Guard

1. The RECON Guard project began in 1981 and has streched into mid-1984 with the successful conclusion of testing on the prototype system. During the three years of development, OCR/IAB programmers created several new software products and procedures to handle the transfer of data between the two systems. They have also attempted to keep track of potential problems in the handling of the different system functions and responsibilities such as data security, batch versus interactive queries, and data verification, response and query verification, lengthy update times, and many more. This memo attempts to point out items that must be addressed if the RECON Guard System is redesigned for production.

a. Query: The prototype was designed as a batch system which required the use of a SYTEK GUARD "editor" to create queries. This editor was installed for use by programmers and was not meant for the user or for heavy use as it proved to be very cumbersome.

Recommendation: The production RECON Guard System should be designed as an interactive system or, least, contain a functional way to enter queries.

b. Update Guard: The prototype system was designed to use a magnetic tape update procedure to demonstrate that the Guard System could be isolated from the on-line systems. The major problems encountered were: magnetic tapes produced by the IBM system used TMS and ACF2 rules that had to be bypassed by logging the tape back in as a Z-tape and bypass label processing; the Update function of the Guard is very slow, and requiring some 60-90 minutes to process 2,000 records, depending on the type of checksum being calculated. On two occasions tapes were produced by the Update Guard that could not be read.

Recommendation: The production RECON Guard System should have a direct link to JES/MVS and eliminate the magnetic tape problem.

ADMINISTRATIVE - INTERNAL USE ONLY

c. Data Security: The protection and verification of the data being processed through the Update Guard was not addressed in the systems design. OCR/IAB wrote software and procedures to be used during the verification process, but this was not exercised because only test (unclassified) data was processed. The verification software consists of a simple comparison of the data records, before and after processing through the Update Guard (minus length and checksum fields). Any non-matches would have halted the RECON update cycle.

Recommendation: The production RECON Update cycle should contain such a feature or a similar data verification procedure.

d. ACF2 Security: Security concerns were raised on several occasions by OCR/IAB that protection of the Linear Files (production data base) was paramount and that if testing ever progressed beyond the test data base, that ACF2 security rules would be written to limit access.

Recommendation: The production RECON Guard System should be accessed through the ACF2 security systems for the data bases involved.

e. RECON Software: The RECON software and procedures have been modified to limit the types of commands that may be invoked. All RECON output type commands, such as Display, Print, Save, History, etc., have been suppressed. The user query will only be permitted to generate a final 'hit' set containing requested terms. This hit set is then saved and a predetermined 'Canned Query' is generated according to the originator's address. The hit set and the Canned Query results are combined and any record matches are eliminated from the final hit set..This final hit set contains only those records that the users organization has access to. The final hit set is then returned to the Guard System for a checksum security verification.

Recommendation: CIA should consider a similar method to handle interactive queries on the production RECON System.

f. OCR/IAB Software Security: The RECON software is controlled by OCR/IAB and is strictly protected by ACF2 rules. This must continue to be the case and should be considered in a production RECON Guard System.

STAT g. Guard Software and Hardware Security: During testing of the prototype system, the Guard System resided in the GCO3 [redacted] Center. Although the system was in a protected area, there were several instances that the Guard System had been 'played' with during non-prime time. There was no damage done nor intended but this does point out that the Guard System and software must be closely controlled.

SUBJECT: Production Version of the RECON Guard

Recommendation: The production Guard System hardware and software physical security controls should be closely considered.

h. Guard and JES/MVS Linkage: The Guard and JES/MVS linkage uses 80-character card image protocol for queries and variable-length spanned-record protocol during RECON output to the Guard. The Guard software does not have any problems with this, but it will require alteration if an interactive production system is required.

2. The above items are, at best, a partial list that should be considered for a production Community RECON Guard System. Of all of the above, only the interative RECON System represents a major task. It would require a great deal of effort to write software to handle interactive users and multiple organizations.

STAT

STAT DI/OCR/SSG/SSD/IAB/

STAT Typed Final: (13 Aug 84)

Distribution:
Original - IAB File
STAT 1 - ORD
1 - C/SSD

CONFIDENTIAL

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Testing of the RECON GUARD Prototype

25X1 FROM: [redacted]

NO.

DATE 5 JUL 1984

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. ~~RECON Project Officer PATG/ISG/ORD 720 Ames Building~~				Chuck,
2.				Attached is the RECON GUARD Prototype Test Report, which I showed you last week. I've sent a copy of this to [redacted] as a draft.
25X1 3. [redacted] Mgmt Staff, OOP				
4.				I intend to submit this same memo to go from the Director of Security to [redacted] and Claire Rice, therefore, please consider this official between you and me but not the official OS response.
25X1 5.				
6.				
7.				Tom,
8.				As we discussed, there will be another test report forwarded to OOP signed by D/S. I don't anticipate that the actual test results will change in any way.
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 1-79 **610** USE PREVIOUS EDITIONS

GPO : 1983 O - 411-632

CONFIDENTIAL

~~CONFIDENTIAL~~

29 JUN 1984

MEMORANDUM FOR: RECON Project Officer
Processing and Analysis Technology Group,
Information Systems Research Division,
Office of Research and Development

25X1 FROM: [redacted]
Industrial Systems Branch,
Information Systems Security Group, OS

25X1 SUBJECT: Testing of the RECON GUARD Prototype [redacted]

1. Between 14 May and 11 June 1984, Information Systems Security Group performed testing of the RECON GUARD prototype hardware which was developed by Sytek, Incorporated, under contract to the Office of Research and Development. The objective of this Project was to demonstrate the feasibility of the GUARD-Device concept and its applicability to the problem of connecting classified Agency data bases to external networks. Preliminary examination of the test results, indicate that the GUARD performs this function. I recommend, therefore, that the GUARD Device be certified as having passed the tests described
25X1 in attachment A. [redacted]

2. Testing was performed using the Guard Test System (GTS) which emulated a Host Access System (HAS). Use of the GTS allowed for easier manipulation and verification of the data than if using a live COINS HAS. Additionally, testing was performed using only a 2,000 record test RECON data base. It is most important to note that extensive testing with a live network and a live data base must take place before a GUARD-Device can hold the trusted position of protecting classified Agency data from unauthorized exposure to an external network.
25X1 [redacted]

3. It is also noted that the GUARD cannot control what happens to data before data enters RECON via the Update Guard, while data is stored in the RECON data base, or after data is
25X1 released from RECON via the On-line Guard. [redacted]

4. The boundary of effect of the GUARD system is defined to be these entry and exit points. There are currently no known Trojan Horses or trap-doors in the MVS, JES3 or RECON systems. Since RECON GUARD, as it is presently configured does not address the Trojan Horse issue, the GUARD system must
25X1 be assessed on this basis. [redacted]

25X1 [redacted]

~~CONFIDENTIAL~~

5. Testing was intended to address the trustworthiness of the GUARD as a gateway to allow the release of authorized data and to prevent the release of unauthorized data. It did not, for instance, consider issues such as throughput. 25X1 [redacted]

6. All currently planned testing has been accomplished.

25X1 [redacted]
25X1 [redacted]

Attachments:
A. RECON GUARD Test Plan (Attached)
B. RECON GUARD Test Results (Pending)

APPROVED:

25X1 [redacted]

Chief, Information Systems Security Group

5 July 1984
Date

RECON GUARD TEST PLAN

The tests outlined in the following pages were performed based upon several assumptions. The GUARD must be operated within these constraints for the test results to remain valid. These assumptions are as follows:

- One AGB[1] is dedicated to each site for this test (i.e., State, DIA, and NSA).
- Individuals at each site are cleared system high and identified to the network; terminals are physically located in system high approved areas.
- Sufficient physical and personnel security standards for system high processing are afforded to the GUARD hardware and the Security Officer Interface Device (SOID).
- The GUARD cannot control what happens to data before data enters RECON via the Update Guard, while data is stored in the RECON data base, or after data is released from RECON via the Online Guard. The boundary of effect of the GUARD system is defined to be these entry and exit points.
- Testing was performed using identical secret keys for the multiple sites.
- Testing was performed using the Guard Test System (GTS) which emulated a Host Access System (HAS). Use of the GTS allowed for easier manipulation and verification of the data than if using a live COINS HAS.
- A Trap-Door program was utilized to allow for limited data manipulation of RECON records. Releasable RECON records could probably be created within the RECON data base given the knowledge of the appropriate secret key, sufficient time, systems knowledge, and accessibility.
- Testing was performed using only a 2,000 record test RECON Data base.
- There are currently no known Trojan Horses or trap-doors in the MVS, JES3 or RECON systems. Since the GUARD as it is presently configured, does not address the Trojan Horse issue, the GUARD system must be assessed on this basis.

1 See the glossary of definitions on the following page.

The following definitions will be used throughout this document:

- A record or a RECON record is defined to be a collection of data which meets the format requirements for entrance to RECON, or such a collection of data after it has been marked for distribution to specified communities.

- A secret key or key and initial value consists of a cryptographic type of numeric key value and initial value used by the DES algorithm to encrypt or decrypt a given data stream. Both the secret key and the category expression reside in an erasable programmable read only memory (EPROM) that is located on one or more Authentication Generator Board (AGB).

- An authenticator is a digital signature attached to a record. It is either a blank field called a null authenticator or it is a field of the record containing a value calculated for the record with an algorithm such as DES using the record itself and a secret key. Authenticators are used to control release and distribution of RECON records.

- A category can be identified for a record by specific fields of the record. A boolean function called a category expression is associated with each releasable data set. If the category expression when applied to a given record evaluates to "TRUE," then the authenticator is computed with the secret key associated with that category expression.

- A record is a candidate for release by the GUARD or the GUARD is authorized to release a record if and only if there is a category expression and secret key within the GUARD which is associated with the record.

EXAMINE CODING OF SOFTWARE

Review and confirm that Theorems and Corollaries are valid in the "GUARD System Verification Report," dated 3 May 1984.

Review and confirm "vmulti pl" master, dated 11 May 1984.

Review and confirm "vupislv pl" (outer block of code that runs on the Update Guard Input Slave Board), dated 11 May 1984.

Review and confirm "vupdate pl" master, dated 11 May 1984.

Review and confirm "vassembly al", dated 11 May 1984.

Review and confirm "vagbmod al", dated 4 January 1984.

Review and confirm "vagb pl" (outer block of code that runs on the AGB), dated 4 January 1984.

Evaluate security relevant material from "Guard System Operation and Maintenance" report, dated 16 April 1984.

Evaluate security relevant material from "RECON IV Users Manual," dated April 1980.

VERIFY FUNCTIONAL OPERATION OF GUARD

1. Develop 20 test queries.

2. Run the test queries directly through the RECON Test Data Base without interfacing with the GUARD.

3. Run the test queries through the GUARD System utilizing all possible AGB's and sites (nine runs per query).

4. Compare the results of the test runs to ensure functional operation of the GTS and ensure that improper release or spillage has not taken place.

SECURITY VULNERABILITY DETERMINATION

Operational Tests

1. Incorrect EPROM insertion/removal.

2. Induced errors on the Update Guard (UDG).

   a. Write to an output tape where the records from the input tape exceed the length of the output tape.

   b. Invalid record test requiring improperly formatted input tapes.

      1) A record too short.

      2) A record longer than the UDG buffer (2048 bytes).

      3) A record with an incorrect checksum.

      4) A record that already has an authenticator.

      5) A record with a category expression unknown to the UDG.

      6) A record that goes off the end of the input tape.

      7) A record with incorrect tape parity.

c. Configuration test illustrating UDG's reaction to changes in slave board configuration and placement.

   1) Remove output slave processor board.

   2) Start system with drives off load-point and offline.

   3) Start system with drives powered off.

d. Manipulation of alarm system and auditing device connection.

   1) Unplug the alarm cable before starting UDG.

   2) Unplug the audit cable before starting UDG.

   3) Unplug the alarm cable while UDG is running.

   4) Unplug the audit cable while UDG is running.

e. Abnormal AGB data EPROM contents.

   1) Improper checksum.

   2) Corrupted secret key.

   3) Corrupted initial value.

   4) Corrupted stock plain text.

   5) Corrupted cyphertext.

f. Abnormal tape contents.

   1) A tape without IBM labels.

   2) A tape with improper IBM labels.

g. Abnormal tape procedures.

   1) Attempt to combine multiple input tapes given a single output tape.

   2) Take drives offline.

   3) Alter tape position by hand.

   4) Put write ring on input tape.

   5) Remove write ring from output tape.

3. Induced errors on Online Guard (OLG).

   a. Manipulation of alarm system and auditing device connection.

      1) Unplug the alarm cable before starting OLG.

      2) Unplug the audit cable before starting OLG.

      3) Unplug the alarm cable while OLG is running.

      4) Unplug the audit cable while OLG is running.

   b. Random start, stop and power disruption.

GUARD System Outage Tests

1. Random start/stop during record transmission.

   a. Power off the protocol converter during record transmission.
   b. Reset GUARD during record transmission.
   c. Power off GUARD during record transmission.

2. Random unplugging of Online Guard.

   a. During record transmission.
   b. After system configuration but prior to query submission.

3. Random switching/removal of AGB's.

   a. Removal of AGB during record transmission.
   b. Insertion of new AGB after system configuration but prior to query submission.
   c. Insertion of new AGB during record transmission.

4. Disruption of Security Officer Interface Device.

   a. By random/intermittent power down.
   b. Incorrect keyboard entries.
   c. Preparation of EPROM on a EPROM burner which is not a part of the SOID.

5. Inducement of tape errors for Update Guard.

   a. Tape too short for specified records.
   b. Random manipulation of alarm, audit device, etc.
   c. Invalid data.

Manipulation of AGB Boards

1. No AGB.
2. Single AGB with multiple category expressions.
3. Single AGB with multiple category expressions and secret keys.
4. Multiple AGB's with same category expression and secret key.
5. Multiple AGB's with different category expressions.
6. Multiple AGB's with same secret key.
7. Multiple AGB's with different secret keys.
8. Random manipulation of AGB's from one site and office/ organization identification from another site.
9. General manipulation of AGB sites, secret keys and release categories.

Trap - Door Program

1. Manipulate data without modifying authenticator.
2. Modify only authenticator.
3. Modify both authenticator and data.
4. Attempt to manipulate data in such a way to achieve same checksum.
5. Attempt to manipulate data in such a way to achieve same authenticator.
6. Modify data, attempt to release, then return data to original condition.
7. Modify data and/or authenticator, determine and append new checksum.
8. Modify data and/or authenticator, determine and append new authenticator.
9. Reauthenticate records in test RECON.
10. Alteration of record content.

Covert Signalling Channel Tests Attempt to Transmit Data:

1. Modulation of handshake sequence.

   a. Time lapse between error responses.
   b. Device Interrupt error.
   c. Number of interrupts/time period.
   d. Use of CANCEL and STATUS acknowledge requests.

2. Modulation of error messages through manipulation of records via the trap door program.

3. Modulation of legitimate traffic (intact RECON records).