

~~SECRET~~

DIRECTOR OF CENTRAL INTELLIGENCE
Intelligence Information Handling Committee
WASHINGTON, DC 20505

25 July 1984
DCI/ICS 84-4030

MEMORANDUM FOR:




25X1

FROM:

DCI Intelligence Information Handling Committee

SUBJECT:

Comments on CIA 4-Cs Assessment

1. Jim's group did a good job of assessing the 4-Cs system using the questionnaire developed by . The responses are clear and appear to be unbiased as an assessment.

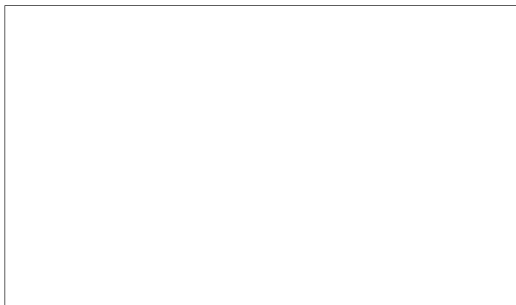
25X1

2. My concerns are:

a. I had indicated to Jim several times over the past few months that a report should be written in the format of NFIB ADS report as the end product of CIA's assessments. While these answers to the questionnaire are good, it lacks the analysis, assessment, and recommendations (resources) that I thought we needed. There are no resource estimates. It appears that all is well and that there are no problems with 4-Cs.

b. Unfortunately, we still seem to have a basic definitional problem with the DCID 1/16 terms:

- Dedicated mode
- System-high mode
- Compartmented mode



25X1

25X1

~~SECRET~~

SECRET

c. This report indicates the system is operated in "dedicated mode." Jim told me in conversations it was "system high." The answers to Questions 7-11 tend to indicate the system is running in "compartmented mode" IAW DCID 1/16. This may be a fundamental problem that the policy group may need to address.

d. I have not discussed these concerns with Jim.

e. Would you like for me to discuss them with him?



25X1

Attachment: As Stated

25X1

SECRET

Distribution:

Orig-Addee [redacted] The Pymatuning Group, Inc., 2000 L St NW, Suite 702,
Washington D. C. 20036

1-IHC Subject (LGS)

1-IHC Chrono

1-ICS Registry

DCI/ICS/IHC/[redacted] (15 Jul 84)

STAT

STAT

~~SECRET~~

24 JUL 1984

MEMORANDUM FOR: [redacted]

25X1

FROM: [redacted] Chief [redacted]

25X1

Information Systems Security Group, OS

SUBJECT: Response to Computer Security Questionnaire on 4C System [redacted]

25X1

1. Pursuant to your request, we have reviewed and completed the questionnaire on the 4C's computer system. Since the questionnaire was general in nature, certain portions were not applicable to the 4C's system. The Information Systems Security Group, in conjunction with the Chief, Special Security Center, and other Agency components, has attempted to answer the spirit of the questions when none of the listed choices fully described 4C's. [redacted]

25X1

2. Attached to this paper is our response to the questionnaire. Two things should be kept in mind when reviewing our response. First, when multiple choices are available and applicable, our response lists the items which pertain and excludes the others. Second, when the item on the questionnaire did not present an option which best described 4C's, the question or answer has been rewritten so as to be more applicable to the 4C's system and annotated with an asterisk (*). [redacted]

25X1

3. [redacted] is the Information Systems Security Officer for this Project. If there are any questions, he may be contacted on secure [redacted]

25X1

25X1

[redacted]

25X1

~~SECRET~~

RESPONSE TO QUESTIONNAIRE
ON 4C's COMPUTER SYSTEM

1. What is the name of your organization?
Central Intelligence Agency
ISSG/PTAS/OS/DDA
2. Please give a short description of the purpose of function of your system/application.

The 4C system is a single Intelligence Community registry for recording the accesses to compartmented information held by Government and industry personnel and the Government and industry facilities which will provide for storage of compartmented information. The 4C system will provide its services via terminals and remote job entry/printer stations to National Foreign Intelligence Board member agencies and their subordinates.
3. What hardware is used to implement the application/system?
IBM 370/158
4. What operating system is used with the hardware described in 3?
IBM MVS/SP Release 1.3.1
5. Are you using any add-on security packages? If so, which ones?
ACF2
6. What applications development or support system are you using?
GIMS
7. What is the highest classification of data continuously resident on or processed by the system?
Top Secret
* The system is also handling data with the caveat SI and B.
8. What is the lowest classification of data resident on or processed by the system?
Unclassified
* Certain individual entries concerning military personnel and their associated clearances would be at the unclassified level.
9. What is the lowest clearance of individuals who use the systems, OR ITS OUTPUT (reports, messages, etc.)?
Top Secret - SI

- SECRET
10. Which of the following statements BEST describes the classification environment of the system?
 - * e. Two or more compartments and other than compartmented data. The term compartment is used to differentiate access authorization. Everyone on the system is cleared to the highest level. They are not authorized access to certain compartments. 4C's is a dedicated system.
 11. Which of the following statements BEST describes the users of the system, or its products?
 - e. All users and consumers are cleared to the highest level, some users are not approved for some compartments.
 12. Periods processing IS NOT practiced with this system.
 13. Does the system provide a means to control which users may use specific programs, applications or data?
 - b. By classes (e.g., Finance, Project Z people, Managers).
 - c. By (lists of) individuals.
 14. Do the controls make it possible to specify the mode of access of the groups or individuals?
 - d. Yes. They are Read Write, Execute, Append.
 15. Do the controls make it possible to specifically exclude individuals or groups from access to the controlled object.
Yes.
 16. The control(s) are applied by:
 - c. A system administrator.
 - * The applications designer/programmer and the Data Base Administrator specify the control which is to be applied by the system administrator.
 17. The control is enforced by:
 - a. The operating system.
 - b. The application development or support system.
 - c. The application or program.
 18. What percentage of the data and program objects on the system are protected by these mechanisms?
 - e. All.
 19. Does the system reuse data storage media?
 - b. Frequently
 - * Floppy disks are not used on the system but all other storage media (tapes and discs) are reused.

SECRET

20. What preparation is involved in data storage reuse?
- * b. The system erases file names from the temporary directories upon successful job completion or via a utility once a week when a job does not complete successfully.
 - * e. Tapes are overwritten prior to reuse. Floppy disks are not used on the system.
21. Does the system require users to identify themselves before it will initiate a job, accept a program or start an application?
- a. Yes.
22. Does the system have a method to authenticate the users' claimed identity?
- b. Yes. Passwords.
23. Does the identification technique identify individual users?
- a. Yes.
24. Is the users' identity associated with all auditable events?
- Yes.
25. Does the users identity record maintained by the system contain clearance data?
- No.
- * Clearance level/access of a user is determined before access is granted. The user is then assigned to a group for which the security attributes are already established.
26. Does the user's identity record contain authorization data?
- * The GIMS logical file called SYSMAN2 contains authorization data whereby the user is granted access to local data files.
 - * Provisions are available but not implemented to identify access to specific devices (terminals, RJE stations).
27. Is there a trusted communications path between the system and the user for initial logon and authentication?
- Yes.
28. Does the system maintain an audit trail of all users' activities?
- Yes - SMF, ACF2, and GIMS.
29. For which event is an audit record taken?
- a. Logon
 - b. File Open
 - c. Program Initiation

SECRET

- d. File Close
- e. Program Termination
- f. Interactive System Commands
- g. Initialization
- h. System Shut Down
- i. User Logon
- j. System or Hardware Maintenance Activities
 - * Some But Not All Are Audited
- k. System Software Maintenance Actions
 - * Some But Not All Are Audited
- l. Reconfiguration Actions
- m. Security Files Maintenance Actions

30. Audit data is taken for the following classes of users:

- a. Ordinary Terminal Users
- b. Ordinary Batch Users
- c. System Programmers
- d. Operators
- e. System Administrators
- f. System Security Officers
- g. Maintenance Personnel
 - * Some hardware maintenance information is kept via a manual log.

31. The audit event record includes:

- a. User Identification
- b. Job Source
- c. Data and Time of Event
- d. Processor Id
- e. The Event Causing the Record to be Taken
- * f. User privilege level can be determined but the information is not included in the audit log.
- g. File, Program or Command Name or Identification
- * h. The security level of the file referenced can be determined manually but the security level is not included in the audit record.

32. Does your installation use software that permits one to selectively examine audit records based on one or more audit information categories?

Yes - Standard search routines are not available but through the use of RAMIS and other software available on site, routine and exception reports can be performed on information in the audit records.

33. Does the audit mechanism contain a count of security related events beyond which there is an automatic notification to security personnel?

Yes - e.g., three illegal signon attempts cut a security violation audit record.

34. *4C's does not use labeling but access controls are associated with:
- a. Each Data File
 - b. Each User
 - * c. Certain programs or functions in execution (job, process, session).
 - * d. Controls are available but not implemented for devices (terminals, comm channels, RJE stations, etc.).
 - * e. Controls are available but not implemented for printers.
35. The system does not use classification or documentation control labels.
36. Human readable output security labels.
- a. Are applied to output on a case-by-case basis by the users.
37. *Human readable output security labels.
- * b. All VM output requires a user action to assign or override classification assignment at the top and bottom of each page.
 - * c. External users can not generate hardcopy reports on other than controlled slave printers.
38. Does the system enforce a mandatory security policy over all data referencing "subjects" and data storage objects under its control using classifications and dissemination control labels as the basis for making access decisions?
- No.
39. Excluding any long-haul network connections (e.g., through COINS, or IDHSC), how many terminals are connected to the system or application being described?
- c. 51 - 200
- * Total number of terminals.
40. Of the terminals identified in question 39, what percentage have extraordinary privileges associated with the terminal (as opposed to the user or operator of the terminal)?
- a. 0 - 10 Percent
- Only the GIMS Master Terminal, which has a dedicated line, and the OS system console have extraordinary privileges. All other privileges are associated with users and not terminals.
41. A system security plan:
- a. Identifies the security policy that must be followed by the system.
 - b. Defines the maximum security level the system may process.

- d. Defines the minimum physical and procedural security elements that must be established to provide the proper environment for the system.
- e. Identifies the complete set of applicable regulations affecting the system.
- f. States the expected mode (System High, Dedicated) of operation of the system.

42. Intelligent terminals and PC's:

* One not currently authorized on the system but if substituted for a system terminal, the system would not be able to detect. A proposal is currently under study to attach a limited and controlled number of PC's to 4C's.

43. Maintenance Personnel Clearances

b. Some system maintenance persons, while cleared Top Secret, do not have approval for all of the compartments on the system.

44. The last formal "accreditation" of the system (i.e., one with a letter written from the accreditation authority) was written on 22 June 1982 to the Chairman of the 4C's Project. Although the memorandum addressed only the mainframe functions and features, procedures previously distributed require that all connections to 4C's meet predefined standards and be approved by the Chairman of the 4C's Project. No attempt has been made to certify the remote terminal connections.

45. The system is accredited to operate as a:
a. Dedicated Mode System.

46. Is the system connected to a network?
b. There are no network connections.

47. The date and office serial of the last accreditation for the system is:

22 June 1982

Memorandum For:

[Redacted] Chairman, 4C Working Group

From:

[Redacted] Chief

Subject:

Information Systems Security Group, OS
4C's System - Computer Security Design

25X1

25X1

48. The last accreditation of the system was based on:
Participation in the system design by members of the Office of Security, Information Systems Security Group, and an analysis of its features by both the Office of Security and the Office of Data Processing.

49. The letter accrediting the system:
* Addressed the security design and features of the system - not the security levels of information contained in the system.
50. *The system provides data flow controls based on the USER security level.
a. True.
51. Crypto-Keys for dial-up connections to the system are:
e. Not applicable.
* Dial-up connections are not permitted.
52. The integrity of security-related elements of the system software is provided by:
a. All software developers are cleared to the highest level of information processed by the system.
53. Security sensitive system support duties are:
a. Routinely assigned and handled by more than one individual.
* All individuals are cleared to the highest level of information processed by the system.
54. Access approval authorities (system administrators, ISSO's, security administrator, etc.) are able to specify the data object accesses of an individual subject to:
a. Any data object.
b. Specified individual data objects.
55. Access to critical systems and their terminals is controlled by:
a. Physical access controls.
b. Password authentication of user.
56. The system physical environment complies with "U.S. Intelligence Community Standards for SCI Facilities" (i.e., NFIB/NFIC - 9.1/47) dated 23 April 1981.
a. Yes.
57. All individuals with direct access to the systems meet the clearance standards of DCID 1/14.
a. Yes.
58. The system meets the TEMPEST standards of NACSIM 5100A.
e. No.
* The terminals are TEMPEST and meet NACSIM 5100A but the mainframe does not meet the standard, but is in compliance with OC/COMSEC policy.

SECRET

59. All system-to-system and terminal to system communications lines are protected by:
- a. Approved cryptographic equipment.
 - b. Protected wire ways.
 - * e. Terminals are installed in SCIF's. The mainframe is manned 24 hours a day.
60. The average annual growth of primary users of this system over the past 3 years has been:
- d. Greater than 25 percent.
61. This system was installed or last underwent a major hardware or software upgrade:
- b. Between 1 and 5 years ago.
62. Is it is planned to connect this system to a long-haul (e.g., COINS, DDN, etc.) network (or additional networks)?
- * The system is not now nor are there any plans to connect the 4C system to a network.
63. Is it is planned to connect this system to one or more in house local-area networks (or additional networks)?
- * All connections to 4C's are dedicated standalone terminals. The system is not now nor are there any plans to connect the 4C system to a local/in house network.
64. What is your biggest unresolved security problem?
- There are, of course, the standard penetration possibilities by trusted computer operators or systems personnel that face all computer systems but these are negligible in the case of the 4C's system. Based on interviews with system personnel and the project manager, it is our opinion that there are no unusual security problems with the 4C system. The security of the system is based on some of the following features:
- MVS/SP, ACF2, and GIMS features create audit records of transactions and limit unauthorized accesses.
 - Programming is not permitted from remote terminals.
 - Data base changes are limited by access category.
 - Slave printer hardcopy is limited to the information an authorized user is permitted by his/her assigned category.
 - The system is isolated physically and electronically from all other computer systems.
 - Access to the system requires a password and userid.
 - The issuance of passwords and userids is controlled by the data base administrator and changed periodically.

SECRET