CSC input November 1983

Community-Wide Computer Assisted Compartmentation Control System (4C's)

INTRODUCTION:

(C) The 4 C's project is the Intelligence Community-Wide Computer Assisted Compartmentation Control System centralized data base containing compartmented clearance information on personnel within the Intelligence Community as well as contract personnel. The 4 C's project is an attempt to reduce redundant background checks on people and to reduce the amount of paperwork necessary to pass clearance information among members of the Intelligence Community.

SECURITY DEPENDENCY:

(C) Once this system is fully operational, individual records in the system is classified no higher than SECRET, however, the aggregation of all the data will be considered TS/SI. The data base is divided into two portions; a community file which is considered unclassified and open to all subscribers to retrieve at least some data from, and several private SECRET files which are available only to a limited subset of subscribers. The present system, implemented on an IBM 370/158, has connections via dedicated, encrypted lines to 85 terminals spread throughout the Intelligence Community. By 1985, there will be approximately 100 - 110 terminals available. 4 C's uses IBM's Multiple Virtual Storage (MVS) operating system with the GIMS 2 data base management system. All terminal communications are through a dedicated Comten, and all equipment for the system, with the exception of the remote terminals, is contained in a separate room. The system runs in the System High mode of operation. This system, when fully operational, will replace the largely paper-based, man-power intensive manual system now in use.

RISK ASSESSMENT:

(C) 4 C's has several major problems which should be addressed:

(C) 1. Annual Accreditation Requirement: There is no clearly defined accreditation process, nor a delineated accreditation authority for the project. This is a direct result of the fact that there is no clearly identified central authority for this system. Each member of the Intelligence Community who is connected to the system has the authority for entering and maintaining their own data.

(C) 2. System Security Plan and Design Specification and Verification: There are no clearly defined system security requirements, nor a clearly defined system security policy, or an over-all system security plan.

(C) 3. Labels: There is no consolidated internal file labeling scheme for the system. It is questionable whether or not GIMS marks each file with a security label.

CONFIDENTIAL

(C) 4. Audit: Because there is a lack of a consolidated audit package, there is no convenient method to extract applicable audit information from all of the individual audit trails currently being produced.

(C) 5. Object Reuse: There is no provision for mandatory internal or external sanitization of unused storage objects.

RISK REDUCTION:

(C) 1. The appointment of a central authority for the system would help consolidate the security focus for this project. 25X1

(C) 2. A Security Policy statement and a Management review should be done to clearly define the security model, requirements, and practices for this system. / one man-year of effort. 25X1

(C) 3. A scheme for creating and maintaining file and record labels which accurately reflect the classification of the individual file or record must be researched and implemented. 25X1

(C) 4. Funding for software, hardware, and personnel should be made available to create a process by which all audit trail information can be consolidated and made readily available for system security officer use on a timely basis. 25X1

(C) 5. A mandatory method for assuring that all internal and external reused storage objects are cleared should be developed.

25X1

SHORTCOMINGS:

(C) 1. A full-time security officer should be hired whose only concern is overseeing system security. This person should be tasked to review audit trail information on a daily basis and be able to have exception information available on a real-time basis.

(C) 2. An on-line interactive backup capability should be available at an alternate site in case of problems with the primary system.

(C) 3. The software which "sanitizes" data from records is untrusted and should be formally validated and verified. This same software should be placed under strict configuration management control, once validated and verified.