ROUTING AND TRANSMITTAL SLIP Date

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. Alan.	AW	
2. Mgt Staff /AIT		
3.		
4.		
5.		

Action		File		Note and Return
Approval		For Clearance		Per Conversation
As Requested		For Correction		Prepare Reply
Circulate		For Your Information	✓	See Me
Comment		Investigate		Signature
Coordination		Justify		

REMARKS

Here is The evaluation of
The next ISSD "security
program".

will be briefed

5-12-87

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions.

FROM: (Name, org. symbol, Agency/Post) | Room No.—Bldg.

| Phone No.

5041-102 | OPTIONAL FORM 41

STAT

STAT

STAT

FILE-KO Utility Program

The purpose of the FILE-KO Utility Program is to overwrite the file's contents before deleting it.

The DOS Delete or Erase function only marks the file's directory entry with one byte to indicate that the space occupied by that file can be reused. Utilities designed to unerase or undelete a file can return the file's data intact if the space has not been reused.

VERSION TESTED:

FILE-KO Version 3.2 dated 3/25/87

CRITICAL PROBLEMS:

The utility does not check the type of media in the disk drive. The read/write heads of certain drives are only half the width of standard drives. This can result in only a narrow portion of each track being overwritten, leaving residual data in the remaining width of the track. This data is potentially recoverable with special equipment. An example would be deleting a file on a 320/360 Kbyte diskette, in a 1.2 Mbyte drive, that was orginally written by a standard 320/360 Kbyte drive.

The utility only overwrites the portion of the file's allocated space that is determined by the file's data size and adjusted to a sector (512 byte) boundary. Files are allocated space based on clusters which can be a multiple of sectors. This can result in residual data at the end of the file's allocated space which can be recovered simply with the use of a Norton utility. As an example, the 320/360 Kbyte standard allocation format is 2 sectors per cluster. If the file to be deleted is 128 bytes in length, only the first of 2 sectors of the file's allocated space would be overwritten before deletion. The residual data in the last sector could be data remaining from an editing session that reduced the file's size.

SUMMARY:

The utility uses an ANSI.SYS command to clear the standard output device. If the ANSI.SYS driver is not loaded, this results in garbage characters being displayed on the screen. The use of this command assumes that the standard output device is the video monitor but the DOS redirection capability allows the standard output device to be changed which could cause unpredictable results.

The utility uses the archaic architecture of File Control Blocks (FCB's) which does not allow the use of path definitions. This results in action being taken only on files that are in the current or logged on directory.

Files are overwritten once with an ASCII space character. This is not consistent with the DISK-KO utility program which overwrites with alternating writes of binary ones and zeros. After the file is deleted, the directory entry FCB is left intact. This entry contains the file's

1

name, size, date and time last updated or created and the file's starting
sector on the disk. This data should be overwritten after the deletion
function.

SUMMARY:

Before any use or distribution of this program is considered, it should be
rewritten to be consistent with other security utility programs of this
type and to correctly perform its intended purpose.

STAT