SECRET

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Computer Security Report

STAT **FROM:**

Chief, DDA Management Staff
STAT 7D18 HQS

EXTENSION

NO. DA 87-1590

DATE 31 July 1987

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. STAT O/COMPT				STAT
2.				
3.				
4.				
5.				
6.				
STAT 7. STAT				
8.				
9. STAT				
10.				
11.	10-10			
12.				
13.				
14.				
15.				

Attached -- on time -- you will find the Computer Security Report. Regarding paragraph 2, we checked it with Security and we can give no examples, as we did last year, of the program surfacing computer hackers, etc.

Could you work with Leo and see if we can't persuade the IC Staff to settle for a briefing next year instead of going through the tortuous process of writing this report which is really not worth the effort. STAT [redacted] tells me when she had what is probably now [redacted] job, she would work with the IC Staff and give them suggestions on what to include and not include in the guidance letter. Maybe we could save all of us some work.

Distribution:
Orig - Addressee
1 - DDA Registry
1 - DA/MS Subj file
1 - DDA/MCHRONO

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

SECRET

☆ U.S. Government Printing Office: 1985—494-834/49156

CENTRAL INTELLIGENCE AGENCY

COMPUTER SECURITY REPORT

JULY 1987

INTRODUCTION

This report responds to the DCI's 1989-1993 National Foreign Intelligence Guidance, which requires a status report on the computer security efforts from the Intelligence Community agencies. The Central Intelligence Agency's primary goals in 1987 are to improve our auditing capability and to develop an automated data labeling standard for the Agency's mainframe computers.

AUDITING

This Agency firmly believes that a strong auditing program establishes the baseline for an effective information security program. The audit program has grown since November 1986 from three to five man-years dedicated to the auditing of all 12 of our IBM or IBM compatible mainframe automated information systems, including VM, CAMS and 4C. The program serves as a deterrent to would-be computer system abusers and enables us to monitor system activities for abuse, misuse, and violations of established security policy.

25X1

The Agency has also initiated a contract to analyze the audit capability of stand alone word processing systems that are becoming prevalent in our office environment. The contractor will determine how to optimize the systems' audit trail capabilities without degrading system response times to unacceptable levels.

AUTOMATED LABELING

The labeling (classifying) of information is a basic security requirement that is a mandatory national policy regardless of the form used to store the information (paper, electronic, etc.). The access to information is regulated by matching an individual's access rights and clearances to the document's sensitivity labels. The primary differences between labeled paper and labeled electronic data are the system and procedures that allow access to the information.

In the paper world, the control of access to information depends on human checks and balances. With electronic data stored and transferred in automated information systems or contained on magnetic media, the traditional human checks and determinations are, in most cases, no longer applicable. It is up to the computer to make the required access determinations.

Automated labeling will provide a computer the capability to enforce the "need-to-know" principle regarding user access to data. Labeling is a key element that will enforce a deliberate management decision as to what mandatory, discretionary, and flow controls are required for sensitive data stored in ADP equipment. The computer will enforce this process by comparing a user's previously defined clearances and accesses with the label of the data in question and then make a determination as to whether or not access should be granted.

We have taken delivery of the data labeling model contracted for in FY 1986. Following testing we will contract for implementation of the model on the 4C system, one of the Agency's critical systems. The contract will provide (1) a feasibility study for implementing the labeling model, (2) the design specifications for the data label model, and (3) implementation of the label model on the 4C system. If successful, the labeling model will serve as the standard for use within the Agency.

SUMMARY

We will use funds in the FY 1988 Computer Security initiative to continue work in auditing and labeling. We will focus efforts in the outyears (1989-93) on improving the security and control of information processed and stored on personal computers; implementing data labeling on critical systems; evaluating products that could enhance the security of our information system networks; and continuing promising development and engineering efforts in the computer security arena. We will continue to share the results of our efforts with the rest of the Intelligence Community.