ROUTING			
TO:	NAME AND ADDRESS	DATE	INITIALS
1	IC STAFF		
2	[illegible] C/IHC		
3			
4			

	ACTION		DIRECT REPLY		PREPARE REPLY
	APPROVAL		DISPATCH		RECOMMENDATION
	COMMENT		FILE		RETURN
	CONCURRENCE		INFORMATION		SIGNATURE

REMARKS:

FROM: NAME, ADDRESS, AND PHONE NO.	DATE
SAF/SS PENTAGON, RM 4C1052	860213

~~SECRET~~

(Security Classification)

14 FEB 1986

LOGGED

CONTROL NO. _____

COPY 1 OF 2

STAT

Handle Via

TALENT-KEYHOLE

Channels

Access to this document will be restricted to those approved for the following specific activities:

_____ _____ _____ _____

_____ _____ _____ _____

Warning Notice

Intelligence Sources and Methods Involved

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Criminal Sanctions

~~SECRET~~

(Security Classification)

DISSEMINATION CONTROL ABBREVIATIONS

NOFORN-	Not Releasable to Foreign Nationals
NOCONTRACT-	Not Releasable to Contractors or Contractor/Consultants
PROPIN-	Caution-Proprietary Information Involved
USIBONLY-	USIB Departments Only
ORCON-	Dissemination and Extraction of Information Controlled by Originator
REL . . .-	This Information has been Authorized for Release to . . .

Declassified in Part - Sanitized Copy Approved for Release 2014/01/08 : CIA-RDP89B01354R000200210010-6

SECRET

HANDLE VIA
TALENT-KEYHOLE
CONTROL SYSTEM

(S) NATIONAL RECONNAISSANCE OFFICE

WASHINGTON, D.C.

THE NRO STAFF

13 February 1986

MEMORANDUM FOR IC STAFF [redacted] CHAIRMAN, DCI INTELLIGENCE INFORMATION HANDLING COMMITTEE) STAT

SUBJECT: Response to a HAC-Requested Report on Security Implications of Expanded Use of Computers and Office Automation Equipment (DCI/ICS 86-4010 Memo, 17 Jan 86)

This report outlines actions being taken by the NRO to strengthen physical and electronic computer and automated office equipment security.

I believe from your memo you have an understanding of the risks associated with personal computers and word processors.

The following are security measures employed to limit risks to program information handling systems, including word processing and small computers:

a. All employees must be currently accessed and active on program activities.

b. All employees must have received a Special Background Investigation (SBI) less than 5 years old or are in the process of a Periodic Reinvestigation.

c. All employees have received or are subject to a Counter-intelligence polygraph. Those with ADP system manager/operator privileges are subject to periodic polygraphs.

Security procedures employed to limit the risk of compromise by disloyal employees are:

a. All systems are fully enclosed in accredited program areas. No unencrypted links to any other system are permitted and all systems on the net must operate at the same security level.

b. All media and runs must be marked with highest classification at time of creation.

c. All magnetic media are treated as a program level "document" controlled at the highest security level contained on the media. This policy includes floppy discs, removable hard discs, Winchester technology disc systems (when removed from carriers/drive units) and older technologies.

HANDLE VIA
TALENT-KEYHOLE
CONTROL SYSTEM

Classified by:
Multiple Sources

SECRET

DECL: OADR

CONTROL NO [redacted]
COPY 1 OF 2 COPIES
PAGE 1 OF 2 PAGES

STAT

d. All transportation of computer runs and magnetic media is only performed by sponsor approved couriers and controlled at each end.

e. All system users are assigned unique user and application passwords and may use unique lockwords to protect online storage from other users.

f. Selected audits of user files can be conducted by system managers and security staff.

g. All persons granted access to facilities or computer equipment are continually monitored by peers and supervisors for reliability concerns (substance abuse, financial problems, emotional disorders, etc.) and those matters referred to the security or medical staff as required.

h. We comply with DCID 1/16 (Security Policy on Intelligence Information in Automated Systems and Networks).

In regard to resource short falls or problem areas, we identify the following:

a. Because the greatest vulnerability is human personnel failure, we need support for 100% polygraphing.

b. State of the art systems are growing much faster than security staffs or technical security evaluation. Thus, we must continually address the demands on program/engineering staffs to bring new and developing systems on board before full security impact can be assessed. For example, we need to explore safeguards for software when multi-level compartments are within the computer.

c. With budget cuts, additional efforts will rely primarily on administrative and procedural controls.

d. Qualified personnel with background in ADP and computer security are scarce and in high demand both in industry and government.

e. We are exploring the technical solution of marking transportable media with magnetic labels that could be detected when illegally removed from a secure facility.

Questions regarding this response should be directed to Capt [redacted] 25X1

[redacted] 25X1

[redacted] 25X1

CAPT, USN
Deputy for Policy and
Security

STAT

ROUTING			
TO:	NAME AND ADDRESS	DATE	INITIALS
1	IC STAFF		
2			
3			
4			

	ACTION		DIRECT REPLY		PREPARE REPLY
	APPROVAL		DISPATCH		RECOMMENDATION
	COMMENT		FILE		RETURN
	CONCURRENCE		INFORMATION		SIGNATURE

REMARKS:

FROM: NAME, ADDRESS, AND PHONE NO.	DATE
SAF/SS PENTAGON, RM 4C1052	860226

SECRET

(Security Classification)

LOGGED

26 FEB 1986

CONTROL NO. _____

COPY 1 OF 2

STAT

Handle Via

TALENT-KEYHOLE

Channels

Access to this document will be restricted to those approved for the following specific activities:

_____ _____ _____ _____

_____ _____ _____ _____

Warning Notice

Intelligence Sources and Methods Involved

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Criminal Sanctions

SECRET

(Security Classification)

DISSEMINATION CONTROL ABBREVIATIONS

NOFORN-	Not Releasable to Foreign Nationals
NOCONTRACT-	Not Releasable to Contractors or Contractor/Consultants
PROPIN-	Caution-Proprietary Information Involved
USIBONLY-	USIB Departments Only
ORCON-	Dissemination and Extraction of Information Controlled by Originator
REL . . .-	This Information has been Authorized for Release to . . .

Declassified in Part - Sanitized Copy Approved for Release 2014/01/08 : CIA-RDP89B01354R000200210010-6

SECRET

HANDLE VIA
TALENT-KEYHOLE
CONTROL SYSTEM

(S) NATIONAL RECONNAISSANCE OFFICE
WASHINGTON, D.C.

THE NRO STAFF

26 February 1986

MEMORANDUM FOR THE IC STAFF [redacted] CHAIRMAN, DCI INTELLIGENCE INFORMATION HANDLING COMMITTEE) STAT

SUBJECT: Response to a HAC-Requested Report on Security Implications of Expanded Use of Computers and Office Automation Equipment (DCI/ICS 86-4010 Memo, 17 Jan 1986)

REFERENCE: NRO Staff Memo, Same Subject, 13 Feb 1986, [redacted]) STAT

This report provides additional information concerning the numbers of past and future use of personal computers and word processors by our organization. With 1985 considered as the current year, in the past three years we used 16 personal computers and word processors. We project to use in the next three years 569 personal computers and word processors. These systems are or will process intelligence information.

Questions regarding this response should be directed to Capt [redacted] 25X1

[redacted] 25X1

[redacted] 25X1

CAPTAIN, USN
Deputy Director
for Policy and Security

HANDLE VIA
TALENT-KEYHOLE
CONTROL SYSTEM

Classified by:
Multiple Sources

SECRET

DECL: OADR

CONTROL NO [redacted]
COPY 1 OF 2 COPIES
PAGE 1 OF 1 PAGES

STAT