

~~CONFIDENTIAL~~

U.S. DEPARTMENT OF ENERGY  
**memorandum**

DATE **MAR 10 1980**

REPLY TO **DP-353**  
ATTN OF

SUBJECT **Security Protection for Secure Telephones Within the DOE (C)**

TO **Duane C. Sewell, ASDP (DP-1)**  
**Leslie J. Goldman, ASIA (IA-1)**  
**Frank R. Pagnotta, D/OSE**  
**Milton Iredell, SIO, IA**  
**Maj. Gen. William W. Hoover, OMA (DP-20)**

The Office of Safeguards and Security, in cooperation with the Office of Computer Services and Telecommunications Management, is taking steps to identify and correct security insufficiencies for secure telephone systems within DOE Headquarters. Your support and cooperation is needed to accomplish the following plan of action: (C)

1. In the interest of immediate improvement, these steps should be taken by all organizations who control or have access to secure phone systems. (U)
  - a. An individual or small number (2-3) of individuals should be specifically charged with the responsibility for each secure phone. (C)
  - b. Access to areas housing secure phones and/or associated cryptologic units must be strictly controlled at all times. (C)
  - c. No uncleared persons, or persons with a clearance other than Q or TS should be permitted into the area when a secure phone is in use. (C)
  - d. Any suspicious incidents which might indicate misuse or tampering with phones of any type should be reported immediately to the Office of Safeguards and Security. When notifying OSS, do not make any mention of the matter over the phone. Simply request that a Security Officer visit your office. (C)
2. Shortly, a team from OSS and Office of Computer Services and Telecommunications Management will inspect all secure phone installations within DOE Headquarters and identify ways to improve the physical and technical security protection afforded to these systems. The National Security Agency is also being invited to assist in this inspection. It would be helpful if a person from your respective staffs was named to accompany the team during its inspection of your areas. (C)

DEPARTMENT OF ENERGY DECLASSIFICATION REVIEW	
1ST REVIEW DATE: <i>7/1/82</i>	DETERMINATION BY/CLA NUMBER:
AUTHORITY: <i>EO 11652</i>	1. CLASSIFICATION RETAINED
NAME: <i>M. Iredell</i>	2. CLASSIFICATION CHANGED TO:
2ND REVIEW DATE: <i>9/1/82</i>	3. CONTAINS NO DOE CLASSIFIED INFO
AUTHORITY: <i>EO 11652</i>	4. COORDINATE WITH:
NAME: <i>M. Iredell</i>	5. CLASSIFICATION CANCELED
	6. CLASSIFIED INFO BRACKETED
	7. OTHER (SPECIFY): <i>7/1/82</i>

DECLASSIFY  
OR  
 REVIEW ON: 3/3/1986  
(date or event)

~~CONFIDENTIAL~~

~~NATIONAL SECURITY INFORMATION~~  
Unauthorized disclosure of this information may result in Administrative and Criminal Sanctions.

3. When the investigation is completed, a report and recommendations will be made on appropriate corrective measures to be taken to bring the security for secure phone systems into compliance with Intelligence Community requirements. (C)
4. Our greatest security protection is informed staff who are aware of their security responsibilities. Please insure that all personnel who work in secure areas and who have access to secure telephones know the importance of properly using and protecting these encryption systems. (U)

My staff would be pleased to arrange a threat briefing on Communications Security for your personnel. If you are interested, please contact M. J. Dowd, Robert O'Brien or Tim Pflaum at 353-4243. (U)

  
George Weisz  
Director  
Office of Safeguards and Security

cc: William Heffelfinger, AD-1

# ROUTING AND TRANSMITTAL SLIP

Date

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. <i>Frank Pagnotta</i>	<i>[Handwritten Initials]</i>	
2.		
3.	<i>[Handwritten Initials]</i>	
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**

*Frank,*  
*I thought these may*  
*be of interest to the Boss.*

*Dave*

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

<b>FROM:</b> (Name, org. symbol, Agency/Post)	<b>Room No.—Bldg.</b>
	<b>Phone No.</b>



U.S. Department of Energy  
Washington, D.C. 20585

October 9, 1979

MEMORANDUM FOR: Robert T. Duff  
Director  
Office of Classification

FROM: Frank R. Pagnotta *FRP*  
Director  
Office of The Secretary

SUBJECT: ~~Information Security Oversight~~  
Office Semiannual Report

Attached you will find the Semiannual Classification Report for the Office of The Secretary of Energy.

Also please note the corrections made to the list of Authorized Original Classifiers, Authorized Derivative Classifiers and/or Authorized Declassifiers for the Office of The Secretary.

Should you have any questions please contact me directly.

Thanks.

Attachments

*Security*



Department of Energy  
Washington, D.C. 20585

October 11, 1979

MEMORANDUM FOR: The Secretary  
FROM: Frank Pagnotta *FP*  
SUBJECT: Incident Reports

Attached, for your information, is a copy of incident reports regarding Halifax Security Guards in the James Forrestal Building who are under contract to DOE.

I have taken appropriate actions and will follow up and keep you informed.

Instructions have been issued to close the ramp entrance to the Garage at 12th and C Street from Midnight to 5:00am. Entry will be by buzzer and telephone contact with Guards on duty. This should prevent a recurrence of last night's incident in the Garage.

Attachment

**memorandum**

DATE: SEP 27 1979

REPLY TO  
ATTN OF: DP-351SUBJECT: Mandatory Portion Marking of National Security Information (NSI)  
Documents

TO: Those on the Attached Listing

You are reminded of the existing requirement (DOE Order 5650.2, Classification of Information Manual, dated December 12, 1978) for portion marking of documents classified in accordance with Executive Order 12065, and containing no Restricted Data or Formerly Restricted Data.

For your further information, classifiers shall identify the level of classification of each portion of NSI documents (including subjects and titles), and shall also identify those portions that are not classified. Portion marking shall be accomplished by placing, as appropriate, the symbols "TS" for Top Secret, "S" for Secret, "C" for Confidential, and "U" for Unclassified. These symbols shall immediately precede or follow the text to which they apply. Mandatory portion markings apply to NSI documents only. Portion marking need not be observed if all portions are classified at the same level, and a statement to that effect is included in the document. Maps, tape recordings, charts, drawings, matrices, photographs, motion picture films, graphs, microfilms, and microfiche are considered "portions" in themselves.

Requests for portion marking waivers shall be submitted to the Director of Classification.

*Tom Isaac*

George Weisz

for Director

Office of Safeguards &amp; Security

*Security badges*



U.S. Department of Energy  
Washington, D.C. 20585

November 14, 1979

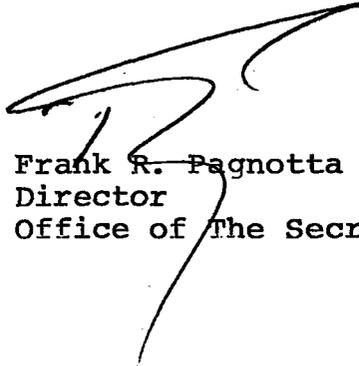
NOTE TO E. F. HEINLEIN

Attached you will find DOE "Q" Personnel Badges for the following Office of The Secretary staff who are now longer with the Department:

- 1) John F. O'Leary
- 2) Dale D. Myers
- 3) Phillip Sam Hughes
- 4) Evelyn C. Irons
- 5) Donald C. Legates
- 6) Kathleen Linehan
- 7) Margaret S. Sellers

As a reminder, Al Richardson of your staff has been preparing for approximately 3 weeks a Q Badge for John M. Deutch, Under Secretary of Energy, with the number 3. I would like to have this Badge for John Deutch provided to me immediately.

Thanks.

  
Frank R. Pagnotta  
Director  
Office of The Secretary

Attachments

*Current x72 of Im file*  
U.S. DEPARTMENT OF ENERGY

# memorandum

DATE February 8, 1980

REPLY TO  
ATTN OF AD-653

SUBJECT Headquarters Computer Security Program—Administrative

TO Assistant Secretaries  
General Counsel  
Assistants to the Secretary  
Administrators  
Directors  
Inspector General  
Controller  
Chairman, FERC  
Office and Division Directors, HQ

00010049 SECRETARIAL OFFICERS SEC OFF  
002 1 COPY

OFFICE OF THE SECRETARY  
DOSE  
RM 7E-054 FORRESTAL

The Office of Computer Services and Telecommunications Management (CSTM) is responsible for developing the Headquarters Computer Security Program. Specific responsibilities are identified in DOE Order 1360.2, Computer Security Program for Unclassified Computer Systems, and DOE Order 5636.2, Security Requirements for Classified Automatic Data Processing Systems. Among other things, these orders require the appointment of a management official to key positions of responsibility for the conduct of the Computer Security Program.

At Headquarters, Mr. Alfred W. Kuebler is temporarily hereby appointed the Computer Protection Program Manager (CPPM) and the Computer Security Operations Manager (CSOM) for all administrative computing. The responsibilities of the CPPM and CSOM are delineated in DOE Orders 1360.2 and 5636.2, respectively. These appointments do not include responsibility for energy data systems which fall under the purview of the Administrator, Energy Information Administration.

While a rather extensive computer security program for classified systems has always been in effect at Headquarters, a new Computer Protection Program Plan has been recently developed. This plan is currently undergoing the review and approval process and is designed to be implemented over the next two to four years. It embraces all of the requirements set forth for the protection of unclassified sensitive data as well as classified data. The plan requires the reexamination of all computer applications and automatic data processing (ADP) hardware installations and is applicable to all in-house (CSTM), commercial timesharing and minicomputer applications at Headquarters.

Our initial efforts to implement the Headquarters Computer Security Program will include the conduct of user security awareness training and a risk analysis of all administrative ADP assets and computer systems serving Headquarters. Additional information and schedules will be provided on these aspects of the program as they develop. In the meantime, you are encouraged to contact Mr. Kuebler should you have any specific questions or if you feel some early remedial actions may be appropriate for your particular system or application.



U.S. Department of Energy  
Washington, D.C. 20585

*Carole* *Security File*  
741

March 12, 1980

MEMORANDUM FOR THE RECORD

I was notified this date (12 March 1980) by Barry Dalinsky that Vito Stagliano was cleared 11 March 1980 for Q.

Security office has been requested to provide him with a permanent I.D. Badge for his trip to Atlanta, Georgia, next week.

A handwritten signature in black ink, appearing to read "Frank R. Pagnotta", is written over the typed name.

Frank R. Pagnotta

(See instructions below)

5

1. ORGANIZATION: (Include correspondence symbol) <i>Office of the Secretary</i>		2. REPORTING PERIOD: (Mo./Yr.) <i>10/1/79 - 9/30/80</i>	
3. PREPARED BY: (Print or type) <i>Conrad J. Gouy</i>		4. TELEPHONE NUMBER: <i>252-5777</i>	

PART A

TYPE OF DOCUMENTS CLASSIFIED			NUMBER OF DOCUMENTS CLASSIFIED		
5. NATIONAL SECURITY INFORMATION (NSI) DOCUMENTS			CONFIDENTIAL	SECRET	TOP SECRET
ACTIONS	5a. ORIGINAL CLASSIFICATION ACTIONS	5b. SIX YEARS OR LESS	<i>3</i>	<i>5</i>	<i>2</i>
		5c. OVER SIX YEARS	<i>0</i>	<i>0</i>	<i>0</i>
	5d. DERIVATIVE CLASSIFICATION ACTIONS		<i>0</i>	<i>2</i>	<i>0</i>
6. RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATA (FRD) DOCUMENTS			<i>0</i>	<i>0</i>	<i>0</i>
7. NUMBER OF AUTHORIZED DERIVATIVE CLASSIFIERS			<i>4</i>	<i>34</i>	<i>34</i>

PART B

8. DESCRIBE EFFORTS TO LIMIT THE AMOUNT OF CLASSIFIED MATERIAL GENERATED:  
*Every effort is made to restrict the incorporation of classified information in written communications*

9. DESCRIBE ACTIONS TAKEN TO LIMIT CLASSIFICATION TO SIX YEARS:  
~~Every effort is made~~ whenever feasible *classified information falls within the category require for classification of only six years.*

10. DESCRIBE MAJOR PROBLEMS ENCOUNTERED IN IMPLEMENTING E.O. 12958:  
*no major problems encountered*

11. SIGNATURE OF PREPARER: <i>Conrad J. Gouy</i>	12. DATE: (Mo./Day/Year) <i>10/24/80</i>
---	---

INSTRUCTIONS

This information is collected under authority of Executive Order 12065 and Information Security Oversight Office (ISOO) Directive No. 1 for use in compiling a DOE semiannual report to the ISOO. Refer to DOE Order 5650.2 "Classification of Information - Manual" for definitions of terms.

Send completed form to the Office of Classification, DP-632.

PART A

Use exact numbers; do not estimate number of documents. If it is impracticable to provide exact numbers, authorization should be requested from the Office of Classification to utilize sampling methods in lieu of an actual count. Use "0" to indicate no entry. Do not leave columns blank.

Item 5. National Security Information (NSI) is separated into three categories for counting: Original Classification Actions (Six

Years or Less vs. Over Six Years) and Derivative Classification Actions.

Item 6. Restricted Data (RD) and Formerly Restricted Data (FRD) are to be counted together.

Item 7. Number of Authorized Derivative Classifiers in your organization certified to classify Confidential, Secret, and/or Top Secret documents. Make entries only for the highest level authorized; i.e., entries for individuals with Top Secret authority shall be shown only under "Top Secret" and not under "Secret" or "Confidential". The same applies to Secret authorities. Do not count Authorized Original Classifiers.

PART B

This area is for your comments. If you have no comments, please indicate so. If additional space is needed, please attach a continuation sheet.

AUTHORIZED REPRESENTATIVES, HEADQUARTERS

(CONTINUED)

OFFICE OF THE SECRETARY

SECRETARY

PAGE 68

DUNCAN CHARLES W JH

8

2 July 1980

Date: 20 June 1980

Place: Guatemala,  
Guatemala City

Assassination of Coca-Cola  
Franchiser in Guatemala

The personnel chief of the Guatemalan Bottling Company, a Coca-Cola franchiser, was assassinated as he was driving in Guatemala City. Unidentified assassins machine-gunned him and fled; the Revolutionary Armed Forces (FAR) claimed responsibility. The bottling company has been involved in conflicts with workers. (U)

Date: 21 June 1980

Place: Guatemala,  
Guatemala City

Coca-Cola Union Secretary Assas-  
inated in Guatemala

The "discipline" secretary of the Coca-Cola union in Guatemala City was shot and killed inside the tightly guarded grounds of the bottling company plant only ten hours after the personnel chief was assassinated. The unidentified killers took the body by truck from the plant area and left it several blocks away. (U)



Department of Energy  
Washington, D.C. 20585

Office of The Secretary  
Telecopier Center  
James Forrestal Building

Xerox 200 Telecopier

Telephone Numbers

Commercial (202) 252-5097

Verification (202) 252-5093

DATE: 10-23-80

TO: Glenda I. Murray DP-632 CXXI 353-4747  
(location) (telephone)

FROM: *Carole J. Gorry* D/OSE Forrestal 252-5777  
Carole J. Gorry (location) (telephone)

This transmittal consists of 2 page(s) -- excluding cover sheet.

Your name: Dee Bordner

Room No.: 7A-219

Ext.: 252-5777

Return Original -- Yes  No

U.S. DEPARTMENT OF ENERGY  
SEMIANNUAL CLASSIFICATION REPORT

(See instructions below)

5

1. ORGANIZATION: (Include correspondence symbol) Office of The Secretary	2. REPORTING PERIOD: (Mo./Yr.) 10/1/79 - 9/30/80
3. PREPARED BY: (Print or type) Carole J. Gorry	4. TELEPHONE NUMBER: 252-5777

PART A

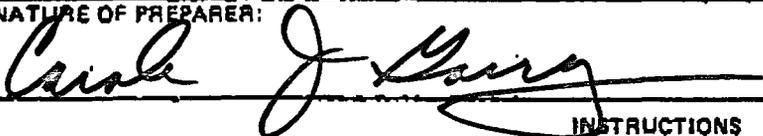
TYPE OF DOCUMENTS CLASSIFIED		NUMBER OF DOCUMENTS CLASSIFIED		
5. NATIONAL SECURITY INFORMATION (NSI) DOCUMENTS		CONFIDENTIAL	SECRET	TOP SECRET
ACTIONS	5a. ORIGINAL CLASSIFICATION ACTIONS	3	5	2
	5b. SIX YEARS OR LESS	0	0	0
	5c. OVER SIX YEARS	0	2	0
6. RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATA (FRD) DOCUMENTS		0	0	0
7. NUMBER OF AUTHORIZED DERIVATIVE CLASSIFIERS		4	4	4

PART B

8. DESCRIBE EFFORTS TO LIMIT THE AMOUNT OF CLASSIFIED MATERIAL GENERATED:  
Every effort is made to restrict the incorporation of classified information in written communications.

9. DESCRIBE ACTIONS TAKEN TO LIMIT CLASSIFICATION TO SIX YEARS:  
Whenever feasible classified information falls within the category requiring classification of only six years.

10. DESCRIBE MAJOR PROBLEMS ENCOUNTERED IN IMPLEMENTING E.O. 12065:  
No major problems encountered.

11. SIGNATURE OF PREPARER:  


12. DATE: (Mo./Day/Year)  
10/22/80

INSTRUCTIONS

This information is collected under authority of Executive Order 12065 and Information Security Oversight Office (ISOO) Directive No. 1 for use in compiling a DOE semiannual report to the ISOO. Refer to DOE Order 5650.2 "Classification of Information - Manual" for definitions of terms.

Send completed form to the Office of Classification, DP-632.

PART A

Use exact numbers; do not estimate number of documents. If it is impracticable to provide exact numbers, authorization should be requested from the Office of Classification to utilize sampling methods in lieu of an actual count. Use "0" to indicate no entry. Do not leave columns blank.

Item 5. National Security Information (NSI) is separated into three categories for counting: Original Classification Actions (Six

Years or Less vs. Over Six Years) and Derivative Classification Actions.

Item 6. Restricted Data (RD) and Formerly Restricted Data (FRD) are to be counted together.

Item 7. Number of Authorized Derivative Classifiers in your organization certified to classify Confidential, Secret, and/or Top Secret documents. Make entries only for the highest level authorized; i.e., entries for individuals with Top Secret authority shall be shown only under "Top Secret" and not under "Secret" or "Confidential". The same applies to Secret authorities. Do not count Authorized Original Classifiers.

PART B

This area is for your comments. If you have no comments, please indicate so. If additional space is needed, please attach a continuation sheet.

AUTHORIZED CLASSIFIERS, HEADQUARTERS

OFFICE OF THE SECRETARY

SECRETARY  
ACTING DEPUTY SECRETARY  
ACTING UNDER SECRETARY  
EXECUTIVE OFFICER

DUNCAN, CHARLES W., JR.  
COLEMAN, LYNN R.  
BATEMAN, C. WORTHINGTON  
GORRY, CAROLE J.

Authorized Top Secret  
Original Classifiers

COUNSELOR TO THE SECRETARY  
EXECUTIVE OFFICER

KELLY, J. MICHAEL  
GORRY, CAROLE J.

Authorized Secret  
Original Classifier

AUTHORIZED DECLASSIFIERS, HEADQUARTERS

OFFICE OF THE SECRETARY

SECRETARY

DUNCAN, CHARLES W., JR.



UNCLASSIFIED ONLY

U.S. DEPT. OF ENERGY

004005

Department of Energy  
Washington, D.C. 20545

930 OCT 22 AM 10 11

MSG. NR. \_\_\_\_\_

(Commcenter Use Only)

Communications Center

Germantown, Maryland

THIS COVER SHEET IS FOR THE TRANSMITTAL OF UNCLASSIFIED MESSAGES ONLY

USE BLACK FELT  
TIP PEN ONLY

XEROX 200 TELECOPIER  
FTS 233-3870  
COMMERCIAL 301-353-3870

REMOVE ALL STAPLES

VERIFICATION  
FTS 233-3486  
COMMERCIAL 301-353-3486

DATE 10-22-80

TO: Carole Jan Gorry D/OST FORSTL. 252-5097  
Name Location Telephone Nr.

FROM: Glenda J. Murray DP-632 CXXI 353-4747  
Name Location Telephone Nr.

THIS TRANSMITTAL CONSISTS OF 5 PAGES. (Excluding Cover Sheet)

I WANT ORIGINAL BACK: YES \_\_\_\_\_ NO

NAME \_\_\_\_\_ EXT.: \_\_\_\_\_ (For Pickup)

OR MAIL STOP \_\_\_\_\_ (If by MAIL)

THIS MESSAGE CONTAINS ONLY UNCLASSIFIED INFORMATION:

Glenda J. Murray  
SIGNATURE

UNCLASSIFIED ONLY

*Blair* (1)

U.S. DEPARTMENT OF ENERGY  
**memorandum**

DATE August 28, 1980

REPLY TO  
ATTN OF DP-632

SUBJECT Information Security Oversight Office Annual Report

TO Those on Attached List

We are gathering information for the Information Security Oversight Office (ISOO) in accordance with Executive Order 12065 and ISOO Directive No.1. In order to prepare a consolidated DOE report, we need for you to fill out the attached DOE Form HQ-F-5650.2 for the period October 1, 1979 through September 30, 1980.

In addition, please provide names, titles and levels of authority (Top Secret, Secret and Confidential) for all authorized Derivative Classifiers in your organization.

Attached for verification is/are list(s) of Authorized Classifiers and/or Authorized Declassifiers for your organization as they appear on our records. Please indicate any changes or corrections that need to be made and return to us with the attached form. All data to be included in the ISOO Annual Report should be submitted to this office by October 15, 1980.

If you have any questions regarding this report, you may contact Glenda Murray (353-4747) or Eric Bragg (353-4748).

*Robert T. Duff*  
Robert T. Duff  
Director  
Office of Classification

Attachments

2

OFFICE OF THE SECRETARY

*officer*  
~~EXEC ASST TO THE DIRECTOR~~

PAGE 6

GORRY CARMIE JAN

*→ Counselor to the  
Secretary*

*J. Michael  
Kelly*

Authorized Secret  
Original Classifier

AUTHORIZED CLASSIFIERS, HEADQUARTERS

3

OFFICE OF THE SECRETARY

*Acting*  
*Acting*

SECRETARY  
DEPUTY SECRETARY  
UNDER SECRETARY  
~~DIRECTOR, OFFICE OF THE SECRETARY~~  
*Executive OFFICER*

*Lynn Coleman*

DUNCAN CHARLES W JR  
~~SARHILL JIM E~~  
~~DEUTEN JIM M~~ *W. Bateman*  
~~PAGNITTA FRANK R~~  
*Carole J. Gorry*

Authorized Top Secret  
Original Classifiers

Secret Original Classifiers

ITERS

(CONTINUED)

OFFICE OF THE SECRETARY

EXEC ASST TO THE DIRECTOR

GORRY CAROLE JAN

Top Secret Original Classifiers

AUTHORIZED CLASSIFIERS, HEADQUARTERS

OFFICE OF THE SECRETARY

SECRETARY

DEPUTY SECRETARY

UNDER SECRETARY

DIRECTOR, OFFICE OF THE SECRETARY

John C. Sawhill

DUNCAN CHARLES W., Jr.

~~BATEMAN WORTH~~

DEUTCH JOHN M

PAGNOTTA FRANK R

AUTHORIZED DECLASSIFIERS, HEADQUARTERS

(CONTINUED)

OFFICE OF THE SECRETARY

SECRETARY

DUNCAN CHARLES W., Jr.

U.S. DEPARTMENT OF ENERGY  
SEMIANNUAL CLASSIFICATION REPORT

(See instructions below)

1. ORGANIZATION: (Include correspondence symbol) <b>Office of The Secretary (OSE)</b>	2. REPORTING PERIOD: (Mo./Yr.) <b>October 1979</b>
3. PREPARED BY: (Print or type) <b>Frank R. Pagnotta, Director, OSE</b>	4. TELEPHONE NUMBER: <b>252-5777</b>

**PART A**

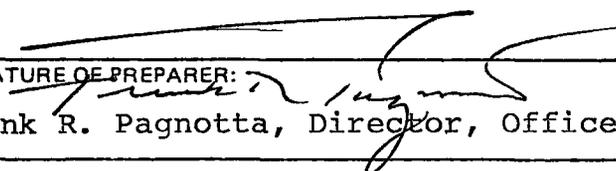
TYPE OF DOCUMENTS CLASSIFIED		NUMBER OF DOCUMENTS CLASSIFIED		
5. NATIONAL SECURITY INFORMATION (NSI) DOCUMENTS		CONFIDENTIAL	SECRET	TOP SECRET
ACTIONS	5a. ORIGINAL CLASSIFICATION ACTIONS	0	0	0
	5b. SIX YEARS OR LESS	0	2	10
	5c. OVER SIX YEARS	0	0	0
5d. DERIVATIVE CLASSIFICATION ACTIONS		0	0	0
6. RESTRICTED DATA (RD) AND FORMERLY RESTRICTED DATA (FRD) DOCUMENTS		0	0	0
7. NUMBER OF AUTHORIZED DERIVATIVE CLASSIFIERS				

**PART B**

8. DESCRIBE EFFORTS TO LIMIT THE AMOUNT OF CLASSIFIED MATERIAL GENERATED:  
**NO COMMENT**

9. DESCRIBE ACTIONS TAKEN TO LIMIT CLASSIFICATION TO SIX YEARS:  
**NO COMMENT**

10. DESCRIBE MAJOR PROBLEMS ENCOUNTERED IN IMPLEMENTING E.O. 12065:  
**NO COMMENT**

11. SIGNATURE OF PREPARER:  <b>Frank R. Pagnotta, Director, Office of The Secretary</b>	12. DATE: (Mo./Day/Year) <b>October 9, 1979</b>
--	--

**INSTRUCTIONS**

This information is collected under authority of Executive Order 12065 and Information Security Oversight Office (ISOO) Directive No. 1 for use in compiling a DOE semiannual report to the ISOO. Refer to DOE Order 5650.2 "Classification of Information - Manual" for definitions of terms.

Send completed form to the Office of Classification, DP-632.

**PART A**

Use exact numbers; do not estimate number of documents. If it is impracticable to provide exact numbers, authorization should be requested from the Office of Classification to utilize sampling methods in lieu of an actual count. Use "0" to indicate no entry. Do not leave columns blank.

Years or Less vs. Over Six Years) and Derivative Classification Actions.

Item 6. Restricted Data (RD) and Formerly Restricted Data (FRD) are to be counted together.

Item 7. Number of Authorized Derivative Classifiers in your organization certified to classify Confidential, Secret, and/or Top Secret documents. Make entries only for the highest level authorized; i.e., entries for individuals with Top Secret authority shall be shown only under "Top Secret" and not under "Secret" or "Confidential". The same applies to Secret authorities. Do not count Authorized Original Classifiers.

**PART B**

Addressees - Memorandum dated 9/4/79

Director, Office of the Secretary  
Assistant Secretary for Energy Technology  
Assistant Secretary for Defense Programs  
Assistant Secretary for Policy and Evaluation  
Assistant Secretary for Resource Applications  
Assistant Secretary for Environment  
Assistant Secretary for Intergovernmental and  
Institutional Relations  
Director, Office of Energy Research  
Controller  
Inspector General  
General Counsel  
Administrator, Energy Information Administration  
Director of Administration  
Director, Office of Procurement and Contracts Management  
Director, Office of Military Application  
Secretary, Federal Energy Regulatory Commission  
Director, Office of Uranium Resources and Enrichment  
Director, Office of Nuclear Waste Management  
Program Director, Office of Nuclear Energy  
Director, Office of Inertial Fusion  
Director, Office of Nuclear Materials Production  
Director, Office of Administrative Services  
Director, Office of Computer Services and  
Telecommunications Management  
Director, Division of Naval Reactors

# memorandum

DATE: September 4, 1979

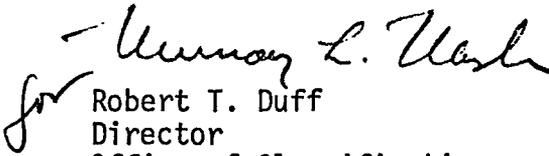
REPLY TO  
ATTN OF: DP-632

SUBJECT: Information Security Oversight Office Semiannual Report

TO: Those on Attached List

Attached is DOE Form HQ-F-5650.2. Please fill out the information requested on this form for the period May 1 through September 30, 1979 and return it to the Program Manager for Policy, Office of Classification (DP-632) by October 10, 1979. This deadline must be met to allow time for the preparation of an overall DOE submission to the ISOO due on October 30. Also attached is a list of the Authorized Original Classifiers, Authorized Derivative Classifiers, and/or Authorized Declassifiers for your organization as they appear in our records. Please annotate the list with any changes that need to be made and return it with the form.

Questions you may have regarding this report should be directed to Eric Bragg (353-4748).

  
for Robert T. Duff  
Director  
Office of Classification

2 Attachments

**ROUTING AND TRANSMITTAL SLIP**

Date **June 12**

<b>TO:</b> (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. Mr. Pagnotta		
2.		
3.		
4.		
5.		

*[Handwritten initials and signatures are present in the routing table, including 'J' and 'see me']*

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**

Sorry you haven't seen this. Here is a copy.

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

<b>FROM:</b> (Name, org. symbol, Agency/Post)	Room No.—Bldg.
	Phone No.

Doug Miller  
*[Handwritten initials]*

5041-102

**OPTIONAL FORM 41 (Rev. 7-76)**  
Prescribed by GSA  
FPMR (41 CFR) 101-11.206



Department of Energy  
Washington, D.C. 20545

MAR 10 1978

TO: Principal Deputy Assistant Secretary, IA  
Deputy Assistant Secretaries, IA  
Office Directors, IA

FROM: IA Security Officer

*Sal Brannello*

SUBJECT: SAFEGUARDING OF CLASSIFIED INFORMATION

As the IA Security Officer, I am establishing certain office and individual procedures to insure that classified information is properly safeguarded.

Under the DOE concept of individual obligations for security, each employee must exercise full responsibility for the proper safeguarding of classified information. Therefore, each of your employees must be completely knowledgeable of the security procedures outlined in Manual Chapter 2105. The concept of individual obligation for security does not release supervisory personnel from their responsibility of assuring that all employees under his or her supervision are kept fully informed as to their security responsibilities.

The following office procedures are effective immediately:

1. Each safe will have an up-to-date sign-out sheet.
2. The names of the supervisor and the individuals responsible for securing and checking the safe must be posted in a conspicuous place on each safe.
3. The individual designated to close the safe shall do so no later than 15 minutes prior to COB each workday. The individual designated to check the safe shall do so at the COB each workday. Each is responsible for designating someone else to make the safe check if unable to do so at the required time. Members of the staff who work beyond normal working hours and require access to classified information are charged with the responsibility for securing their safes and work areas.

MAR 10 1978

4. Identify, in writing, an individual in your office to assume primary responsibility for securing your work area at the close of business. This task may be rotated; however, it is your responsibility to insure that the individual who has this duty is aware of his or her responsibilities during the period of assignment. Please provide me with a copy of your written designation, including periodic updates. The tasks involved in securing an area include checking the sign-out sheets on each safe, physically insuring that each safe is closed, and checking each office area to insure that no classified material has been left unsecured.

As stated above, each IA employee has an obligation for security and accordingly must exercise full responsibility for safeguarding classified information. Listed below are guidelines for individual security procedures:

1. If you must leave your office unattended, insure that access to your office is controlled by an appropriately-cleared person or secure all classified information in your safe. Do not leave classified material in your office unattended after COB.
2. Do not permit any unauthorized individual (charforce, maintenance, etc.) into any area where classified information is or may be exposed unless such individual is under direct observation while in that area and is denied visual access to the information.
3. Do not use open phone lines (non-secure phones) when classified information is being discussed. Do not discuss classified information in any area where someone is using a non-secure phone.
4. Do not commingle classified and unclassified materials in your work area unless you plan to secure all the material in a safe before you leave the office for an extended period or overnight.
5. Keep reference and other unclassified material to a minimum and in clearly defined locations in your work area and clear all desks, tables and mailboxes of paper before leaving for the day to assure no classified material is inadvertently left unsecured.
6. If classified material has been typed on your typewriter, the cassette or ribbon must be removed from the machine at close of business and secured in a safe. Likewise,

MAR 10 1978

- 3 -

all magnetic tape cassettes and other similar memory/ reproduction devices in word processing equipment must be secured in a safe during non-business hours if they hold any classified information.

7. If classified information has been written down on a note pad, the impression will transfer through at least the next two sheets of the pad and the writing can easily be recovered. Therefore, either write classified information on a single sheet of paper or be sure to treat the next two pages under the original as classified waste. The same holds true for typewritten copy.
8. All classified documents transmitted to/from your office must have affixed to the front of the document Form HQ-308, "This Document is Classified." This form should remain with the classified document until it is filed. If copies of the document are reproduced on a copy machine, each copy should have Form HQ-308 affixed to the front of the copy and removed only when the copy is filed or destroyed.
9. Use common sense. Never assume someone is covering for you unless he/she has specifically acknowledged so to you. Don't make office security a problem for your co-workers. Don't leave classified material on another person's desk without advising that person directly.

Please call me if you have any questions.

cc: Each IA Employee  
Mike DeMatteis, DSS

# Command Post Contacts

Control	Forrestal Guard Off.
Eagle One	Sullivan
Eagle Two	Chase Car
Eagle Four	FPS, Sgt Stallworth
Eagle 82	FPS, Officer Tapley
S-1	Heinlein
S-2	Miller
S-5	Carstens
S-10	Richardson
S-19	Security Office
JF-1	Halifax; Lt. Cooper
JF-13	" Coker
JF-14	" 9 <sup>th</sup> St Garage Opener

*Squad Post  
(A/B) wing*

PHOTOGRAPHS REQUIRED

ARTHUR, Elizabeth  
BATEMAN, C. Worthington  
BRILL, Jay R.  
CLARK, LaWanna G.  
COLEMAN, Pati  
DOVEN, Jacqueline  
FISCHER, C. William  
HARAN, Elizabeth  
HARDENBURGH, Sylvia J.  
HENDRICK, Dolores  
HULSEY, Travis  
MARROW, Edward  
LONGENECKER, M. Susan  
NICHOLS, Judith  
PAYNE, Grace  
RATHKOPF, Christina  
UNKLE, Patricia  
WEINER, John  
WISE, Betty

DELETE PHOTOGRAPHS

AMMEN, Helan  
BAILEY, Maryellyn  
BYRNE, Phyllis  
CATAPANO, Andrea  
DELUCA  
ECKLOFF, Winifred  
GRAFF, Vivian  
GRANT, Gordon  
JONES, Hannah  
MASON, Kathleen  
MUEHLEIB, Jo  
KRETZER, Karen  
HILL, Stephen  
POE, Loreen  
PUSATERI, Kenneth  
SMITH, Elizabeth  
WALTERS, Raymond  
YOUNG, John D.  
IRONS, Evelyn  
RITCHIE, Russell

July 30, 1979

DEPARTMENT OF ENERGY PRINCIPALS

James R. Schlesinger, The Secretary  
John F. O'Leary, Deputy Secretary  
John M. Deutch, Acting Under Secretary

SECRETARIAL OFFICERS

Omi Walden, Assistant Secretary, Conservation and  
Solar Applications  
Duane Sewell, Assistant Secretary, Defense Programs  
Charles Williams, Acting Assistant Secretary, Energy  
Technology  
Ruth Clusen, Assistant Secretary, Environment  
P. Sam Hughes, Assistant Secretary, Intergovernmental and  
Institutional Affairs  
Alvin Alm, Assistant Secretary, Policy and Evaluation  
George McIsaac, Assistant Secretary, Resource Applications  
David Bardin, Administrator, Economic Regulatory  
Administration  
Lincoln Moses, Administrator, Energy Information  
Administration  
N. Doug Pewitt, Deputy Director, Office of Energy Research  
Lynn Coleman, General Counsel  
J. Kenneth Mansfield, Inspector General  
C. William Fischer, The Special Assistant to The Secretary,  
Deputy Secretary and Under Secretary  
Frank R. Pagnotta, Director, Office of The Secretary  
C. Worthington Bateman, Deputy Under Secretary  
Jackson Gouraud, Deputy Under Secretary, Commercialization  
Jay R. Brill, Deputy Under Secretary, Strategic Petroleum  
Reserve  
William S. Heffelfinger, Director of Administration  
Jack Hobbs, Controller  
Michael Tashjian, Director of Procurement and Contracts  
Management

FEDERAL ENERGY REGULATORY COMMISSION

Charles B. Curtis, Chairman  
George Hall, Commissioner  
Matthew Holden, Commissioner  
Georgiana Sheldon, Commissioner

July 30, 1979

DEPARTMENT OF ENERGY STAFF OFFICERS

James Bishop, Director, Public Affairs  
Rick Wright, Director, Congressional Affairs  
William Peacock, Director, Intergovernmental Affairs  
Tina Hobson, Director, Consumer Affairs  
Larry Stewart, Director, Office of Education, Business  
and Labor Affairs  
Marion Bowden, Director, Office of Equal Opportunity  
John Farmakides, Chairman, Board of Contract Appeals  
Paul Bloom, Special Counsel  
Melvin Goldstein, Director, Office of Hearings and Appeals  
Christina Rathkopf, Executive Secretary

July 30, 1979

ACCESS LIST  
The Secretary's Area  
7th Floor - Forrestal Building  
(A/B Wing)

SCHLESINGER, James R.  
DUNCAN, Charles W.  
O'LEARY, John F.  
DEUTCH, John M.  
BARTON, Ulysses  
BATEMAN, C. Worthington  
BORDNER, Eldyne  
BRILL, Jay  
BURRIS, Margaret A.  
CLARK, LaWanna  
COOPER, Jeffrey R.  
DEEGAN, Byron  
FELDBAUM, Carl  
FERGUSON, Mary Ann  
FISCHER, C. William  
FOSTER, Carl  
GORRY, Carole J.  
GOURAUD, Jackson  
HANFLING, Robert  
HARAN, Elizabeth  
HARDENBURG, Sylvia, J.  
HERRINGTON, Arthur  
HUDDLESTON, Delores  
JACKSON, Robert  
KAUFMANN, William  
KAY, Brenda B.  
KOZLOWSKI, Michelle

LARKIN, Nancy  
LEGATES, Donald  
LEYSON, Alberto  
LINEHAN, Kathleen M.  
LONGENECKER, Susie  
MADDEN, Lois E.  
MARROW, Edward  
MELVIN, Albert  
OWENS, Ulysses  
PAGNOTTA, Frank R.  
PAYNE, Grace  
POWELL, Colin  
RATHKOPF, Christina  
RIDDLE, Kelly  
RUSH, Gregory  
SELLERS, Margaret S.  
SIBERT, Dennis  
SIEMER, Deanne  
SWANSON, Joyce  
STANFIELD, Jeffrey L.  
TOWNSEND, Frank A.  
VAJDA, Ernest J.  
WALLACE, Carolyn  
WRUBLE, Bernie  
UNKLE, Patricia  
ZAUSNER, L. Andrew

July 30, 1979

ACCESS LIST

The Secretary's Area  
7th Floor - Forrestal Building

OTHER DOE PERSONNEL

ALM, Alvin	LANGENKAMP, Dobie
BARDIN, David	LEGASSIE, Robert
BERGOLD, Harry E., Jr.	LINDEN, Alfred
BISHOP, James	MANSFIELD, J. Kenneth
BLOOM, Paul	MARBLE, Ray
BORRE, Peter	MATHEWS, Colin
BOWDEN, Marion	McISAAC, George
BRATTON, Joseph K.	MILLS, Bernie
BUCAR, Rosemarie	MITCHELL, C. N. "Dean"
CLUSEN, Ruth	MORRIS, Kathleen
COLEMAN, Lynn	MOSES, Lincoln
CORASH, Michelle	NEWLIN, Robert
CURTIS, Charles	PEACOCK, William
DAVIS, William	PECK, Diane
D'ANGELO, Louis	RAUCH, Hilary J.
ELLERMAN, A. Denny	RAY, Stuart
ELLSBREE, Norman	ROBINSON, Douglas
FARMAKIDES, John	RYAN, P. Marshall
FUENTES, Ann	SAVITZ, Maxine
FURSE, James	SCHULE, Robert
FYGI, Eric	SEWELL, Duane
GOLDMAN, Leslie	SHELDON, Georgiana
GOLDSTEIN, Melvin	SILVEY, Jack
GUSTIN, Carl	SMITH, Richard
HALL, George	TASHJIAN, Michael
HANDYSIDE, Holsey	TOLLE, Chris
HARRIS, John	TREAT, John
HEFFELFINGER, William	TUSZKA, Mary
HEINLEIN, Butch	VARRASTERO, Frank
HOBBS, Jack	WALDEN, Omi
HOBSON, Tina	WARD, Erica
HOLDEN, Matthew	WEISS, Stanley
HOUSE, Bart	WILLIAMSON, Thomas
HUGHES, P. Sam	WRIGHT, Rick
HYSTAD, Carlyle	YOHALEM, Harry
JONES, Danny	
JACKSON, Sarah	
JANIS, James R.	

July 30, 1979

THE SECRETARY (S)

Schlesinger, James R.	252-6210	7A-257
Sellers, Margaret S.	252-6210	7A-257
Madden, Lois E.	252-6210	Secretary

Deputy Secretary (DS)

O'Leary, John F.	252-5500	7B-252
Burris, Margaret (Peggy)	252-5500	7B-252
Ferguson, Mary Ann	252-5500	7B-252
Hanfling, Robert I.	252-5700	7B-252
Hardenburg, Sylvia J.	252-5600	7B-252
Huddleston, Dee	252-5700	7B-252
Kay, Brenda	252-5500	7B-252
Linehan, Kathleen M.	252-5600	7B-252
Zausner, L. Andrew	252-5500	7B-252

Under Secretary (US)

Deutch, John M.	252-5704	7B-226
Clark, LaWanna	252-5277	7B-226
Brill, Jay	634-5510	12th & Penn
Gouraud, Jackson S.	252-5266	7B-222
Stanfield, Jeffrey	252-5260	7B-222
Payne, Grace	252-5277	7B-222
Haran, Elizabeth	252-5266	7B-222
Bateman, C. Worthington	252-5270	7B-222
Longenecker, Susie	252-5270	7B-222

Special Assistant

Fischer, C. William	252-6230	7B-260
Unkle, Patricia	252-6230	7B-260
Swanson, Joyce	252-6230	7B-260
Cooper, Jeffrey R.	252-5110	7A-207
Kozlowski Michelle M.	252-6230	7B-260

Director, Office of The Secretary (D/OSE)

Pagnotta, Frank R.	252-5777	7A-219
Gorry, Carole J.	252-5777	7A-219
Anders, Roger M.	252-5235	7G-033
Barton, Ulysses	252-5090	7E-054
Bordner, Eldyne (Dee)	252-5777	7A-219
Buck, Alice J.	252-5235	7G-033
Deegan, Byron	252-5093	7E-074
Digman, Mary B.	252-5561	7E-074
Duncan, Francis	252-5235	7G-033
Foster, Carl A.	252-5562	7E-074
Hewlett, Richard G.	252-5235	7G-033
Holl, Jack M.	252-5235	7G-033
Hulsey, Travis	252-5235	7G-033
Jackson, Robert C.	252-5095	7E-074
Leyson, Alberto D.	252-5090	7E-074
Marrow, Edward	252-5090	7E-074
Melvin, Alvin	252-5095	7E-074
Morris, Kathleen	252-5098	7E-074
Owens, Ulysses	252-5090	7E-074
Riddle, Kelly	252-5777	7A-219
Rush, Gregory R.	252-5563	7E-074
Sibert, Dennis	252-5090	7E-074
Townsend, Frank A.	252-5090	7E-074
Vajda, E. J. (Jim)	252-5090	7E-074
Walthall, Connie H.	252-5090	7E-074
Wise, Betty	252-5235	7G-033

Executive Secretary (ES)

Rathkopf, Christina	252-5230	7A-198
Arthur, Betty Mae	252-5230	7A-198
Gravatt, Patricia	252-5230	7A-198
Coleman, Pati	252-5230	7A-198
Weiner, John	252-5230	7A-198
Banks, Reaskia	252-5075	7E-054
Burch, Michael J.	252-5131	7E-054
Burkins, Joan M.	252-4470	7E-054
Carroll, Sherri	252-5068	7E-054
Coughlin, Janice A.	252-5081	7E-054
Doven, Jacqueline	252-5136	7E-054
Hallion, Marie E.	252-5089	7E-054
Henderson, Deborah "Toby"	252-5074	7E-054
Hendrick, Dolores	252-5914	7E-054
Hodgin, Marilyn K.	252-5132	7E-054
Hooks, Frances	252-5061	7E-054
Hordan, Diane M.	252-5063	7E-054
Irving, Martha A.	252-5073	7E-054
Keister, Anna E.	252-5911	7E-054
Kennedy, Carole Anne	252-4528	7E-054
Laverty, Nancy S.	252-5064	7E-054
Legates, Donald C.	252-5079	7E-054
Lichtman, Gerald N.	252-5137	7E-054
Ludwick, Charlton W.	252-5137	7E-054
Martin, Dora E.	252-5133	7E-054
Neubeiser, Joseph R.	252-5115	7E-054
Nichols, Judith	252-5132	7E-054
Rosser, Richard D.	252-5062	7E-054
Seltzer, Lyn M.	252-5115	7E-054
Walker, Esperanza P.	252-5134	7E-054
Ware, Ethel L.	252-5069	7E-054
West, Yvonne R.	252-5244	7E-054

OFFICE OF SAFEGUARDS AND SECURITY

Organization Chart

Functional Statements

Manpower Requirements

**OFFICE  
OF THE  
DIRECTOR**

**MANAGEMENT SUPPORT  
STAFF**

**DIVISION  
OF  
POLICY AND ANALYSIS**

**THREAT AND RISK  
ANALYSIS BRANCH**

**PROGRAM DEVELOPMENT  
AND REQUIREMENTS  
BRANCH**

**EXTERNAL COORDINATION  
BRANCH**

**DIVISION  
OF  
INCIDENT MANAGEMENT**

**CONTINGENCY PLANNING  
AND RESPONSE BRANCH**

**OPERATIONS CENTER**

**INFORMATION SYSTEMS  
BRANCH**

**DIVISION  
OF  
SAFEGUARDS SYSTEMS  
DEVELOPMENT AND  
IMPLEMENTATION**

**COMPONENT AND SYSTEM  
DEVELOPMENT BRANCH**

**SYSTEMS IMPLEMENTATION  
BRANCH**

**INTERNATIONAL SUPPORT  
BRANCH**

**DIVISION  
OF  
SECURITY**

**FACILITIES SECURITY  
BRANCH**

**INTERNAL SECURITY  
BRANCH**

**OPERATIONS SECURITY  
BRANCH**

**PERSONNEL SECURITY  
ADMINISTRATION BRANCH**

## OFFICE OF SAFEGUARDS AND SECURITY

### DIRECTOR'S OFFICE

This Office is responsible for the direction and conduct of those activities necessary to assure adequate protection and response capabilities for DOE and U.S. energy resources. Included are operations involving DOE nuclear weapons and associated materials and facilities, nuclear and non-nuclear energy-related operations, classified information and valuable government property. In addition, the Office is responsible for providing full safeguards technical support to the U.S. non-proliferation efforts. Activities are designed to: (1) gain a comprehensive understanding of the characteristics and intentions of potential adversaries; (2) identify vulnerabilities within facilities and operations, and the possible consequences if these vulnerabilities are exploited by an adversary; (3) translate the understanding of potential risks posed by potential adversaries into programs, policies, standards, requirements, guidelines, etc., which, when implemented at Headquarters and in the field, will reduce the risks to low, acceptable levels; (4) maintain contingency plans, response capabilities, and an operations center to effectively respond to incidents or emergencies, including assumption, when appropriate, of the directorship of Emergency Action and Coordination Team (EACT); plan and conduct exercises, games, etc., to verify and improve the DOE response capabilities; (5) conduct a research and development program to assist in the design, implementation, and operation of effective safeguards and security components and systems, including liaison and support to the private sector, NRC, IAEA, and the international community; (6) conduct a security program to insure high personnel reliability, effective Headquarters security, adequate protection of classified information, proper control of visitors to DOE operations, operational security, and related activities; (7) maintain the necessary liaison with the NRC, FBI, and DOD, as well as the appropriate Federal, state, and local governments and private industry to effectively coordinate on safeguards and security issues; and (8) maintain an information capability which interacts with relevant components, including the intelligence community to acquire timely information necessary to proper threat characterization, incident response, and non-proliferation initiatives, and, concomitantly channels OSS requirements to the appropriate organizations.

#### Management Support Staff

This Branch is responsible for the budget formulation, presentation, and execution activities for the Office of Safeguards and Security (OSS). This includes the direct funded programs (the Nuclear Materials Security and Safeguards, and the Security Investigations Programs), the "Technical Assistance to the International Atomic Energy Agency," which is primarily a reimbursable work program, and the financial management aspects of the DOE-wide Safeguards Crosscut Program. Also included in this Branch are the administrative

activities including personnel, staffing, travel, time and attendance, space management, centralized mail and files, graphic arts, training, management and manpower studies, and similar services.

### DIVISION OF POLICY AND ANALYSIS

This Division consists of the following Branches:

Threat and Risk Analysis Branch  
 Program Development and Requirements Branch  
 External Coordination Branch

It is responsible for the conduct of those activities necessary to: (1) gain a comprehensive understanding of potential adversaries to DOE resources; (2) determine the vulnerabilities to and consequences of adversarial actions against these resources with national security significance; (3) identify the extent of risks to U.S. national security and public security and well-being arising from the potential successful exploitation of these vulnerabilities; (4) work with other appropriate government and non-government organizations to agree upon cooperation and the split of responsibilities in assuring adequate resource protection and incident response; and (5) prepare and issue programs, policies, guidelines, standards, requirements, etc., within the responsibilities and authorities as identified above which, when implemented, will result in acceptable residual risks.

#### Threat and Risk Analysis Branch

This Branch is responsible for conducting those activities necessary to the timely understanding of the characteristics of potential adversaries to DOE energy and national security resources, and for packaging that information in ways that allow for: effective programs, policies, and standards to be made; adequate and appropriate deterrence, protection, and response systems to be implemented and evaluated; and proper inspections and assessments of security system adequacy to be carried out. This Branch is also responsible for the determination of potential risks to national security and public well-being which might arise due to actions by criminal adversaries against DOE resources. This would include activities to determine the vulnerabilities and the potential consequences to national security or energy adequacy should such vulnerabilities be exploited by an adversary.

#### Program Development and Requirements Branch

It is the primary responsibility of this Branch to conduct the planning necessary for managing the overall safeguards and security program, coordinate the preparation of office planning documents, and formulate

and disseminate policy and guidance in the form of Orders, requirements, standards, etc., which, when implemented, result in satisfactory protection of resources against potential malevolent activities.

#### External Coordination Branch

This Branch is responsible for establishing and maintaining effective liaison between the Office and those other organizations with whom the Office requires continuing effective communication. Liaison and maintaining clear communication and understanding with the FBI, DOD, DOS, etc., are primary responsibilities of this Branch, as well as continuing coordination with other responsible DOE Offices. A primary purpose is to insure adequate liaison with information organizations, including the intelligence community so that Office requirements are formulated and communicated as necessary, and that intelligence information necessary to ensure effective threat characterization, emergency response, and non-proliferation initiatives are received and disseminated in a timely manner. Also important are effective, responsive interactions with cognizant Congressional committees and members, the media, and, as appropriate, private industry, and the public so that there is broad understanding and support for the program which is of particular importance in times of incidents or crises.

### DIVISION OF INCIDENT MANAGEMENT

This Division consists of the following Branches:

Contingency Planning and Response Branch  
 Operations Center Branch  
 Information Systems Branch

It is responsible for assuring that DOE is adequately prepared to effectively respond to nuclear-related incidents or emergencies, including those affecting DOE resources. Included are: (1) the management, maintenance, and operation of the DOE Operations Center (including support to EACT during response to an incident or exercise); (2) the preparation and maintenance of contingency plans which delineate responsibilities and actions to be taken in the event of an incident, including coordination and understanding with other organizations and agencies; (3) the maintenance, improvement, and expansion of response resources, such as the Nuclear Emergency Search Team (NEST); (4) the planning, preparation, and conduct of exercises and tests to gain experience in responding to incidents, verify the adequacy of capabilities, and identify areas of needed improvement; and (5) real-time liaison with the FBI and other agencies in the event of a potential, anticipated, or ongoing incident.

### Contingency Planning and Response Branch

This Branch is responsible for preparing and disseminating those contingency plans necessary so that in the event a nuclear-related incident or emergency occurs, the appropriate individuals and organizations are fully aware of their responsibilities. Included shall be the regular conduct of tests and exercises designed to acquaint decision-makers with the range of incidents that they may have to cope with. The Branch will identify and modify contingency plans or response capabilities to increase our capabilities to respond in case of emergency. This Branch is also responsible for assuring that existing emergency response capabilities are adequate and prepared in the event of a contingency for which they are required. Included, for example, is the management of the NEST capability to enable us to most effectively respond to nuclear-related incidents.

### Operations Center Branch

This Branch is responsible for identifying operations, maintaining all the communications equipment systems and backup support necessary for DOE to be able to effectively carry out its responsibilities to anticipate and respond to incidents and potential emergency situations, and for establishing the necessary procedures and links to assure rapid, secure communications with other response individuals and organizations, as required.

### Information Systems Branch

This Branch is responsible for the management and oversight of the information policies, procedures, and systems necessary for the maintenance of inventory-related information of safeguards relevance. Primary responsibility is for the direction of the Nuclear Material Management and Safeguards System (NMSS). The objectives, scope of responsibility, and proper placement of this function will be a high priority, near-term activity. Any appropriate organizational changes will be made upon resolution of these issues.

## DIVISION OF SAFEGUARDS SYSTEMS DEVELOPMENT AND IMPLEMENTATION

This Division consists of the following Branches:

- Component and System Development Branch
- Systems Implementation Branch
- International Support Branch

It is responsible for activities to support development, implementation, and operation of effective safeguards and security systems. Included

are activities to: (1) test, evaluate, and develop (when necessary) components and subsystems which may form part of safeguards and security systems; (2) work to support DOE programs and, as appropriate, private industry in the development, implementation, and operation of effective systems; (3) develop, refine and apply techniques to evaluate and verify the effectiveness of various systems, with the particular objective of analyzing the relative advantages and disadvantages of candidate systems for protection in terms of effectiveness, cost, operational impact, reliability, etc.; and (4) participate in the U.S. non-proliferation initiatives in the international context through technical and analytical support to the IAEA safeguards function, by the development of safeguards components and systems which minimize proliferation potential (in cooperation with other DOE and government elements), as well as by enhancing IAEA inspection effectiveness, and through bilateral and multi-lateral technical exchanges with other countries charged with the responsibilities of protection of nuclear resources.

#### Component and System Development Branch

This Branch will be responsible for the development and evaluation of components to be used in the safeguarding and protection of vital resources. Included will be components for physical protection, as well as nuclear material control and accountability. These components are then used in the design, development, test, and evaluation of safeguards and security systems. Systems will be designed to increase the effectiveness of existing DOE facilities (both nuclear and non-nuclear) to assist in the incorporation of effective security systems into new DOE facilities, to prepare representative designs of effective safeguards and security systems for potential commercial nuclear facilities, and to support U.S. non-proliferation initiatives. These designs will be closely coordinated with the DOE program managers who are primarily responsible for the systems being secured.

#### Systems Implementation Branch

This Branch is responsible for the implementation of developed safeguards and security systems and technology into DOE programs and operations, and, where appropriate, to private industry. The Branch will evaluate the effectiveness of safeguards and security systems at DOE facilities to determine the increased safeguards benefits to be derived from the application of candidate systems for protection, considering effectiveness, cost, operational impact, reliability, maintainability, etc. Implementation will be closely coordinated, on a continuing basis, with DOE program managers and Safeguards and Security Directors at Headquarters, field offices, and contractor levels. Cost effectiveness evaluations will be performed on safeguards and security upgrading measures of systems identified in annual

budget projections for the various DOE programs. The Branch will be responsible for performing periodic appraisals of the safeguards and security systems at DOE facilities.

#### International Support Branch

This Branch is responsible for research, development and design activities to support the international nuclear community, and in particular, the IAEA. The Branch will coordinate the International Safeguards Project Office (ISPO) activities which provide technical support to the IAEA in order that their inspections may be of maximum effectiveness. This Branch will conduct bilateral and multi-lateral exchanges of information with other nuclear nations, and support U.S. non-proliferation initiatives. They will also provide technical input to policy-related issues being considered with regard to non-proliferation, and will conduct programs to provide timely and responsive input into international activities to maximize non-proliferation, such as follow-on efforts to the International Fuel Cycle Evaluation Program (INFCE).

### DIVISION OF SECURITY

The Division of Security consists of the following Branches:

- Facilities Security Branch
- Internal Security Branch
- Operations Security Branch
- Personnel Security Administration Branch

It is responsible for setting DOE-wide policy and for exercising oversight responsibilities in matters associated with the security of classified information, work, or materials, and in the protection of facilities and installations under the cognizance of the Department. Specifically, this Division engages in activities to assure the proper implementation of security standards and systems at Headquarters and in the field. These responsibilities are carried out through the management of systematic programs for personnel security, internal security, visitor control, physical security, security education and awareness, document and information control, and the coordination of activities associated with violations of Federal statutes affecting the security of Restricted Data, National Security Information, strategic resources or installations.

In addition to DOE-wide oversight responsibilities, the Division manages a program for insuring the reliability of DOE Headquarters personnel in Critical/Sensitive positions, including those requiring

security clearances for access to Restricted Data and National Security Information. This personnel security activity involves the maintenance of DOE-wide budget responsibility for security investigations; a computerized central personnel clearance index system; and the granting of appropriate clearances for members of Congress, Congressional staff, and employees of the Executive Branch in the Washington, D.C., area. The physical security of Headquarters operations and facilities, and the enforcement of security standards at Headquarters contractor installations is an integral part of the Division's areas of concern. The protection of program operations information and including the institution of appropriate countermeasures to preclude the compromise of sensitive data through surreptitious listening devices, emanations and/or the penetration of computer-related activities are also responsibilities of this Division.

The security programs of the Department are administered in accordance with appropriate laws and Executive Orders, including the Atomic Energy Act of 1954, as amended, Executive Orders 10450, 10865, and 12065; and DCI Directives associated with the protection of foreign and compartmented intelligence information.

#### Facilities Security Branch

This Branch is responsible for: (1) conducting surveys and inspections as to the suitability of security systems at DOE and DOE contractor facilities and installations; (2) conducting a program of indoctrinations, and continuing security education and awareness among employees of the Headquarters; (3) administering a program of classified document and information control for the Headquarters, and including operation of the DOE-wide Top Secret central registry; and (4) maintaining a central register of Energy facilities and installations of security interest.

#### Internal Security Branch

This Branch is responsible for: (1) DOE-wide counterintelligence, counterespionage and security violations procedures; (2) conducting intelligence analyses and assessments, and for coordination of intelligence and counterintelligence information affecting DOE classified and sensitive Energy programs with other agencies and within DOE; (3) providing expert technical advice on counterintelligence and counterterrorism responsibilities of the DOE; (4) maintaining liaison relationships with the FBI, CIA, Department of State, and the DOD on central intelligence and internal security matters; and (5) managing a system of control over visits by foreign nationals to DOE classified facilities, and visits by DOE-cleared employees to Communist-bloc nations.

### Operations Security Branch

This Branch is responsible for: (1) the development of Department-wide Operations Security procedures to insure the integrity of sensitive program logistics, plans, and developmental activities; (2) the conduct of research and analyses of activities associated with sensitive departmental programs to insure the continued integrity of such programs; (3) the direction of a Department-wide program for insuring the integrity of communications equipment used in electrical or electronic transmission of classified or official information or material; (4) the coordination of technical and computer security policy with other agency and intelligence community programs; and (5) the maintenance of appropriate technical inspection equipment and conducting inspections of sensitive Headquarters areas.

### Personnel Security Administration Branch

This Branch is responsible for: (1) the development of criteria and procedures for DOE-wide application of personnel security and employee suitability policy; (2) the management of the central Personnel Security Administrative Review Program; (3) the management of the DOE budget controls for security investigative processing; (4) directing the processing of investigations, screening, analysis and adjudication of clearances or suitability for employment in Headquarters cases; (5) conducting the Headquarters reinvestigation program; (6) processing and adjudicating interim access authorization cases, Congressional and other Washington agency employee "Q" clearance actions; (7) managing the central personnel clearance index and personnel security files retention systems; (8) managing the Headquarters visitor control program; and (9) administering the Headquarters Security FOIA and Privacy Act responsibilities.

3/16/79

OFFICE OF SAFEGUARDS AND SECURITY

Manpower Requirements

Director's Office (8)

Director	EES
Secretary	GG-8
Deputy Director	EES
Secretary	GG-8
Deputy Director for Plans	EES
Secretary	GG-8
Special Assistant for NATO Affairs	GG-15
Special Assistant for IAEA Affairs	GG-15

Management Support Staff (9)

Chief	GG-15
Senior Budget & Financial Officer	GG-15
Visual Aid Specialist	GG-12
Administrative Assistant	GG-11
Mail/Records Supervisor	GG-7
Mail/Records Assistant	GG-6
Mail/Records Assistant	GG-6
Mail Clerk	GG-3
Secretary	GG-6

Division of Policy and Analysis (21)

Director	EES
Secretary	GG-7

Threat and Risk Analysis Branch (6)

Chief	GG-15
Senior Threat Analyst	GG-14
Senior Program Manager	GG-14
Policy Specialist	GG-13
Program Coordinator	GG-12
Secretary	GG-6

Program Development and Requirements Branch (8)

Chief	GG-15
Senior Policy Coordinator	GG-14
Senior Program Coordinator	GG-14
Policy Analyst	GG-13
Planning Specialist	GG-12
Program Coordination Assistant	GG-9
Top Secret Control Technician (Stenographer)	GG-7
Secretary	GG-6

External Coordination Branch (5)

Chief	GG-15
Senior Coordination Officer	GG-14/15
Senior Information Specialist	GG-14
Liaison Officer	GG-12
Secretary	GG-6

Division of Incident Management (21)

Director	EES
Secretary	GG-7

Contingency Planning and Response Branch (5)

Chief	GG-15
Exercises and Gaming Specialist	GG-14
NEST Coordinator	GG-14
Contingency Planner	GG-13
Secretary	GG-6

Operations Center (8)

Chief	GG-15
EOC Operator	GG-9
OC Trainee	GG-7
Secretary	GG-5

Information Systems Branch (6)

Chief	GG-15
Operations Manager	GG-14
Nuclear Materials Accountant	GG-14
Systems Analyst	GG-11
Systems Analyst	GG-9
Secretary	GG-6

Division of Safeguards Systems Development and Implementation (19)

Director	EES-17
Technical Information Specialist	GG-9
Secretary	GG-7
 <u>Component and System Development Branch (6)</u>	
Chief	GG-15
Physical Protection Specialist	GG-14
Materials Control & Accountability Specialist	GG-14
Systems Design Engineer	GG-13/14
Systems/Operational Control Analyst	GG-13
Secretary	GG-6
 <u>Systems Implementation Branch (5)</u>	
Chief	GG-15
Systems Application Engineer	GG-14
Materials Control & Accountability Specialist	GG-14
Physical Protection Operations Officer	GG-11
Secretary	GG-6
 <u>International Support Branch (5)</u>	
Chief	GG-15
Policy Liaison Specialist	GG-14/15
International R&D Support Officer	GG-14
International Liaison Officer	GG-11
Secretary	GG-6

Division of Security (43)

Director	EES
Secretary	GG-7
 <u>Facilities Security Branch (11)</u>	
Chief	GG-15
Senior Security Specialist	GG-14
Security Specialist/Administration	GG-11/13
Security Specialist/Administration	GG-11/13
Security Specialist/Physical Security	GG-11/13
Security Specialist/Physical Security	GG-11/13
Secretary	GG-7
Receptionist 1/	GG-6/7
Receptionist 1/	GG-6/7
Receptionist 1/	GG-6/7
Clerk Stenographer	GG-5

1/ Three receptionists, presently included in the Office of Safeguards and Security's ceiling, are proposed for transfer to the Office of Administrative Services.

Internal Security Branch (6)

Chief	GG-15
Internal Security Specialist	GG-14
Intelligence Security Specialist	GG-11/13
Intelligence Analysis Specialist	GG-11/13
Secretary	GG-6
Clerk/Stenographer	GG-5

Operations Security Branch (5)

Chief	GG-15
OPSEC Analyst	GG-13
Technical Security Specialist	GG-11/13
Computer Security Specialist	GG-11/13
Secretary	GG-6

(Personnel Protection Officers) 2/

Personnel Security Administration Branch (19)

Chief	GG-15
Secretary	GG-6

Headquarters Personnel Security Section

Section Chief	GG-14
Personnel Security Analyst	GG-11/13
Personnel Security Analyst	GG-11/13
Case Screener	GG-7/9
Case Screener	GG-7/9
Security Administration Supervisor	GG-9
Pre-Screening Clerk	GG-6
Security Clerk	GG-5
Security Clerk	GG-5

---

2/ The question of where the Security detail for the personal protection of the Secretary and/or other Secretarial Officers remains to be decided by the Office of the Secretary, as does the number of staff officers (3-4 proposed) required to perform this function.

Budget & Administration Review Section

Section Chief	GG-14
Personnel Security Specialist	GG-11/13
Personnel Security Specialist	GG-11/13
Administrative Assistant	GG-7
CPCI Chief	GG-9
CPCI Clerk	GG-5/7
CPCI Clerk	GG-5/7
CPCI Clerk	GG-5/7

*Security*

U.S. DEPARTMENT OF ENERGY

**memorandum**

DATE: April 12, 1979

REPLY TO  
ATTN OF: DP 345

SUBJECT: Security Infractions

TO: Frank Pagnotta

Reference your memo of April 10, 1979 concerning the above subject, this office has carefully documented and monitored each violation for appropriate follow-up. There have been nine actual infractions during the first quarter of 1979, two in January, five in February and two in March.

In each case the responsible person was identified, and follow-up interviews were conducted, or weak security procedures were identified and corrected. Additionally, this office has implemented a security education program to acquaint selected DOE employees with proper classified handling procedures.

*E. F. Heinlein/oxm*

E. F. Heinlein, Chief  
Washington Security Office

*4/14/79*  
*Butch*  
*good*  
*has been passed*  
*[Signature]*

FRP 4/10/79 Memo

*Due*  
*Security Gate* (3)  
11/18/78

OCT 2 1978

**Principal Staff, DOE Headquarters**

**SECURITY INSPECTION OF DOE HEADQUARTERS OFFICES AND FACILITIES**

During the period October 11-20, 1978, a team of DOE Security Experts will conduct a security inspection of Headquarters offices and facilities having national security interests. The inspection team, which has been drawn from the Nevada, Albuquerque and Savannah River Operations Offices of the Department, will concentrate their efforts on an assessment of the security protection being afforded classified national security interests at the various Headquarters buildings. The team members will endeavor to examine classified document accountability, records and systems, physical security measures in effect at our respective buildings, and the measures being taken by the various Headquarters offices which have national security responsibilities in the implementation of Departmental security policies and procedures.

The team leader, Mr. Thomas Blankenship, Director of Safeguards and Security at the Nevada Operations Office, and/or representatives of his team will be in communication with your respective offices on the scheduling of appropriate meetings and/or security reviews.

I request that you provide Mr. Blankenship and his team with your utmost cooperation during the inspection period in order that the work of the team may be accomplished in the most expeditious and efficient manner. It is suggested that you assign the responsibility for oversight of security administrative matters within your organization to a specific staff officer who may be in a position to effect the necessary liaison with Mr. Blankenship and his team during the inspection.

In the event there are any questions on this matter, please feel free to contact this office.

**H. E. Lyon, Director  
Office of Safeguards and Security**

bcc: D. M. Kerr, O/ASDP  
T. Blankenship, SS, NV  
H. J. Badini, OSS

bcc: F. R. Pagnotta, OSE ✓  
W. J. McDonald, O/IA

*[Handwritten signature]*  
ASA  
L.Dowd/mbs  
9/28/78

DEP DIR  
LMBrenner  
9/ /78

DIRECTOR  
HELyon  
9/ /78

**U.S. Department of Energy**  
**Washington, D.C.**

**ORDER**

DOE 5631.2

11-13-80

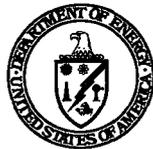
SUBJECT: PERSONNEL SECURITY PROGRAM

1. PURPOSE. To implement the provisions of the Atomic Energy Act of 1954, as amended, and Executive Orders 10450, 10865, and 12065.
2. CANCELLATION. Interim Management Directive No. 6101, PERSONNEL SECURITY PROGRAM, of 9-29-77.
3. SCOPE. The provisions of this Order apply to all Departmental elements, including the Federal Energy Regulatory Commission.
4. BACKGROUND. The Personnel Security Program of the Department of Energy applies to its employees and contractors, as follows:
  - a. The provisions of the Atomic Energy Act of 1954, as amended, Executive Orders 10450 and 12065, and Federal Personnel Manual chapter 732 apply to Departmental employees, applicants for employment, consultants, employees of other Federal agencies, and assignees for employment and access; and
  - b. The provisions of the Atomic Energy Act of 1954, as amended, and Executive Orders 10865 and 12065 apply to Departmental contractors, subcontractor employees and consultants, and access permittees for access.
5. REFERENCES.
  - a. Atomic Energy Act of 1954, as amended, Section 143, "Department of Defense Participation," Section 145, "Restrictions," and Section 161.b, "General Provisions," which are the legislative requirements for establishment of a DOE security program for controlling access to Restricted Data and special nuclear material.
  - b. 10 CFR Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material," as published in the "Federal Register", Vol. 42, No. 190, of 9-30-77, which is used in those cases in which there are questions of eligibility for DOE access.
  - c. DOE 1360.2, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS, of 3-9-79, which established policies and procedures for developing, implementing, and administering a program for safeguarding DOE computer systems and in particular, DOE sensitive unclassified information.

DISTRIBUTION:  
All Departmental Elements  
Federal Energy Regulatory Commission

INITIATED BY:  
Office of Safeguards  
and Security

- d. Executive Order 10450, of 4-27-53, as amended, which established the requirement for determining that all Federal employees be loyal, reliable, trustworthy, and of good conduct and character.
  - e. Executive Order 10865, of 2-24-60, as amended which established the basis for industrial security program for civilian personnel.
  - f. Executive Order 12065, of 12-1-78, which established the restriction for access to classified information.
  - g. Federal Personnel Manual, Chapter 731, "Suitability," which contains requirements for employment by the Government regarding the character, reputation, and fitness of the individual under consideration.
  - h. Federal Personnel Manual, Chapter 732, "Personnel Security Program," which implements Executive Order 10450 throughout Federal departments and agencies.
  - i. Federal Personnel Manual, Chapter 736, "Investigations," which deals primarily with national agency checks and inquiries (NACI) and full field investigations conducted by the Office of Personnel Management.
  - j. Federal Personnel Manual Letter 732-7, "Personnel Security Program for Position Associated with Federal Computer Systems," which establishes policy for a personnel security program covering positions that are involved in the design, storage, retrieval, access, and dissemination of information maintained in Federal computer systems, as well as positions associated with automated decisionmaking systems.
  - k. Office of Management and Budget Circular No. A-71, "Security of Federal Automated Information Systems," of 7-27-78, with Transmittal No. 1, which promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.
6. IMPLEMENTATION. Additional implementation procedures will be published as necessary as extra chapters. These chapters will be coordinated separately.



William S. Heffelfinger  
Director of Administration

TABLE OF CONTENTS

	<u>PAGE</u>
<u>CHAPTER I - DEFINITIONS</u>	
1. Access .....	I-1
2. Access Authorization or Security Clearance .....	I-1
3. Access Permittee .....	I-2
4. Classified Information .....	I-2
5. Derogatory Information .....	I-2
6. Formerly Restricted Data .....	I-3
7. Hearing Counsel .....	I-3
8. Interim Access Authorization .....	I-3
9. National Security Information .....	I-3
10. Naval Nuclear Propulsion Information .....	I-3
11. Personnel Security Board .....	I-3
12. Position Sensitivity Designation .....	I-3
13. Restricted Data .....	I-3
14. Security Area .....	I-4
15. Sensitive Data .....	I-4
16. Sensitive Position .....	I-4
17. Special Nuclear Material .....	I-4
 <u>CHAPTER II - RESPONSIBILITIES AND AUTHORITIES</u>	
1. The Secretary .....	II-1
2. The Assistant Secretary for Defense Programs .....	II-1
3. Heads of Departmental Elements and Chairman, Federal Energy Regulatory Commission .....	II-2
4. General Counsel .....	II-2
5. Heads of Headquarters Elements .....	II-2
6. Director of Personnel .....	II-3
7. Director of Safeguards and Security .....	II-3
8. Heads of Field Organizations .....	II-5
 <u>CHAPTER III - POSITION SENSITIVITY DESIGNATIONS</u>	
1. General .....	III-1
2. Categories .....	III-1
a. Department of Energy Employees, Applicants for Employment, Consultants, and Assignees .....	III-1
b. DOE Contractor and Subcontractor Employees and Consultants and Access Permittees .....	III-3
c. Other Federal Department or Agency Employees .....	III-4

3. Sensitive Compartmented Information ..... III-5  
4. General Guidelines ..... III-5

CHAPTER I  
DEFINITIONS

1. ACCESS.

- a. The knowledge, use, or possession of classified information or other sensitive information not protected by National Security regulations which is required by an individual in the performance of official duties and which is provided to the individual on a "need-to-know" basis; or
- b. Situations involving the responsibilities of an individual in the performance of official duties which may provide proximity to or control over special nuclear material in Category I or II quantities.

2. ACCESS AUTHORIZATION OR SECURITY CLEARANCE. An administrative determination that an individual who is either a DOE employee, applicant for employment, consultant, assignee, other Federal department or agency employee (and other persons who may be designated by the Secretary of Energy) or, a DOE contractor or subcontractor employee, is eligible for access to Restricted Data, other classified information, or special nuclear material. Clearances granted by the DOE are designated as "Q," "L," "Top Secret," or "Secret."

- a. "Q" access authorizations or clearances are based upon full field investigations conducted by the Federal Bureau of Investigation, Office of Personnel Management, or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need-to-know" basis, to Top Secret, Secret and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of duties. When "Q" access authorizations or clearances are granted to employees of access permit holders they are identified as "Q(X)" access authorizations or clearances and permit access only to the type of Secret Restricted Data specified in the permit.
- b. Top Secret access authorizations or clearances are based upon full field investigations conducted by the Office of Personnel Management or another Government agency which conducts personnel security investigations. They permit an individual to have access, on a "need-to-know" basis, to Top Secret, Secret, Confidential National Security Information, and Formerly Restricted Data as required in the performance of duties.
- c. "L" access authorizations or clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks (NAC) for non-Federal employees, conducted by the Office of

Personnel Management. They permit an individual access, on a "need-to-know" basis, to Confidential Restricted Data, Secret and Confidential, Formerly Restricted Data, or Secret, and Confidential National Security Information, required in the performance of duties, provided such information is not designated "CRYPTO" (classified cryptographic information), other classified communications security ("COMSEC") information, or intelligence information. When "L" access authorizations or clearances are granted to employees of permit holders, they are identified as "L(X)" access authorizations or clearances and permit access only to the type of Confidential Restricted Data specified in the access permit. Additionally, the cognizant DOE official may grant an "L" access authorization or clearance to craft or manual workers, community management and service personnel, nurses, medical technicians, cafeteria workers, health and safety workers, purchasing and accounting groups, and the like, who are employed in classified construction or operations areas; provided the work of such individuals do not afford them:

- (1) More than visual access to buildings and equipment classified not higher than Secret Restricted Data; or
- (2) Access to information classified higher than Confidential Restricted Data concerning plant operating characteristics, process data, weapons, or weapons components.

d. Secret access authorizations or clearances are based upon National Agency Checks and Inquiries (NACI) for Federal employees, or National Agency Checks (NAC) for non-Federal employees, conducted by the Office of Personnel Management. They permit an individual access on a "need-to-know" basis, to Secret and Confidential National Security Information as required in the performance of duties.

3. ACCESS PERMITTEE. An individual or organization which has been issued a permit by the Department of Energy, providing access to Restricted Data applicable to civil uses of atomic energy in accordance with the terms and conditions stated on the permit and in accordance with applicable security regulations.
4. CLASSIFIED INFORMATION. Any information which requires protection against unauthorized disclosure in the interests of the national defense and security or foreign relations of the United States pursuant to U.S. Statute or Executive order. The term includes Restricted Data, Formerly Restricted Data, and National Security Information, each of which has degrees of importance denoted by the classifications Top Secret, Secret, or Confidential.
5. DEROGATORY INFORMATION. Unfavorable information concerning an individual which creates a question as to the individual's eligibility or continued eligibility for access or employment.

6. FORMERLY RESTRICTED DATA. Classified information jointly determined by the Department of Energy (or its predecessors, the Atomic Energy Commission and the Energy Research and Development Administration) and the Department of Defense to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.
7. HEARING COUNSEL. A DOE attorney assigned to prepare and conduct Personnel Security Board Hearings.
8. INTERIM ACCESS AUTHORIZATION. A determination by the Secretary, for access to National Security Information, or by the Assistant Secretary for Defense Programs, for access to Restricted Data, that it is clearly consistent with the national interest for the DOE to permit an individual to have such access prior to the DOE's receipt of full field reports of investigation. Interim Access Authorizations are not processed for Access Permittees or for those individuals whose accesses will require an "L" or Secret clearance.
9. NATIONAL SECURITY INFORMATION. Information which requires protection in the interest of national defense or foreign relations of the United States and classified in accordance with an Executive order which does not fall within the definition of Restricted Data or Formerly Restricted Data.
10. NAVAL NUCLEAR PROPULSION INFORMATION. All information classified or unclassified concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships, including the associated nuclear support facilities.
11. PERSONNEL SECURITY BOARD. A board appointed by the Head of a Field Organization to make findings and recommendations in granting access authorization to an individual which consists of three members, one of whom shall be designated chairperson.
12. POSITION SENSITIVITY DESIGNATION. A written certification by the appropriate DOE official that a position under his or her jurisdiction (to be occupied by a DOE employee, applicant for employment, consultant, or assignee) is critical-sensitive, noncritical-sensitive, or nonsensitive.
13. RESTRICTED DATA. Data which is defined in section IIy of the Atomic Energy Act of 1954, as amended, as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but

shall not include data declassified or removed from the Restricted Data category pursuant to section 142."

14. SECURITY AREA. A physically defined space containing classified matter (documents or material) or special nuclear materials subject to physical protection and personnel access controls.
15. SENSITIVE DATA. Information requiring a degree of protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data, sensitive energy data, sensitive financial or supply data, and so forth).
16. SENSITIVE POSITION. Any position in the DOE affected by, connected with, or related to the national security or welfare; i.e., a position whose occupant could, by virtue of the nature of such a position, bring about a materially adverse affect on the national security as prescribed in Executive Order 10450 and the Atomic Energy Act of 1954, as amended.
17. SPECIAL NUCLEAR MATERIAL. Special nuclear material, as defined in section II.aa of the Atomic Energy Act of 1954, as amended, not subject to a Nuclear Regulatory Commission license. For the purpose of this Order, special nuclear material in one facility or shipment is divided into the following categories:
  - a. Category "I" Quantities of SNM.
    - (1) Uranium 235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with Plutonium and Uranium 233 when (multiplying the Plutonium and Uranium 233 content by 2.5) the total is 5,000 grams or more.
    - (2) Plutonium and Uranium 233 when the Plutonium and Uranium 233 content is 2,000 grams or more.
    - (3) SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities in Items (a) or (b) of this category.
  - b. Category "II" Quantities of SNM.
    - (1) Uranium 235 (contained in Uranium enriched to 20 percent or more in the isotope U-235) alone, or in combination with Plutonium and Uranium 233 (multiplying the Plutonium and/or Uranium 233 content by 2.5) when the total is 1,000 to 4,999 grams.

- (2) Plutonium and Uranium 233 when the Plutonium and Uranium 233 content is 400 grams to 1,999 grams.
- (3) SNM in lesser quantities but which is located in the same area or shipment with other SNM with which it could be selectively combined to produce the equivalent quantities in subparagraphs (1) or (2) of this category.



.

.



CHAPTER II  
RESPONSIBILITIES AND AUTHORITIES

1. THE SECRETARY shall:

- a. Certify those specific positions which are of a high degree of importance or sensitivity under section 245f of the Atomic Energy Act of 1954, as amended, which are to be subject of an investigation by the Federal Bureau of Investigation.
- b. Designate those specific positions within DOE which are sensitive under section 3(b) of Executive Order 10450.
- c. Authorize, in the case of emergency, and for a limited period of time, a sensitive position (including either critical-sensitive or noncritical-sensitive) to be occupied within the DOE by an individual for whom a preappointment full field investigation has not been completed, if such action is necessary in the national interest under section 3(b) of Executive Order 10450.
- d. Grant authorization for access to National Security Information pursuant to section 4-201 of Executive Order 12065 prior to completion of the required investigation when it has been determined that such action is in the national interest.
- e. Establish standards and specifications in writing as to the scope and extent of investigations under section 145g of the Atomic Energy Act of 1954, as amended.
- f. Make determinations required by 10 CFR part 710.27(m)(2)(ii) and 10 CFR part 710.33.

2. THE ASSISTANT SECRETARY FOR DEFENSE PROGRAMS shall:

- a. Grant authorization for access to Restricted Data pursuant to Section 145b of the Atomic Energy Act of 1954, as amended, prior to completion of the required investigation when he has determined that such action is in the national interest.
- b. Direct the suspension of access authorization in accordance with 10 CFR part 710.21.
- c. Issue subpoenas to witnesses in all cases processed in accordance with 10 CFR part 710.20 et seq.

- d. Act as "special designee" under 10 CFR part 710.27(m)(2)(j) to determine whether statements may be received by Personnel Security Boards and determine whether new evidence may be received in accordance with 10 CFR part 710.29(b)(2).
  - e. Submit records in Administrative Review proceedings in accordance with 10 CFR part 710.30(d)(2) and (e).
  - f. Grant, deny, or revoke access authorization in accordance with 10 CFR part 710.24(a) and 710.32.
  - g. Approve reconsideration of access authorization cases in accordance with 10 CFR part 710.34.
  - h. Select and appoint the individuals who offer findings and recommendations in administrative review cases in accordance with 10 CFR part 710.31.
3. HEADS OF DEPARTMENTAL ELEMENTS AND CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION shall:
- a. Generate requests to the Secretary for waivers of preappointment full field investigation requirement for candidates under consideration to occupy a critical-sensitive position which does not require access to Restricted Data.
  - b. Generate requests to the Secretary or the Assistant Secretary for Defense Programs, through the Director of Safeguards and Security, for Interim Access Authorizations.
4. GENERAL COUNSEL shall:
- a. Approve notification letters to individuals whose eligibility for access authorization is in question in accordance with 10 CFR part 710.22.
  - b. Concur in request for issuance of subpoenas to witnesses in cases processed in accordance with 10 CFR part 710.20 et seq.
  - c. Concur in request for suspensions in cases processed in accordance with 10 CFR part 710.21.
5. HEADS OF HEADQUARTERS ELEMENTS shall:
- a. Certify, in writing to the Director of Personnel, Position Sensitivity Designations for each position under their jurisdiction to be occupied by a DOE employee or applicant for employment, consultant, or assignee.

- b. Approve and transmit to the Director of Safeguards and Security, Headquarters, requests for access authorization of employees of other Federal departments or agencies who require access to Restricted Data.
  - c. Approve and transmit to the Director of Safeguards and Security, Headquarters, applications for access authorizations for foreign nationals.
  - d. Furnish Data Report on Spouse (DOE Form DP-354) for personnel under their jurisdiction who possess an access authorization.
  - e. Approve and transmit to the Director of Safeguards and Security, Headquarters, requests for access authorizations for members of the Armed Forces and civilian employees of the Department of Defense and the National Aeronautics and Space Administration assigned to duty with DOE Headquarters organizations, for access to Restricted Data.
6. HEADQUARTERS, DIRECTOR OF PERSONNEL shall:
- a. Receive position sensitivity designations for Headquarters positions and provide copies of certifications to the Director of Safeguards and Security, Headquarters.
  - b. Process all requests for investigations for DOE Headquarters employees, applicants for employment, consultants, and assignees to the Director of Safeguards and Security, Headquarters.
  - c. Determine final action to be taken in those cases where questionable suitability information is developed.
7. HEADQUARTERS, DIRECTOR OF SAFEGUARDS AND SECURITY shall:
- a. Develop policy, objectives, standards, guides, and procedures for the DOE Personnel Security Program.
  - b. Authorize Heads of Field Organizations to initiate security investigations relative to foreign nationals who are applicants for security clearance.
  - c. For cases processed in accordance with the provisions of 10 CFR part 710.20 et seq. and 10 CFR part 710.38, perform the functions assigned to the Director of Safeguards and Security, Headquarters, and make recommendations to the Assistant Secretary for Defense Programs as appropriate.
  - d. Process all requests by other Government agencies for verification of an individual's DOE security clearance status.

- e. Maintain centralized records for all DOE security clearance actions.
- f. Coordinate requests by the Inspector General for access to personnel security information for investigative purposes.
- g. For Headquarters, approve and maintain records of review of personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.
- h. Recommend to the Controller funding necessary for conducting personnel security investigations.
- i. Maintain liaison with the Federal Bureau of Investigation and the Office of Personnel Management and is principal point of contact with these agencies on all personnel security matters.
- j. Notify the Federal Bureau of Investigation or Office of Personnel Management of withdrawals of requests for investigation.
- k. Initiate:
  - (1) Investigation of spouses of individuals who marry after having been processed for an access authorization.
  - (2) Appropriate investigation and grant access authorizations for access to Restricted Data for:
    - (a) Personnel of the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) assigned for duty with DOE or DOE contractors or with other Federal departments or agencies, and
    - (b) Employees of other Federal departments or agencies who require such access.
- l. Accept properly executed certifications for DOD and NASA personnel assigned for duty with DOE who require access to Restricted Data.
- m. Concur in requests to the Secretary for waivers of preappointment full field investigation requirements for candidates under consideration to occupy critical-sensitive positions not requiring a "Q" clearance.
- n. Accept properly executed requests for Interim Access Authorizations; conduct appropriate indices checks and forward such requests to the Assistant Secretary for Defense Programs with appropriate recommendations.

- o. For DOE Headquarters (including Grand Junction Office, DOE regional offices, energy technology centers, power marketing agencies, (except the Bonneville Power Administration), Federal Energy Regulatory Commission, Strategic Petroleum Reserves Office, and the Environmental Measurements Laboratory):
  - (1) Implement the Personnel Security Program consistent with the objectives, standards, guides, and procedures stated in this Order and in 10 CFR part 710.
  - (2) Perform functions listed on pages II-5 through II-7, subparagraphs 8b, d, e, f, g, and k.
  - (3) Perform functions listed on pages II-7 and II-8, subparagraph 8m(1) through (5), (8), (9), and (10).
  - (4) Make an annual compilation of "Positions of a High Degree of Importance or Sensitivity" for certification.
  - (5) Process Data Reports on Spouse (DOE Form DP-354).
  - (6) Process cases of DOE or DOE contractor personnel who are hospitalized or otherwise treated for a mental illness which may cause a defect in judgment or reliability.
  - (7) Evaluate all reports of investigation conducted on DOE employees and applicants for employment for suitability in sensitive positions, and notify the Director of Personnel, Headquarters, of the results of each investigation for appropriate action.
8. HEADS OF FIELD ORGANIZATIONS, INCLUDING PITTSBURGH NAVAL REACTORS, SCHENECTADY NAVAL REACTORS AND THE ASSISTANT ADMINISTRATOR FOR MANAGEMENT SERVICES, BONNEVILLE POWER ADMINISTRATION (EXCLUDING THOSE ORGANIZATIONS MENTIONED ON PAGE II-5, SUBPARAGRAPH 7o), ALBUQUERQUE, CHICAGO, IDAHO, NEVADA, OAK RIDGE, RICHLAND, SAN FRANCISCO, SAVANNAH RIVER shall:
  - a. Implement the Personnel Security Program consistent with the policy, objectives, standards, guides, and procedures stated in this Order and in 10 CFR part 710.
  - b. Initiate requests for investigation directly to the Federal Bureau of Investigation or Office of Personnel Management.
  - c. Determine the position sensitivity and access requirements prior to requesting investigations for DOE employees or applicants for employment, consultants, and assignees.

- d. Determine the access requirements prior to requesting investigations for DOE contractor or subcontractor employees, consultants, or access permittees.
- e. Implement procedures which require DOE supervisors and DOE contractor organizations to report information received that an individual under their jurisdiction, possessing an active access authorization, is hospitalized or otherwise treated for a mental illness which may cause a defect in judgment or reliability, and to notify the Director of Safeguards and Security, Headquarters, of this fact and when such employee is found to be free of such defect.
- f. Arrange for the service of a psychiatrist to examine an individual when such an examination is determined appropriate in resolving a question of eligibility for access authorization, or continuing access authorization.
- g. Implement procedures under a supervisory security program to assure that DOE supervisors and DOE contractor organizations are aware that:
  - (1) Information concerning an individual possessing an active DOE access authorization (or in process for same) that is a matter of personnel security interest should be reported to a DOE security official.
  - (2) Established reporting channels should be used in communicating a matter of personnel security concern to the appropriate DOE security official.
- h. Request approval of the Director of Safeguards and Security, Headquarters, to initiate security investigations relative to foreign nationals.
- i. Refer to the Director of Safeguards and Security, Headquarters, requests for access authorization for employees of other Federal departments and agencies.
- j. Furnish the Director of Safeguards and Security, Headquarters, with:
  - (1) Written notifications of withdrawals of requests for access authorizations.
  - (2) An annual compilation of "Positions of a High Degree of Importance or Sensitivity" for certification.
  - (3) Data Reports on Spouse (DOE Form DP-354) for personnel under their jurisdiction who marry subsequent to the processing for an access authorization.

- k. Accept for access to "Confidential" or "Secret" National Security Information (Non-Restricted Data) or Formerly Restricted Data involved in DOE contracts and subcontractors, written assurances that personnel of the facility engaged in DOE work possess final DOD or NASA clearances for access to national security information and the type of investigation on which such clearances were granted. Clearances granted by DOD contractors and interim "Confidential" or "Secret" clearances are not acceptable. Appropriate records of accepted clearances shall be maintained by the field organization.
- l. Generate requests to the Secretary or the Assistant Secretary for Defense Programs, through the Director of Safeguards and Security, Headquarters, for Interim Access Authorizations.
- m. In addition to the above, Heads of Field Organizations and the Assistant Administrator for Management Services, Bonneville Power Administration:
  - (1) Grant access authorization in all cases except those requiring processing for a Personnel Security Board hearing.
  - (2) Cause individuals to be interviewed when the reported information falls within the criteria of 10 CFR part 710 or Executive Order 10450.
  - (3) In connection with cases processed in accordance with 10 CFR part 710.20 et seq, perform those functions assigned to the Heads of Field Organizations.
  - (4) Extend, accept for transfer, reinstate, and terminate access authorizations as appropriate.
  - (5) Authorize transfer of contractor personnel, whose access authorizations are based upon investigations by the Office of Personnel Management or other Government agencies, to positions of a "High Degree of Importance or Sensitivity" prior to receipt of Federal Bureau of Investigation reports.
  - (6) Furnish the Director of Safeguards and Security, Headquarters, with appropriate notifications of all access authorization actions.
  - (7) Approve and maintain records of review of personnel security files by properly identified employees of investigative agencies of the Federal Government and other routine users under Privacy Act regulations.

- (8) Accept investigations and reports on the character, associations, and loyalty of individuals made by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individuals by another Government agency based on such investigations and reports.
- (9) Maintain personnel security files, as appropriate, containing copies of reports of investigation and other pertinent data on individuals granted a DOE security clearance by that office, or where an investigation was requested by that office and reports of investigation forwarded by virtue of the fact that the individual occupied a critical-sensitive position.
- (10) Assure that the information reflected on standard employment forms completed by DOE employees, applicants for employment, consultants and assignees is comparable with the information reflected on security forms prior to the security forms being forwarded to the appropriate investigative agency.
- (11) Evaluate all applicable reports of investigation conducted on DOE employees and applicants for employment under their jurisdiction for suitability in sensitive positions and notify the cognizant office of the results of each investigation for appropriate action.

CHAPTER III

POSITION SENSITIVITY DESIGNATIONS

1. GENERAL. The position sensitivity designation for each category of personnel for employment and access are contained in this chapter. Sensitive compartmented information and general guidelines on requests for clearances are in paragraphs 3 and 4.
2. CATEGORIES.
  - a. Department of Energy (DOE) Employees, Applicants for Employment, Consultants, and Assignees.
    - (1) It is DOE policy to afford employment, and access to Restricted Data, National Security Information and other sensitive data not subject to National Security Regulations, and Category I or Category II quantities of special nuclear material to individuals concerning whom the DOE has made a determination that such employment and access will not endanger the common defense and security and is clearly consistent with the national interest. Except as authorized by the Secretary (or designee) that such action is clearly consistent with the national interest, this determination shall be based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individuals by another Government agency based on such an investigation and report.
    - (2) To assure that investigative coverage is appropriate for the individual's level of responsibility and access, a determination shall be made as to the sensitivity of each Departmental position and certified in writing to the Director at Headquarters, or to the appropriate DOE official at a DOE field office. This certification of Position Sensitivity Designation shall indicate whether the position is critical-sensitive, noncritical-sensitive, or nonsensitive; and if critical-sensitive or noncritical-sensitive, shall indicate which of the criteria in (a) or (b) below was used as a basis for that determination, and the degree of access (if any) which is involved. The following criteria shall be used in the determination of the Position Sensitivity Designation.
      - (a) Critical-Sensitive Position. A sensitive position, requiring a pre-appointment Office of Personnel Management full field investigation, the duties of which include any of the following:

- 1 Access to Top Secret National Security Information.
- 2 Access to Secret Restricted Data.
- 3 Access to Special Nuclear Material in Categories I or II.
- 4 Access to, and development or approval of war plans or particulars of future or major or special operations of war, or critical or extremely important items of war.
- 5 Access to, and development or approval of plans, policies, or programs which affect the overall operations of the DOE.
- 6 Fiduciary, public contact, or other responsibilities demanding the highest degree of public trust.
- 7 Responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or the capability to access a computer system during its operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realization of significant personal gain (ADP-1).
- 8 Access to "CRYPTO" (classified cryptographic information) or other classified communications security (COMSEC).

(b) In addition to the above criteria for determining critical-sensitive position designations, the following additional responsibilities or considerations shall be used to establish whether a critical-sensitive position is a "Position of a High Degree of Importance or Sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, requiring a pre-appointment FBI full field investigation.

- 1 Regular access to Top Secret Restricted Data.
- 2 Regular access to Restricted Data involving broad policy or program direction in any of the following:
  - a Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.
  - b Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.

c Research, development, or production in the laser fusion or laser isotope programs.

d Naval nuclear propulsion program.

3 Any other position so designated by the Secretary.

(c) Noncritical-Sensitive Position. A sensitive position, not within the categories described above, requiring a preappointment National Agency Check and Inquiry (NACI), the duties of which include any of the following:

1 Access to Confidential Restricted Data.

2 Access to Secret or Confidential National Security Information.

3 Responsibility for the direction, planning, design, operation, and maintenance of a computer system, and whose work is technically reviewed by a higher authority in a critical-sensitive position to assure the integrity of the system (ADP-II).

(d) Nonsensitive Position. A position requiring a NACI but not requiring a clearance connected with, or relative to the national security or welfare, and which does not fall into any of the categories described above. This also includes all other positions involved in computer activities not specified on page III-2, paragraph 2a(2)(a)7 and page III-3, paragraph 2a(2)(c)3.

b. DOE Contractor and Subcontractor Employees and Consultants, and Access Permittees.

(1) It is DOE policy to withhold the access to Restricted Data, other classified information, and quantities of special nuclear material of DOE contractor and subcontractor employees and consultants and access permittees until the DOE has made a determination that such access will not endanger the common defense and security. Except as authorized by the Secretary or his designee that such action is clearly consistent with the national security, this determination shall be made based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations, provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individual by another Government agency based on such an investigation and report.

- (2) To assure that investigative coverage is appropriate, the individual's type of access (Restricted Data, National Security Information, or unclassified Special Nuclear Material in Category I or II Quantities) and level of access (Top Secret, Secret, or Confidential) shall be determined before a request for investigation is made by the appropriate DOE official. Additionally, a DOE contractor or subcontractor employee or consultant position shall be designated as a "Position of a High Degree of Importance or Sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position include any of the following:
- (a) Regular access to Top Secret Restricted Data.
  - (b) Regular access to Restricted Data involving broad policy or program direction in any of the following:
    - 1 Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.
    - 2 Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.
    - 3 Research, development, or production in the laser fusion or laser isotope programs.
    - 4 Naval nuclear propulsion program.
- (3) It is DOE policy not to establish a separate clearance program for DOE contractor and subcontractor employees and consultants and access permittees for positions associated with unclassified Federal Computer Systems. Rather, the contractor, subcontractor, consultants, or access permittee is responsible for maintaining satisfactory standards of employees qualifications, performance, conduct, and business ethics under its own personnel policies (U.S. Department of Energy Procurement Regulation, Subpart 9-50.12, Labor Relations, 9-50.1201-2(a)).

c. Other Federal Department or Agency Employees.

- (1) It is DOE policy to withhold the access to Restricted Data, other classified information under DOE responsibility, and quantities of special nuclear material of other Federal employees until the DOE has made a determination that such access will not endanger the common defense and security. Except as authorized by the Secretary or his designee that such action is clearly consistent with the

national security, this determination shall be based upon an investigation and report by the Office of Personnel Management, Federal Bureau of Investigation, or another Government agency which conducts personnel security investigations provided (in those instances involving access to Restricted Data) that a security clearance has been granted to such individual based on such investigation and report.

- (2) Additionally, positions within other Federal departments (exclusive of personnel of the Department of Defense and the National Aeronautics and Space Administration, who do not require DOE security clearance by virtue of section 143 of the Atomic Energy Act of 1954, as amended, or section 304(b) of the National Aeronautics and Space Act of 1958) and agencies shall be designated as a "Position of a High Degree of Importance or Sensitivity" within the meaning of section 145f of the Atomic Energy Act of 1954, as amended, when the duties of that position include any of the following:
  - (a) Regular access to Top Secret Restricted Data.
  - (b) Regular access to Restricted Data involving broad policy or program direction in any of the following:
    - 1 Research and development programs pertaining to nuclear or thermonuclear weapons or special nuclear material production.
    - 2 Production or stockpile of nuclear or thermonuclear weapons or special nuclear material.
    - 3 Research, development, or production in the laser fusion or laser isotope separation programs.
    - 4 Naval nuclear propulsion program.
3. SENSITIVE COMPARTMENTED INFORMATION (SCI). Within the DOE, determinations concerning an individual's eligibility for access to SCI are the responsibility of the Senior Intelligence Officer and his or her designated representative(s). The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in Director of Central Intelligence Directive (DCID), No. 1/14.
4. GENERAL GUIDELINES. Requests for clearances shall be submitted only after a determination has been made that the duties of a position require access to classified information, or special nuclear material in Category I or II quantities, or regular access to a security area. Clearances are not to be requested as a means for alleviating individual or management responsibility to safeguard classified information properly or control dissemination of

such classified information on a "need-to-know" basis. It is the intent of this policy to assure that clearances are requested only when absolutely required to avoid the unnecessary expenditure of agency funds and resources or the unwarranted invasion of an individual's right to privacy.

- (1) The DOE will take all reasonable measures to obtain existing reports of investigation which may fulfill the agency standards and specifications as to the scope and extent of investigations established by the Secretary.
- (2) Requests for clearances will not be processed: (a) unless all required security forms are completed and signed (when appropriate) by the applicant; (b) if the printed content of the security forms has been altered; (c) if insufficient information is provided or the forms are illegible.
- (3) The possession of a DOE clearance permits an individual access to the levels of classified information (on a "need-to-know" basis) as shown below:

<u>Type Clearance</u>	<u>Access Permitted*</u>
DOE Employees, Applicants for employment, Consultants, and Assignees; and DOE Contractor and Subcontractor Employees and Consultants:	
"Q - Sensitive"	Top Secret RD, FRD, & NSI Secret RD, FRD, & NSI Confidential RD, FRD & NSI
"Q - Nonsensitive"	Top Secret NSI, & FRD Secret RD, FRD & NSI Confidential RD, FRD, & NSI
Top Secret	Top Secret NSI, & FRD Secret NSI, & FRD Confidential NSI & FRD
"L"	Secret NSI, & FRD Confidential RD, FRD, & NSI
Secret	Secret NSI, & FRD Confidential NSI, & FRD

Employees of DOE Access Permit Holders:

"Q(X)"

Secret RD  
Confidential RD  
(as specified in the  
access permit)

"L(X)"

Confidential RD  
(as specified in the  
access permit)

---

Other Federal Department/Agency Employees:

"Q - Sensitive"

Top Secret RD  
Secret RD  
Confidential RD

"Q - Nonsensitive"

Secret RD  
Confidential RD

"L"

Confidential RD

\*(RD - Restricted Data; FRD - Formerly Restricted Data; NSI - National Security Information)