

REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR: 8107060250. DOC. DATE: 81/06/29 NOTARIZED: YES DOCKET #  
 FACIL: 50-387 Susquehanna Steam Electric Station, Unit 1, Pennsylvania 05000387  
 50-388 Susquehanna Steam Electric Station, Unit 2, Pennsylvania 05000388  
 AUTH. NAME: CURTIS, N.W. AUTHOR AFFILIATION: Pennsylvania Power & Light Co.  
 RECIPIENT NAME: YOUNGBLOOD, B.J. RECIPIENT AFFILIATION: Licensing Branch 1

SUBJECT: Forwards Amend 36 to OL application. Amend contains Revision H to facility security plan. Amend withheld (ref 10CFR2.790).

DISTRIBUTION CODE: S001S COPIES RECEIVED: LTR 3 ENCL 5 SIZE: 2  
 TITLE: Security Plans

NOTES: Send I&E 3 copies FSAR & all amends. 1 cy: BWR-LRG PM(L, RIB) 05000387  
 Send I&E 3 copies FSAR & all amends. 1 cy: BWR-LRG PM(L, RIB) 05000388

	RECIPIENT ID CODE/NAME	COPIES LTR ENCL	RECIPIENT ID CODE/NAME	COPIES LTR ENCL
ACTION:	LIC BR #2 BC STARK, R.	1 0 1 0	LIC BR #2 LA	1 0
INTERNAL:	IE/REGION #4 NMSS/SGPL #2 REG. FILE #1	1 1 1 1 1 1	IE/SB #2 #3 NRC PDR SSPB #6	1 1 1 0 1 1
EXTERNAL:	ACRS #5 NTIS	1 1 1 0	LPDR	1 0

Copy Reproduced  
 For Gaskin, 274010  
 7/16/81 LL

App 4

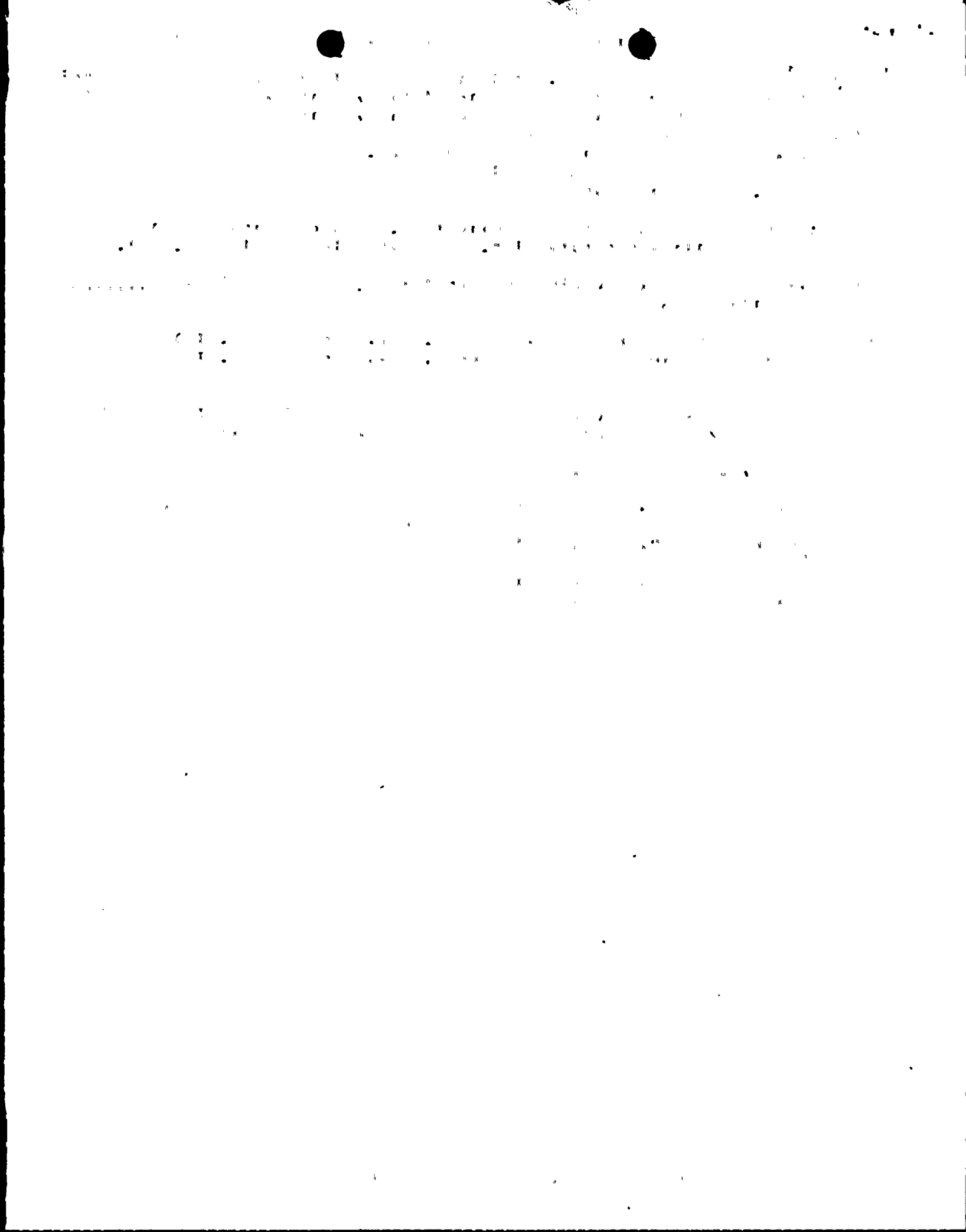
JUL 07 1981

TOTAL NUMBER OF COPIES REQUIRED: LTR

13

ENCL

7



TWO NORTH NINTH STREET, ALLENTOWN, PA. 18101 PHONE: (215) 770-5151

NORMAN W. CURTIS  
Vice President-Engineering & Construction-Nuclear  
770-5381

June 29, 1981

Mr. B. J. Youngblood, Chief  
Licensing Branch No. 1  
Division of Licensing  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

SUSQUEHANNA STEAM ELECTRIC STATION  
AMENDMENT 36 TO OPERATING LICENSE APPLICATION  
ER 100450 FILE 841-1  
PLA - 863

Dear Mr. Youngblood:

Attached are five (5) copies of Amendment No. 36 to the operating license application. This amendment contains Revision H to the Susquehanna SES Security Plan. Pursuant to Section 2.790(d) of 10 CFR Part 2, this document should be withheld from public inspection.

Very truly yours,

*N. W. Curtis*

N. W. Curtis  
Vice President, Engineering and Construction - Nuclear

NRC TRANS P:1

Mr. Thomas M. Gerusky  
Director, Bureau of Radiation  
Protection  
Fulton Building  
P. O. Box 2063  
Harrisburg, PA 17120

Attorney General  
Department of Justice  
Capitol Annex  
Harrisburg, PA 17120

Governor's Office of State  
Planning & Development  
Attn: Coordinator,  
State Clearinghouse  
P. O. Box 1323  
Harrisburg, PA 17120

Mr. Bruce Thomas  
President, Board of Supervisors  
R. D. #1  
Berwick, PA

Mr. George Pence  
U. S. Environmental Protection Agency  
Region III Office  
Curtis Building (Sixth Floor)  
6th & Walnut Streets  
Philadelphia, PA 19106

Mr. J. E. Carson  
Argonne National Laboratory  
Pennsylvania 9700 South Cass Avenue  
Argonne, IL 60439

5001  
3/5

8107060250 810629  
PDR ADDCK 05000387  
F PDR

PENNSYLVANIA POWER & LIGHT COMPANY



BEFORE THE  
UNITED STATES NUCLEAR REGULATORY COMMISSION

---

In the Matter of

:

PENNSYLVANIA POWER &  
LIGHT COMPANY

:

Docket Nos. 50-387 and 50-388

---

AMMENDMENT NO. 36

APPLICATION FOR CLASS 103

OPERATING LICENSES FOR THE SUSQUEHANNA  
STEAM ELECTRIC STATION

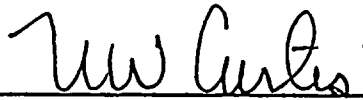
UNITS NO. 1 AND NO. 2

---

Applicant, Pennsylvania Power & Light Company, hereby files Amendment No. 36 to its Operating License Application dated July 31, 1978.

This ammendment contains Revision H to the Susquehanna SES Security Plan. Pursuant to Section 2.790(d) of 10 CFR Part 2, this document should be withheld from public inspection.

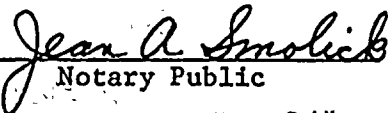
PENNSYLVANIA POWER & LIGHT COMPANY  
BY:



N. W. Curtis

V. P., Engineering and Construction-Nuclear

Sworn to and subscribed before me  
this 29<sup>th</sup> of June, 1981.

  
Notary Public

JEAN A. SMOLICK, Notary Public  
Allentown, Lehigh County, Pa.  
My Commisssion Expires May 14, 1984



PENNSYLVANIA POWER & LIGHT COMPANY

PHYSICAL SECURITY PLAN

SUSQUEHANNA STEAM ELECTRIC STATION

CHANGE H  
JUNE 26, 1981

This Change to the Susquehanna SES Physical Security Plan is issued to all copyholders for posting effective June 26, 1981.


When posting has been completed, this authorization page and the posting instructions should be entered into the Plan immediately following the Table of Contents.

Copyholders are instructed to destroy by burning or shredding all pages which are removed from the Plan during the posting process.


Prepared By:

Reviewed By:

  
Director-Corporate Security

  
Vice President-Nuclear Operations

Approved By:

  
Senior Vice President-Nuclear

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

Copy 4 of 20 copies

## SSES PHYSICAL SECURITY PLAN - CHANGE H

Specific changes which warrant explanation are as follows:

1. Paragraphs 11.2.3.4.3, 11.2.3.4.4, 11.2.3.5.3, 11.2.3.6.1, 11.2.3.6.3, 11.2.3.6.6, 11.2.3.7, 11.2.3.9, 11.2.3.10, 11.2.3.11, 11.2.3.13 and 11.2.3.14 have been amended to reflect NRC notification.
2. Responsibility Matrix 11.2.3.6.1 has been amended to reflect NRC notification.
3. Responsibility Matrix 11.2.3.13 has been amended to include a statement to the effect that during hostage/extortion negotiations, a knowledgeable Company employee will be consulted on matters affecting public health and safety.

A black line in the left margin indicates a significant change in text.

### P O S T I N G   I N S T R U C T I O N S

#### REMOVE

Document Protection  
Table of Contents  
Pages 11-33(G) - 11-34(G)  
Pages 11-35(G) - 11-36(G)  
Pages 11-39(G) - 11-40(G)  
Pages 11-43(G) - 11-44(G)  
Pages 11-47(G) - 11-48(G)  
Pages 11-49(G) - 11-50(G)  
Pages 11-51(G) - 11-52(G)  
Pages 11-53(G) - 11-54(G)  
Pages 11-55(G) - 11-56(G)  
Page 11-75(G) - 11-76(G)  
Page 11-87(G) - 11-88(G)  
Page F-1(G) - F-2(F)

#### INSERT

Document Protection  
Table of Contents  
Pages 11-33(G) - 11-34(H)  
Pages 11-35(H) - 11-36(G)  
Pages 11-39(H) - 11-40(H)  
Pages 11-43(H) - 11-44(G)  
Pages 11-47(H) - 11-48(H)  
Pages 11-49(G) - 11-50(H)  
Pages 11-51(G) - 11-52(H)  
Pages 11-53(H) - 11-54(G)  
Pages 11-55(H) - 11-56(H)  
Page 11-75(G) - 11-76(H)  
Page 11-87(G) - 11-88(H)  
Page F-1(H) - F-2(F)



### Document Protection

This Physical Security Plan identifies detailed security measures for the physical protection of an NRC licensed plant in which NRC licensed special nuclear material will be processed and used. As such, the Plan is exempt from public disclosure in accordance with 10 CFR 2.790 (d) (1) and 9.5 (a) (4) (i).

Within the Pennsylvania Power and Light Company, authorized holders of this Plan will store it in an approved security container, and will restrict dissemination of information contained in the Plan to other Pennsylvania Power & Light Company employees who have demonstrated a right and need-to-know.

Neither this Plan nor any portion of the Plan may be copied without prior written permission of the Pennsylvania Power & Light Company. Requests for permission to prepare a copy of this Plan, or any portion of it, should be addressed to the Director - Corporate Security, Pennsylvania Power & Light Company, Two North Ninth Street, Allentown, Pennsylvania 18101.

All incidents or suspected incidents of unauthorized disclosure of the Plan's contents, whether orally or in writing, should be reported to the Director - Corporate Security, Pennsylvania Power & Light Company, at the earliest practical moment.

2.790 MATERIAL  
EXCLUDED FROM PUBLIC DISCLOSURE



## TABLE OF CONTENTS

	<u>PAGE</u>
INTRODUCTION . . . . .	i(F)
1. Identification of Licensee Applicant . . . . .	i(F)
2. Description of Nuclear Plant . . . . .	i(F)
3. Purpose of Plan . . . . .	ii(F)
4. Summary of Plan . . . . .	iv(F)
5. Terms . . . . .	v(F)
A. Definitions . . . . .	v(F)
B. Abbreviations . . . . .	xi(F)
PART I	
1.0 AUTHORITY OF SECURITY OFFICERS . . . . .	1-1(F)
1.1 Authority to Bear Arms . . . . .	1-1(F)
1.2 Authority to Use Force to Protect Persons and Property . . . . .	1-1(F)
1.3 Authority to Control Property . . . . .	1-3(F)
1.4 Authority to Arrest and Confine . . . . .	1-4(F)
1.5 Authority to Prevent or Delay Radiological Sabotage . . . . .	1-5(F)
2.0 SECURITY MANAGEMENT AND ORGANIZATION . . . . .	2-1(F)
2.1 Security Management . . . . .	2-1(F)
2.1.1 Corporate Management . . . . .	2-1(F)
2.1.2 Plant Management . . . . .	2-5(F)
2.2 Security Organization . . . . .	2-8(F)
2.2.1 Security Section Composition . . . . .	2-8(F)
2.2.1.1 Security Officer Equipment . . . . .	2-9(F)
2.2.2 Reserve Security Force . . . . .	2-11(F)
2.2.3 Law Enforcement Agencies . . . . .	2-11(F)
2.3 Security Data and Management System . . . . .	2-13(F)
2.3.1 Perimeter Intrusion Detection . . . . .	2-14(F)
2.3.2 Threat Assessment (CCTV) . . . . .	2-15(F)
2.3.3 Access Control . . . . .	2-16(F)
2.3.4 Computer Based Security Management System (SMS) . . . . .	2-22(F)
2.3.5 Operator Consoles . . . . .	2-22(F)
2.3.6 Line Supervision . . . . .	2-22(F)
2.3.7 Alarms . . . . .	2-23(F)
2.4 SSES Security Procedures . . . . .	2-24(F)
3.0 PERSONNEL SELECTION, CLEARANCE AND TRAINING PROGRAMS . . . . .	3-1(F)
3.1 Selection . . . . .	3-1(F)
3.1.1 Non-security Personnel . . . . .	3-2(F)
3.1.2 Security Personnel . . . . .	3-2(F)

	<u>Page</u>
3.2 Personnel Security Clearances . . . . .	3-3(F)
3.2.1 Types of Clearances . . . . .	3-3(F)
3.2.2 Requesting Clearances . . . . .	3-5(F)
3.2.3 Granting Clearances . . . . .	3-6(F)
3.2.4 Interim Clearances . . . . .	3-8(G)
3.3 Training . . . . .	3-9(F)
3.3.1 Non-security Personnel . . . . .	3-9(F)
3.3.2 Security Personnel . . . . .	3-11(F)
4.0 ACCESS AUTHORIZATIONS . . . . .	4-1(F)
4.1 Personnel Access . . . . .	4-1(F)
4.1.1 Unescorted Access . . . . .	4-1(F)
4.1.2 Escorted Access . . . . .	4-3(F)
4.1.3 Escorts . . . . .	4-4(F)
4.2 Material Access . . . . .	4-6(F)
4.2.1 Prohibited Items List . . . . .	4-7(F)
4.2.2 Cargo, Vehicles and Trains . . . . .	4-7(F)
4.3 Emergency Response Vehicle Access . . . . .	4-8(F)
5.0 SITE AND ENVIRONS . . . . .	5-1(F)
5.1 General Site and Area Layout . . . . .	5-1(F)
5.1.1 Location . . . . .	5-1(F)
5.1.2 Topography . . . . .	5-2(F)
5.1.3 Site Structures Outside the Protected Area . . . . .	5-3(F)
5.1.4 Buffer Zone . . . . .	5-5(F)
5.2 Mobile Patrol Outside the Protected Area . . . . .	5-5(F)
5.3 Meteorology . . . . .	5-6(F)
6.0 SECURITY OF THE PROTECTED AREA . . . . .	6-1(F)
6.1 Protected Area Perimeter . . . . .	6-1(F)
6.1.1 Isolation Zones . . . . .	6-1(F)
6.1.2 Physical Barriers . . . . .	6-3(F)
6.1.3 Illumination . . . . .	6-5(F)
6.1.4 Surveillance/Intrusion Detection . . . . .	6-5(F)
6.1.5 Intrusion Detection Equipment . . . . .	6-6(F)
6.1.6 Patrols . . . . .	6-7(F)
6.2 Protected Area Perimeter Portals . . . . .	6-9(F)
6.2.1 Personnel Portals and Posts . . . . .	6-9(F)
6.2.1.1 Layout . . . . .	6-10(F)
6.2.1.2 Construction . . . . .	6-12(F)
6.2.1.3 Manning . . . . .	6-12(F)
6.2.1.4 Search and Admittance Control Equipment . . . . .	6-13(F)
6.2.1.5 Access and Egress Control Processing . . . . .	6-14(F)
6.2.1.6 Keycard Badges . . . . .	6-17(F)

	<u>Page</u>
6.2.2 Small Package Access Processing . . . . .	6-17(F)
6.2.3 Vehicle Portals . . . . .	6-18(F)
6.2.4 Train Portals . . . . .	6-20(F)
6.3 Interior of Protected Area . . . . .	6-22(F)
6.3.1 Layout . . . . .	6-22(F)
6.3.2 Physical Structures . . . . .	6-23(F)
6.3.3 Patrols . . . . .	6-25(F)
6.3.4 Licensee Designated Vehicles . . . . .	6-26(F)
7.0 SECURITY OF THE VITAL AREAS . . . . .	7-1(F)
7.1 Vital Area Structures . . . . .	7-1(F)
7.2 Vital Area Portals . . . . .	7-5(F)
7.2.1 Personnel Portals . . . . .	7-5(F)
7.2.2 Personnel Access Processing . . . . .	7-5(F)
7.2.3 Elevator Access . . . . .	7-8(F)
7.3 Patrols and Inspections . . . . .	7-8(F)
8.0 SPECIAL SECURITY MEASURES . . . . .	8-1(F)
8.1 Refueling/Major Maintenance Outages . . . . .	8-1(F)
8.2 Major Construction Periods . . . . .	8-4(F)
8.2.1 Security of the SSES Unit 2 Construction Site . . . . .	8-4(F)
8.2.2 Security of SSES Unit 1 . . . . .	8-5(F)
8.2.2.1 Protected Area . . . . .	8-5(F)
8.2.2.2 Unit 1 - Unit 2 Separation . . . . .	8-6(F)
8.2.2.3 Perimeter Portals . . . . .	8-9(F)
8.2.2.4 Access Authorization . . . . .	8-10(F)
9.0 SECURITY CONTROL CENTERS . . . . .	9-1(F)
9.1 Security Control Center . . . . .	9-1(F)
9.1.1 Alarm and Surveillance Monitoring Equipment . . . . .	9-3(F)
9.1.2 Communications . . . . .	9-3(F)
9.1.3 Manning . . . . .	9-4(F)
9.2 Alternate Security Control Center . . . . .	9-4(F)
9.3 Monitoring Security Posture of SCC and ASCC . . . . .	9-5(F)
9.4 Emergency Access to the SCC and ASCC . . . . .	9-6(F)
10.0 CENTRAL COMMUNICATIONS SYSTEMS . . . . .	10-1(F)
10.1 Telephone System . . . . .	10-1(F)
10.2 Security Section Radio System . . . . .	10-2(F)
11.0 RESPONSE TO SECURITY CONTINGENCIES . . . . .	11-1(F)
11.1 Background . . . . .	11-2(F)
11.1.1 Perceived Danger . . . . .	11-2(F)
11.1.2 Purpose of Contingency Planning . . . . .	11-3(F)

11.1.3	Scope of Contingency Plan . . . . .	11-4(F)
11.1.3.1	Situations Covered . . . . .	11-4(F)
11.1.3.2	Situations Not Covered . . . . .	11-5(F)
11.1.4	Definitions . . . . .	11-5(F)
11.2	Generic Planning Base . . . . .	11-6(F)
11.2.1	General . . . . .	11-6(F)
11.2.2	SSES Security Conditions . . . . .	11-7(G)
11.2.2.1	Normal/Condition 1 . . . . .	11-9(G)
11.2.2.2	Suspicious Events/Condition 2 . . . . .	11-11(G)
11.2.2.3	Degradations/Condition 3 . . . . .	11-15(G)
11.2.2.4	Threats/Condition 4 . . . . .	11-17(G)
11.2.2.5	Adversary Action/Condition 5 . . . . .	11-20(G)
11.2.3	Events, Objectives, Decisions/Actions, Data Required . . . . .	11-24(G)
11.2.3.1	Bomb Threat . . . . .	11-25(G)
11.2.3.2	Adversary Threat Action . . . . .	11-28(G)
11.2.3.3	Civil Disturbance . . . . .	11-30(G)
11.2.3.4	Perimeter and Protected Area Intrusion . . . . .	11-31(G)
11.2.3.4.1	Perimeter Intrusion Alarm Annunciates at the SCC and ASCC . . . . .	11-31(G)
11.2.3.4.2	Visual Observation of Unidentified Person(s) at or within the Protected Area Perimeter . . . . .	11-32(G)
11.2.3.4.3	Discovery of Breach of Perimeter Barrier . . . . .	11-33(G)
11.2.3.4.4	Confirmed Protected Area Intrusion . . . . .	11-34(H)
11.2.3.5	Vital Area Intrusion . . . . .	11-36(G)
11.2.3.5.1	Vital Area Intrusion Alarm Annunciates in the SCC and ASCC . . . . .	11-36(G)
11.2.3.5.2	Visual Observation of Unidentified or Unauthorized Person Entering or Within a Vital Area . . . . .	11-37(G)
11.2.3.5.3	Vital Area Found Unlocked and Unattended or Vital Area Barrier Found Breached . . . . .	11-38(G)
11.2.3.6	Miscellaneous Events . . . . .	11-39(H)
11.2.3.6.1	Member of Security Force Fails to Perform Duty . . . . .	11-39(H)
11.2.3.6.2	Suspected Bomb or Sabotage Device Discovered . . . . .	11-40(H)
11.2.3.6.3	Fire, Explosion or Other Catastrophe . . . . .	11-42(G)
11.2.3.6.4	Internal Disturbance . . . . .	11-44(G)
11.2.3.6.5	Multiple Loss of On-Site Security Communications Systems . . . . .	11-45(G)
11.2.3.6.6	Multiple Loss of Off-Site Security Communications Systems . . . . .	11-46(G)
11.2.3.7	Obvious Attempt to Sabotage or Confirmed Intrusion into Vital Area(s) in Progress . . . . .	11-47(H)

11.2.3.8	Sabotage Device Rendered Inoperable, Tampered/ Deranged Equipment Restored, Intruder/Saboteur Captured or Escaped . . . . .	11-49(G)
11.2.3.9	Loss or Degradation of Security System (Alarm Annunciation, Access Control, Tamper Alarm, Intrusion Detection. . . . .	11-50(H)
11.2.3.10	Loss of Protected Area Lighting . . . . .	11-51(G)
11.2.3.11	Loss of Security System Power . . . . .	11-52(H)
11.2.3.12	Aberrant Behavior (When Observed by Member of Security Section) . . . . .	11-53(H)
11.2.3.13	Hostage/Extortion Situations . . . . .	11-54(G)
11.2.3.14	Security Officer Strike . . . . .	11-56(H)
11.3	Licensee Planning Base . . . . .	11-57(G)
11.3.1	Licensee's Organizational Structure . . . . .	11-57(G)
11.3.2	Physical Layout . . . . .	11-57(G)
11.3.3	Safeguards Systems Hardware . . . . .	11-59(G)
11.3.3.1	Communications . . . . .	11-59(G)
11.3.3.2	Intrusion Detection . . . . .	11-59(G)
11.3.3.3	Surveillance . . . . .	11-59(G)
11.3.3.4	Locks, Keys, Combinations & Related Equipment . . . . .	11-59(G)
11.3.3.5	Security Personnel Equipment . . . . .	11-59(G)
11.3.3.6	Security Vehicles . . . . .	11-60(G)
11.3.4	Law Enforcement and Interface and Assistance . . . . .	11-60(G)
11.3.5	Policy Constraints and Assumptions . . . . .	11-60(G)
11.3.6	Administrative and Logistical Considerations . . . . .	11-61(G)
11.3.7	Responsibility Matrix . . . . .	11-61(G)
12.0	OVERALL SECURITY PROGRAM PERFORMANCE . . . . .	12-1(F)
12.1	Evaluating the Components of the Security Program . . . . .	12-3(F)
12.2	Evaluation of the Planned Security Program . . . . .	12-5(F)
12.2.1	Protected Area . . . . .	12-8(F)
12.2.2	Vital Areas . . . . .	12-9(F)
12.2.3	Protection Against Insiders . . . . .	12-9(F)
12.2.4	Coordination and Assessment . . . . .	12-10(F)
12.2.5	LLEA Support . . . . .	12-11(F)

## PART II

13.0	TESTS AND INSPECTIONS . . . . .	13-1(F)
13.1	Physical Barriers and Access Portals . . . . .	13-1(F)
13.2	Alarms and Annunciators . . . . .	13-2(F)
13.3	Special Purpose Detectors . . . . .	13-2(F)
13.4	Communications Equipment . . . . .	13-2(F)
13.5	Security Officer Equipment . . . . .	13-3(F)
13.6	CCTV Equipment . . . . .	13-3(F)
13.7	Exterior Lighting Systems . . . . .	13-4(F)
13.8	Standby Generator . . . . .	13-4(F)

	<u>Page</u>
14.0 SECURITY RECORDS . . . . .	14-1(F)
14.1 Physical Security Plan . . . . .	14-1(F)
14.2 Security Procedures . . . . .	14-2(F)
14.3 Security Training and Requalification . . . . .	14-3(F)
14.3.1 Personnel Authorized Unescorted Access & Designated Escorts . . . . .	14-3(F)
14.3.2 Security Section Personnel . . . . .	14-4(F)
14.4 Personnel Selection . . . . .	14-4(F)
14.5 Security Logs . . . . .	14-5(F)
14.5.1 Access and Egress Logs . . . . .	14-5(F)
14.5.2 Registration for Escorted Access . . . . .	14-6(F)
14.5.3 Alarms . . . . .	14-6(F)
14.5.4 Responses . . . . .	14-7(F)
14.5.5 Lock and Key Issue . . . . .	14-7(F)
14.6 Inspections, Tests and Maintenance . . . . .	14-7(F)
14.7 Liaison and Agreements with Law Enforcement Agencies . . . . .	14-8(F)
14.8 General Investigative Files . . . . .	14-8(F)
14.9 Personnel Security Investigative Files . . . . .	14-8(F)
14.10 Access Authorization Lists . . . . .	14-9(F)
14.11 Audits . . . . .	14-9(F)
14.12 NRC Inspections . . . . .	14-9(F)
14.13 Selection and Qualification Records . . . . .	14-9(F)
15.0 SECURITY AUDITS . . . . .	15-1(F)
15.1 Susquehanna Review Committee . . . . .	15-1(F)
15.2 Director - Corporate Security . . . . .	15-1(F)
15.3 Plant Operations Review Committee . . . . .	15-2(F)
15.4 Supervisor of Security . . . . .	15-2(F)
15.5 Nuclear Regulatory Commission . . . . .	15-3(F)

#### APPENDICES

Appendix A Letter, Pennsylvania State Police Troop "P", Nov. 15, 1977 . . . . .	A-1
Appendix B Lethal Weapons Training Act . . . . .	B-1(F)
Appendix C Criteria for Denying Personnel Security Clearances . . . . .	C-1(F)
Appendix D Alarm Systems Test Schedule . . . . .	D-1(F)
Appendix E Vital Equipment List . . . . .	E-1(F)
Appendix F NRC Requests for Additional Information . . . . .	F-1(H)

#### FIGURES

2-1 Corporate Management for SSES Security . . . . .	2-3(F)
2-2 Plant Management for SSES Security . . . . .	2-4(F)
2-3 Locations of Pennsylvania State Police Troop "P" Stations . . . . .	2-26(F)
11-1 Security Section Shift Strength . . . . .	11-58(G)
11-2 Responsibility Matrix . . . . .	11-63(G)
12-1 Pitting Security Measures Against Security Threats . . . . .	12-2(F)



## DRAWINGS

(Located at End of Each Pertinent Chapter in the Permanent Plan.)

- 5-1(F) General Map Area
- 5-2(F) Site Map

- 6-1(F) Plan View Scale Drawing of the Protected Area
- 6-2(F) Site Illumination
- 6-3(F) CCTV Locations
- 6-4(F) Intrusion Detection Alarm System
- 6-5(F) North Gatehouse Ground Floor Plan
- 6-6(F) North Gatehouse Second Floor Plan
- 6-7(F) North Gatehouse Vehicle Portals
- 6-8(F) South Gatehouse Floor Plan
- 6-9(F) South Gatehouse Vehicle Portal

- 7-1(F) Plan View of Vital Areas

### Reactor and Diesel Generator Buildings and Control Structure

- 7-2(F) Elevations 645'0" + 656'0"
- 7-3(F) Elevations 670'0" + 676'0"
- 7-4(F) Elevations 683'0", 699'0", 714'0" + 716'3"
- 7-5(F) Elevations 719'1", 729'0" + 714'1"
- 7-6(F) Elevations 745'7", 749'1", 754'0" + 762'0"

### Reactor Buildings and Control Structure

- 7-7(F) Elevations 771'0", 783'0" + 799'1"
- 7-8(F) Elevations 779'1" + 806'0"
- 7-9(F) Elevation 818'1"
- 7-10(F) Reactor Buildings, Elevation 872'4½"
- 7-11(F) Engineered Safeguards Service Water Pumphouse, Elevation 685'6"

- 8-1(F) Plan View of Protected Area, Vital Areas & CCTV Locations  
Unit 1 Operating/Unit 2 Under Construction
- 8-2(F) Site Illumination & Intrusion Detection Alarm System  
Unit 1 Operating/Unit 2 Under Construction

### Reactor and Diesel Generator Buildings and Control Structure

- 8-3(F) Elevations 645'0" + 656'0"
- 8-4(F) Elevations 670'0" + 676'0"
- 8-5(F) Elevations 683'0", 699'0", 714'0" + 716'3"
- 8-6(F) Elevations 719'1", 729'0" + 741'1"
- 8-7(F) Elevations 745'7", 749'1", 754'0" + 762'0"

### Reactor Buildings and Control Structure

- 8-8(F) Elevations 771'0", 783'0", + 799'1"
- 8-9(F) Elevations 779'1" + 806'0"
- 8-10(F) Elevation 818'1"
- 8-11(F) Reactor Building, Elevation 872'4½"

### Turbine Building

- 8-12(F) Elevations 645'0", 656'0" + 666'0"
- 8-13(F) Elevations 670'0" + 676'0"
- 8-14(F) Elevations 683'0", 699'0", 714'0" + 716'3"
- 8-15(F) Elevations 719'1" + 729'0"
- 8-16(F) Elevations 749'1", 754'0" + 762'0"
- 8-17(F) Elevations 779'1" + 806'0"
- 8-18(F) Elevation 818'1"

- 9-1(F) Floor Plan, Security Control Center Building

Personnel authorized access to the SSES will be wearing or in possession of a security identification badge which will designate the area(s) for which access has been authorized and whether or not the individual requires an escort.

Objective:

Determine if the unidentified person(s) is authorized for access to the SSES.

Decisions/Actions:

- Security Officers on the scene shall report all information concerning the unauthorized person(s) to the Security Controller. The Security Controller may, depending upon the location, be able to observe the unidentified individual(s) through use of the CCTV system.
- The Security Controller will consult the SDMS to determine whether or not the person(s) is authorized access.

Next Step:

If an intrusion has occurred, implement Event 11.2.3.4.4.

Data Required:

1. Location of unidentified person(s).
2. Alarm response procedures for Security Officers.
3. Security Officers will attempt to identify the unidentified individual(s).
4. SDMS (list of authorized personnel).
5. SDMS (list of visitors and escorts).

11.2.3.4.3 Discovery of Breach of Perimeter Barrier

The perimeter barrier is observed to be cut open, knocked down or otherwise breached.

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

Objective:

To determine if an intrusion has occurred.

Decisions/Actions:

- The Security Controller will dispatch one or more Security Officers to the scene to investigate. The Security Controller will notify the Security Shift Supervisor and Operations Shift Supervisor.
- The Security Controller will direct the assessment of the alarm and implement the appropriate contingency procedures. If the CCTV capabilities are available in that area, the Controller will monitor the situation via remote cameras. In the event a door is involved, the Security Controller will retrieve from the SDMS names of persons having recently entered the area to assist in resolving the matter. If directed by the Security Shift Supervisor the Security Controller will direct Security Officers to conduct a search of the appropriate area.
- NRC notified, as appropriate.

Next Step:

If an intrusion has occurred, implement Event 11.2.3.4.4.

Data Required:

1. Discovery of unsecured or breached barrier procedure for Security Officers.
2. Location of breach.
3. Complete report of the Security Officer investigation.

11.2.3.4.4 Confirmed Protected Area Intrusion

Unauthorized person(s) in the protected area has resisted efforts by Security

Officers to interdict him, an unexplained breached barrier is assumed to reveal a recent intrusion or a perimeter alarm is found tampered with.

Objective:

- Prevent vital area access by an intruder.
- To restrain and detain the intruder.

Decisions/Actions:

- Normally the Security Controller will receive the alarm from security personnel or from the SDMS. The Security Controller will assess the threat posed by the intruder(s) by using information supplied by the SDMS and/or Security Officers who are at the scene. Upon assessment of the situation, the Security Controller will implement the appropriate contingency procedures. In addition, the Security Shift Supervisor and the Operations Shift Supervisor will be appraised of the situation. If necessary, additional Security Officers will be dispatched to assist the Officers already at the scene.
- When directed, the Security Controller will notify the PA State Police of the situation and, if necessary, request assistance.
- NRC notified, as appropriate.
- If the intruder(s) is discovered in the protected area or in a building not housing vital equipment, Security Officers on the scene will take the necessary actions to isolate if possible, the intruder(s) in one area of the protected area or one section of the building until the arrival of the PA State Police.
- Under the direction of the Security Shift Supervisor, Security Officers will take actions necessary to mitigate consequences of any anticipated sabotage.
- The Security Controller will fully advise the Operations Shift Supervisor of the situation who, in turn, will normally notify the Superintendent of Plant or

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

his designee. Appropriate coordinating efforts between the Operations Shift Supervisor will determine if vital areas have been penetrated or if sabotage is imminent.

Next Step:

If vital areas have been penetrated or if sabotage is imminent, implement Event 11.2.3.7. If intruders have been successfully interdicted, implement Event 11.2.3.8.

Data Required:

1. S-P-O-C to PA State Police.
2. Appropriate SSES contingency procedure(s).
3. Specific location of the intrusion.
4. The status of all vital area portals and alarms is monitored by both the SCC and ASCC Controllers utilizing the SDMS consoles and CRTs.
5. The Operations Shift Supervisor in conjunction with other responsible plant personnel makes the determination of whether or not the intruder had access to vulnerable vital systems.
6. The Operations Shift Supervisor, coordinating other responsible SSES plant personnel, will delineate safety measures to be taken in the event any system as determined in 5. above has been degraded.
7. Complete Security Officer reports are to be provided to the Security Controller.

11.2.3.5 Vital Area Intrusion

11.2.3.5.1 Vital Area Intrusion Alarm Annunciates in the SCC and ASCC

Objective:

Determine whether or not an intrusion into a vital area has occurred.

scene to investigate. The Security Controller will notify the Security Shift Supervisor and Operations Shift Supervisor.

- The Security Controller will direct the assessment of the alarm and implement the appropriate contingency procedure. When a vital door is involved, the Security Controller will retrieve names of persons having recently entered the area to assist in resolving the matter. If directed by the Security Shift Supervisor, the Security Controller will direct Security Officers to conduct a search of the appropriate area.
- NRC notified, (reference Responsibility Matrix 11.2.3.6.1)

Next Step:

If vital areas have been penetrated or if sabotage is imminent, implement Event 11.2.3.7. If something else is found amiss, implement Event 11.2.3.6.

Data Required:

(See Data Required Event 11.2.3.4.3.)

11.2.3.6 Miscellaneous Events

11.2.3.6.1 Member of the Security Force Fails to Perform Duty

Contact is lost with a member of the SSES Security Section, a member of the Security Section fails to report in, SCC/ASCC fails to respond to an alarm or some other indication exists that a Security Section member may have been incapacitated or may have compromised security.

Objective:

- Reestablish adequate level of protection.
- Determine if the Security Section member's failure to execute assigned duties has compromised security.

Decisions/Actions:

- The Security Shift Supervisor will ensure that one or more Security Officers are dispatched to investigate.
- The Security Shift Supervisor will ensure that appropriate compensatory measures to reestablish minimum accepted level of protection are taken.
- The Security Shift Supervisor will make the determination of whether or not the failure of the Security Section member has compromised security.
- NRC notified, as appropriate.

Next Step:

If protected area is penetrated, implement Event 11.2.3.4.4. If a vital area is penetrated or if sabotage is imminent, implement Event 11.2.3.7.

Data Required:

1. Location of Security Section member.
2. Procedures governing duties and responsibilities of each position in the Security Section.
3. Security Officer recall procedure.
4. Assessment of the cause of the Security Section member's failure to perform duty.
5. Assessment of SSES vulnerability due to failure of Security Section member.
6. Results of investigation within area(s) that may have been compromised by failure to perform assigned duties.

11.2.3.6.2 Suspected Bomb or Sabotage Device DiscoveredObjective:

Determine if object is a sabotage device.

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

emergency by dispatching Security Officers to compensate for any breached barriers or to provide access through any inoperable portal. Should an evacuation of the affected area be ordered, the Security Section will direct the actions necessary to accomplish this task.

- The Security Shift Supervisor will assure that all pertinent information pertaining to the incident is forwarded to the Security Controller and recorded. The Security Shift Supervisor will investigate the security-related aspects and impacts of the event insofar as technically capable, or call for off-site assistance if needed.
- The Security Shift Supervisor will attempt to determine whether or not the incident is security-related.
- NRC notified, as appropriate.

Next Step:

If occurrence is security-related, implement Event 11.2.3.7.

Data Required:

1. S-P-O-C for Salem Township Volunteer Fire Department, PA State Police and other appropriate off-site support organizations.
2. SSES procedures for fire and explosions.
3. Source of information regarding catastrophe.
4. A complete analysis of the affected area looking for degraded or threatened safety systems.
5. The Operations Shift Supervisor will ensure that appropriate corrective measures are implemented to compensate for any degraded system.
6. Results of investigation to determine cause of catastrophe.
7. Determination of areas in which security measures were compromised.
8. The assessment of vulnerabilities due to compromised security.



11.2.3.6.4 Internal Disturbance

A disturbance involving one or more individuals within the SSES perimeter other than one perceived to be short-lived and harmless outburst.

Objectives:

- Stop the disturbance.
- Minimize vulnerability of the SSES during the disturbance.

Decisions/Actions:

- The Security Shift Supervisor will direct the Security Section and access the magnitude of its effects upon the security system and specifically vital areas of the SSES.
- The assessment process in coordination with the Operations Shift Supervisor will determine whether or not personnel having safety responsibilities are involved.
- The Security Shift Supervisor will ensure that the disruption is met with an appropriate response to terminate the disturbance to include the requesting of off-site assistance if necessary.
- Along with the Operations Shift Supervisor, determine anticipated safety consequences, if any.
- The Security Shift Supervisor will determine if the disturbance is uncontrollable.

Next Step:

If disturbance is perceived to be uncontrollable, implement Event 11.2.3.7.

Data Required:

1. Exact location of the disruption.

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

Operations Shift Supervisor, who will institute an investigation. The Security Controller will dispatch a mobile patrol to the PA State Police, Shickshinny, PA, to advise of the failure.

- The Security Controller will direct on-duty Security Officers to assume defensive positions and if necessary, direct a Security Officer recall.
- NRC notified, as appropriate.
- The Operations Shift Supervisor will direct an investigation into the nonfunctioning equipment to determine the cause of the failure.
- The Security Shift Supervisor will, with the cooperation of maintenance personnel, determine whether or not the cause is security-related.

Next Step:

If loss is security-related, implement Event 11.2.3.8.

Data Required:

(See Data Required Event 11.2.3.6.)

11.2.3.7 Obvious Attempt to Sabotage or Confirmed Intrusion into Vital Area(s) in Progress

The discovery of a person(s) committing an act of sabotage against the SSES presents one of the most serious of all problems.

Objectives:

- Prevent access to vital equipment.
- Contain adversaries until arrival of PA State Police.
- Mitigate anticipated consequences.

Decisions/Actions:

- The on-duty Security Shift Supervisor will, if time permits, assess the situation by analyzing reports from Security Officers and other personnel or

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

by personally viewing the situation. If time does not permit the Security Shift Supervisor to assess the situation, the Security Controller will direct the Security Officers to neutralize the sabotage threat. After security personnel have neutralized the sabotage threat, they will have to ascertain whether or not the sabotage device is an explosive device.

- The Security Controller will through monitoring the SDMS, ensure security of vital area portals.
- Upon the direction of the Security Shift Supervisor, the Security Controller will request off-site assistance.
- NRC notified, as appropriate.
- The Operations Shift supervisor will make a clear determination on the safety of the SSES.
- The Operations Shift Supervisor, the Security Section and other SSES personnel will mitigate anticipated consequences of the act.
- If deemed appropriate by the Operations Shift Supervisor, appropriate portions of the Emergency Plan will be initiated whenever radiological release is perceived to be imminent or occur.

Next Step:

If intruders are captured or escape, implement Event 11.2.3.8. If off-site radiological consequences are imminent or occur, implement Emergency Plan.

Data Required:

1. Specific location of sabotage device.
2. Security procedures governing attempted sabotage.
3. SDMS data pertaining to status of vital area portals.
4. S-P-O-C for PA State Police.
5. Determination of set of vulnerable vital systems.

6. Delineation of safety measures to take in event of degradation of vital systems determined in 5. above.
7. Emergency Plan initiation procedures.

11.2.3.8 Sabotage Device Rendered Inoperable, Tampered/Deranged Equipment Restored, Intruder/Saboteur Captured or Escaped

Objective:

Determine whether or not any other intrusions or sabotage attempts have been made.

Decisions/Actions:

- Investigate for evidence of sabotage, sabotage devices or intrusions in all affected areas. Often, the Security Controller will be provided with pertinent data from the SDMS.
- The Security Controller, upon the direction of the Security Shift Supervisor, will notify all concerned parties, e.g. Operations Shift Supervisor, PA State Police, etc., of pending situation.
- The Security Section, along with other plant personnel, will determine whether or not anything is amiss.

Next Step:

Dependent upon the result of the investigation, return to Security Condition 1 if nothing is amiss.

Data Required:

1. Result of investigation.
2. S-P-O-C for each notified off-site party.

11.2.3.9 Loss or Degradation of Security System (Alarm Annunciation, Access Control, Tamper Alarm, Intrusion Detection)

The SDMS is a comprehensive computer based security system with redundant features and composed of five major subsystems; perimeter intrusion detection, threat assessment (CCTV), Access Control, Computer Based Security Management System and Operator Consoles.

Objectives:

- Determine if the degradation of the security system is partial or complete.
- Prevent unauthorized persons from penetrating the protected and vital area barriers.
- Determine whether or not a threat to the SSES exists.

Decisions/Actions:

- Because both the SCC and ASCC Controllers will have constant interface with the SSES Security System, any degradation will be noted instantly. After advising the appropriate supervisors of the situation, the Security Controller will implement the appropriate contingency procedure. Security Section personnel will assess any equipment malfunctions.
- The Security Controller will direct on-duty security personnel to assume defensive positions and declare an appropriate security condition. The function of the Security Section personnel is to neutralize any adversary threat or action that occurs in conjunction with a complete or partial loss of the SDMS.
- Upon direction of the Operations Shift Supervisor, the Security Controller will notify the PA State Police, Shickshinny and Wyoming, PA, and initiate a recall of off-duty Security Section personnel.
- NRC notified, as appropriate.

- The Operations Shift Supervisor after notification will initiate actions to repair the SDMS. In addition, the Operations Shift Supervisor in conjunction with the Security Shift Supervisor will attempt to determine the cause of the failure.

Next Step:

If perimeter intrusion alarm annunciates SCC/ASCC, implement Event 11.2.3.4.1. If confirmed protected area intrusion has occurred, implement Event 11.2.3.4.4. If vital area intrusion alarm annunciates in SCC/ASCC, implement Event 11.2.3.5.1. If obvious attempt to sabotage or confirmed intrusion into vital areas in progress, implement Event 11.2.3.7.

Data Required:

(See -Data Required Events 11.2.3.4.1, 11.2.3.4.4, 11.2.3.5.1 and 11.2.3.7 respectively.)

11.2.3.10 Loss of Protected Area Lighting

Objectives:

- Determine if the degradation is partial or complete.
- Prevent unauthorized person from penetrating the protected area barriers.
- Determine whether or not a threat to the SSES exists.

Decisions/Actions:

- The Security Controller will normally become aware of the loss of security lighting through system available in the SCC/ASCC, or be informed of the situation by on-duty security personnel. The Security Controller will notify the Security Shift Supervisor and the Operations Shift Supervisor.

- The Security Controller will direct on-duty Security Officers to assume defensive positions and neutralize any adversary threat that occurs. Upon direction of the Operations Shift Supervisor, the Security Controller will contact the PA State Police to advise of the situation or request a response. Preparations for a Security Officer recall will be made.
- NRC notified, as appropriate.
- The Operations Shift Supervisor upon receipt of a loss of lighting report, will initiate the actions necessary to investigate the loss of security lighting and repair the system as soon as possible. Also, in conjunction with the Security Shift Supervisor attempt to determine the cause of the lighting loss, specifically whether it was an accident or sabotage.

#### Next Step:

If obvious attempt to sabotage, implement Event 11.2.3.7. If confirmed protected area intrusion, implement Event 11.2.3.4.4.

#### Data Required:

(See Data Required Events 11.2.3.7 and/or 11.2.3.4.4 respectively.)

#### 11.2.3.11 Loss of Security System Power

Normal power to the SSES Security System is provided through an uninterruptable power source (UPS). Redundant diesel generators and back-up battery systems are available to provide service when needed.

#### Objectives:

- Determine if the loss of power is partial or complete.
- Prevent unauthorized persons from penetrating the protected and vital area barriers.
- Determine whether or not a threat to the SSES exists.

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

Decisions/Actions:

- Normally the Security Controller will be immediately aware of the loss of power whether partial or complete and will advise the Security Shift Supervisor and the Operations Shift Supervisor.
- After alerting the on-duty Security Officers of the loss of power, the Security Controller will, if necessary, direct on-duty Security Officers to assume defensive positions to neutralize any adversary threats should one occur in conjunction with the loss of power. Upon direction of the Operations Shift Supervisor, a Security Officer recall will be initiated and/or the PA State Police will be advised of the situation or requested to respond.
- NRC notified, as appropriate.
- The SSES Operations Shift Supervisor will initiate the actions necessary to investigate the loss of power and to repair or replace the system as soon as possible. In conjunction with the Security Shift Supervisor, the Operations Shift Supervisor will attempt to determine the cause of the power loss, specifically whether it was an accident or sabotage.

Next Step:

If confirmed intrusion into protected area, implement Event 11.2.3.4.4. If obvious attempt to sabotage or confirmed intrusion into vital areas in progress, implement Event 11.2.3.7.

Data Required:

(See Data Required Events 11.2.3.4.4 and 11.2.3.7 respectively.)

11.2.3.12 Aberrant Behavior (when observed by member of Security Section)

PP&L has developed a separate Employee Assessment Program to assist supervisors in recognizing those traits associated with aberrant behavioral patterns. Reporting



of such occurrences in accordance with that program's provisions is addressed in a separate format developed by PP&L. However, a member of the Security Section could observe such behavior, as it is recognized that any person, regardless of position, could exhibit such traits at any time.

Objectives:

- Identify and control the individual exhibiting the behavior pattern.
- Determine if the behavior pattern is a security threat or has caused a degradation on the security network or plant safety systems.
- Reestablish security commitments.

Decisions/Actions:

(See Decisions/Actions Event 11.2.3.6.4.)

Next Step:

If internal disturbance, implement Event 11.2.3.6.4.

Data Required:

(See Data Required Event 11.2.3.6.4.)

11.2.3.13 Hostage/Extortion Situations

Objectives:

- Determine if the threat is valid.
- Minimize vulnerability of the SSES security and safety systems to the situation.
- If imminent, anticipate consequences of the threat execution.
- Maintain security commitments for SSES.

Decisions/Actions:

- The Security Controller will normally receive the alarm or report from Security Officers at the scene or the Operations Shift Supervisor. The Security Shift Supervisor in conjunction with the Operations Shift Supervisor will decide whether the individual holding the hostage or exercising the extortion threat constitutes a threat of industrial sabotage or other unacceptable disruption of plant operations.
- The Security Controller will dispatch Security Officers to cordon-off the affected area and, if directed, initiate a Security Officer recall and request assistance from the PA State Police. The Security Officers when feasible, will prevent the incident from moving to vital areas and make efforts to contain the perpetrators.
- NRC notified, as appropriate.
- The Security Shift Supervisor and Operations Shift Supervisor will assess the implication of the threat on the security and safety of the SSES and anticipate any consequences of system(s) degradation.
- The Security Shift Supervisor is responsible for maintaining the SSES security commitments.

Next Step:

If a vital area has been penetrated, implement Event 11.2.3.7. If a protected area has been penetrated, implement Event 11.2.3.4.4.

Data Required:

1. Location of the hostage situation or extortion threat.
2. Hostage and/or extortion procedure for security personnel.
3. Security Officer recall procedure.
4. S-P-O-C PA State Police.

5. Results of assessment.
6. Vulnerability assessment.

#### 11.2.3.14 Security Officer Strike

Security Officers are unavailable for duty for reasons other than adversary action. Efforts will be made to determine the unavailability as far in advance as possible.

#### Objective:

- Verify the unavailability of Security Officers.
- Minimize vulnerability of SSES security network because of unavailability of Security Officers.
- Compensate for the unavailability of SSES Security Officers.

#### Decisions/Actions:

- The Supervisor of Security or his designated representative will determine that the number of SSES Security Officers who have failed to report for duty or that have reported for duty but failed to perform assignments properly is of such a nature that the minimum commitment to the security of the SSES cannot be achieved.
- Initiate the reserve force call out to properly compensate loss of regular Security Officer force.
- Prepare the SDMS for reserve security force access authorizations as well as prepare for weapons and equipment issue.
- Notification of PA State Police.
- NRC notified, as appropriate.

#### Next Step:

Any Event 11.2.3.1 through 11.2.3.13 occurs.

Event 11.2.3.5.3 Vital Area Found Unlocked and Unattended or Vital Area Barrier Found Breached

OBSERVER	SCC/ASCC CONTROLLER	SECURITY OFFICER	SECURITY SHIFT SUPERVISOR	OPERATIONS SHIFT SUPERVISOR	
<p>Reports observation to SCC Controller or member of Security section.</p> <p>If possible, maintains surveillance until relieved.</p>	<p>Receives notification.</p> <p>Declares Security Condition 2.</p> <p>Dispatches Security Officers to investigate and report.</p> <p>Notifies Security Shift Supervisor and Operations Shift Supervisor.</p> <p>If possible, utilizes CCTV to monitor barrier and/or implements contingency procedure to secure barrier.</p> <p>Determines whether or not equipment malfunctioned.</p> <p>Determines if intrusion has occurred                      .suspicious person in area                      .suspected bomb or sabotage device found                      .evidence of damage to equipment</p> <p>When directed, notifies NRC within one hour.</p> <p>Instructs Security Officers to conduct searches.</p> <p>If a determination is made that no intrusion has occurred, return to Security Condition 1.</p>	<p>Receives instructions to respond to investigate.</p> <p>Reports to SCC Controller on status of barrier.</p> <p>Secures barrier.</p> <p>Conducts search of area if directed.</p>	<p>Receives notification.</p> <p>Ensure contingency procedures implemented.</p> <p>Ensures affected area searched.</p> <p>Ensures return to Security Condition 1, or</p>	<p>Receives report of equipment malfunction.</p> <p>Orders repairs to be made.</p> <p>Evaluate impact on safety and security systems.</p> <p>Directs NRC notification.</p> <p>Authorizes return to Security Condition 1, or</p>	
←	If an intrusion has occurred, or there is obvious attempt to sabotage, implements Event 11.2.3.7.				→
←	If something else is amiss, implements Event 11.2.3.6.				→

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

## Event 11.2.3.6 Miscellaneous Events

## Events 11.2.3.6.1 Member of Security Section Fails to Perform Duty

OBSERVER .	SCC/ASCC CONTROLLER	SECURITY OFFICER	SECURITY SHIFT SUPERVISOR	OPERATIONS SHIFT SUPERVISOR	
<p>Observes member of Security force:          .unconscious          .asleep          .missing from post          .SCC/ASCC fails to respond.</p> <p>Reports observations to Security Shift Supervisor or SCC Controller.</p>	<p>Receives report.</p> <p>Declares Security Condition 2.</p> <p>Advises Security Shift Supervisor.</p> <p>Dispatches Security personnel to assess.</p> <p>Adjusts Security Condition as needed.</p> <p>Advises Operations Shift Supervisor.</p> <p>Determines if questioned behavior has compromised SSES security.          .Obviously security-related          .Evidence of intrusion          .Aberrant behavior of Security Officer          .Security Officer cannot be found          .Equipment malfunction          .Coincidental unresolvable alarms</p> <p>Notifies NRC as directed.</p> <p>If no compromise of security, return to Security Condition 1, or</p>	<p>Assesses the problem and relays information to SCC Controller.</p> <p>If security problems noted during assessment phase, secures scene.</p> <p>Return to Security Condition 1, or</p>	<p>Receives report.</p> <p>Supervises assessment.</p> <p>Determines security not compromised; authorizes return to Security Condition 1, or</p>	<p>Receives notification.</p> <p>Directs NRC notification if:          .Major loss of physical security effectiveness - within one hour (24 hours if properly compensated in a timely manner)          .Moderate loss of physical security effectiveness - within 24 hours (Logged in security record if properly compensated in a timely manner).</p> <p>Authorizes repair of equipment.</p>	
←		If there is a compromise of security,	implements Event 11.2.3.7 or Event 11.2.3.4.4.		→

**Event 11.2.3.12 Aberrant Behavior - When Observed by Member of Security Section**

SCC/ASCC CONTROLLER	SECURITY OFFICER	SECURITY SHIFT SUPERVISOR	OPERATIONS SHIFT SUPERVISOR
<p>Receives report of aberrant behavior.</p> <p>Notifies Operations Shift Supervisor and Security Shift Supervisor.</p> <p>Declares appropriate security condition.</p> <p>Dispatches Security Officers to control actions of individual, if appropriate.</p> <p>Researches SDMS to provide names of individuals processing through plant areas, if directed; provides results to Operations and Security Shift Supervisors.</p> <p>Dispatches Security Officers to search, if directed.</p> <p>Directs Security Officers to normal posting assignments and</p> <p>Declares Security Condition 1, or</p>	<p>Responds as directed.</p>     <p>Conducts search as directed.</p> <p>Responds as directed.</p>	<p>NOTE: During the absence of the Supervisor of Security from the SSES, the Security Shift Supervisor acts as the Supervisor of Security's designee.</p> <p>Evaluates information and coordinates actions with Operations Shift Supervisor.</p>   <p>Coordinates research of SDMS.</p>  <p>Coordinates search.</p> <p>Coordinates return to normal operations.</p>  <p>If internal disturbance persists,</p>	<p>NOTE: During the absence of the Superintendent of Plant from the SSES, the Operations Shift Supervisor acts as the Superintendent of Plant's designee.</p> <p>Evaluates information in regard to actions required to ensure safe operation of plant.</p>   <p>If deemed appropriate, directs SDMS research to track individual's processing through plant areas.</p> <p>Directs search of areas if applicable</p> <p>Directs return to normal operations upon determination that all is in order, or</p> <p>implements Event 11.2.3.6.4.</p>

2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE

11-87(G)

## Event 11.2.3.13 Hostage/Extortion Situations

SCC/ASCC CONTROLLER	SECURITY OFFICER	SECURITY SHIFT SUPERVISOR	SUPERVISOR OF SECURITY	OPERATIONS SHIFT SUPERVISOR	SUPERINTENDENT OF PLANT
<p>Normally receives an alarm from Security Officers or Operations Shift Supervisor.</p> <p>Declares Security Condition 4 for extortion threat or 5 for hostage situation.</p> <p>Dispatches Security Officers to cordon off area.</p> <p>Notifies Security Shift Supervisor, Operations Shift Supervisor, and Supervisor of Security.</p> <p>Evaluates information and implements appropriate contingency procedures.</p> <p>Notifies:          .PA State Police          .other off site agencies as needed.</p> <p>When directed, notifies NRC within one hour (within 24 hours if the extortion threat is more potential than explicit.)</p> <p>Initiates Security Section recall if needed.</p>	<p>Responds to affected area.</p> <p>Cordons off area.</p> <p>Provides information to SCC Controller.</p>	<p>NOTE: During the absence of the Supervisor of Security from the SSES, the Security Shift Supervisor acts as the Supervisor of Security's designee.</p> <p>Receives notification.</p> <p>Responds to scene.</p> <p>Directs the assessment.</p> <p>Coordinates with Operations Shift Supervisor.</p> <p>Determines whether or not incident is security-related and overall impact on the SSES security network.</p> <p>If hostage situation, establishes single-point-of-contact with the perpetrator. See note below.</p> <p>Ensures notification of off-site agencies and Security Section recall if needed.</p>	<p>Reviews all pertinent information.</p> <p>Ensures that contingency procedures are implemented.</p>	<p>NOTE: During the absence of the Superintendent of Plant from the SSES, the Operations Shift Supervisor acts as the Superintendent of Plant's designee.</p> <p>Receives notification.</p> <p>Notifies Superintendent of Plant.</p> <p>Uses Public Address (PA) system to keep SSES personnel away from affected area.</p> <p>Coordinates with Superintendent of Plant to determine possible effects on the plant's operations and safety systems.</p> <p>Authorizes notification of:          .PA State Police          .other off-site agencies as needed.</p> <p>Directs NRC notification as appropriate.</p> <p>After situation is resolved, directs return to normal, or</p>	<p>Receives notification.</p> <p>Provides assessment on effects on SSES operations and safety systems or feasibility of extortion action occurring.</p>
←		If analysis discloses that Vital Area is penetrated, implements Event 11.2.3.7.			→
←		If analysis discloses that Protected Area is penetrated, implements Event 11.2.3.4.4.			→
<p>NOTE: When LLEA or other off-site agency is negotiating with any perpetrator, a knowledgeable Company employee will be consulted on matters affecting public health and safety.</p>					

## APPENDIX F

## NRC REQUESTS FOR ADDITIONAL INFORMATION

During the period November 29 through December 1, 1978, the NRC staff visited the SSES for the purpose of resolving outstanding issues associated with the staff's review of this Plan.

On December 22, 1978, the NRC staff provided a Memorandum, Subject: Meeting Summary - Unresolved Items Related to the Security Plan for Susquehanna Units 1 and 2. Attachment 2 of the memorandum contained requests for additional information. Attachment 3 contained information relating to the status of unresolved items.

This Appendix provides a listing of the NRC questions (numbered 500.1 through 500.24), and PP&L replies to these questions based upon planning commitments and technical information available as of February 15, 1979.

On April 13 and May 25, 1979, NRC letters, Subject: Susquehanna Steam Electric Station, Unit Nos. 1 and 2, Request for Additional Information, transmitted questions 500.25 through 500.44. This Appendix provides a listing of these questions and PP&L replies to the questions based upon planning commitments and technical information available as of July 31, 1979.

On September 12, 1980, a meeting between the NRC Susquehanna Steam Electric Station Physical Security Plan Reviewer, other NRC officials and representatives of PP&L licensing, engineering and security was held at the Susquehanna Steam Electric Station. As a result of a suggestion by NRC personnel, the answers to questions 500.1 through 500.44, Appendix F, have been incorporated into the written text of the Plan. Appendix F has been revised to reflect the location within the Plan where answers may be located.

During March, 1981, the NRC forwarded an additional ten questions to PP&L for appropriate response. These questions have subsequently been added to this Appendix along with cross reference in-text location of responses.

During April, 1981, the NRC forwarded a request for additional information in regard to the Safeguards Contingency Plan. This request has been added to this Appendix along with cross reference in-text location of responses.

During an NRC/PP&L conference call on June 24, 1981, the NRC requested that Event 11.2.3.6.1 of the Responsibility Matrix and the following sub-paragraphs under Section 11.2.3 be amended to reflect NRC notification: 4.3, 4.4, 5.3, 6.1, 6.3, 6.6, 7, 9, 10, 11, 13 and 14. Additionally, the NRC requested that the statement during hostage/extortion negotiations, a knowledgeable Company employee will be consulted on matters affecting public health and safety, be included within Event 11.2.3.13 of the Responsibility Matrix, for clarification purposes.



2.790 MATERIAL  
WITHHOLD FROM PUBLIC DISCLOSURE