TABLE OF CONTENTS

CHAPTER 13

CONDUCT OF OPERATION

This chapter provides information relating to the preparations and plans for operation of the AP600. Its purpose is to provide reasonable assurance that the Combined License applicant can establish and maintain a staff of sufficient size and technical competence and that operating plans provide reasonable assurance of adequate protection of the public health and safety.

13.1 Organizational Structure of Applicant

This section is the responsibility of the Combined License applicant. The organizational structure must be consistent with the human system interface design assumptions. See Section 1.8 and Chapter 18 for interface requirements pertaining to organizational structure.

13.1.1 Combined License Information Item

Combined License applicants referencing the AP600 certified design will address adequacy of the organizational structure.

13.2 Training

Training programs are the responsibility of the Combined License applicant.

Chapter 18, Section 18.10 references WCAP 14655, "Designer's Input for the Training of the Human Factors Engineering Verification and Validation Personnel" that provides input for the Combined License applicant. This document describes input from the designer on the training of the operations personnel who participate as subjects in the human factors engineering (HFE) verification and validation. The WCAP also describes how training insights are passed from the designer to the Combined License applicant.

13.2.1 Combined License Information Item

Combined License applicants referencing the AP600 certified design will develop and implement training programs for plant personnel. This includes the training program for the operations personnel who participate as subjects in the human factors engineering verification and validation.

13.3 Emergency Planning

Emergency planning is the responsibility of the Combined License applicant. See subsection 1.2.5 for the locations of the technical support center, the operational support center and the decontamination facilities. See Section 9.4 for a description of the HVAC systems for the main control room/technical support center and the annex building. See Section 18.8 for the high level requirements for the technical support center and the operational support

center. See Section 7.5 for identification of plant variables that are provided for interface to the emergency planning areas.

Communication interfaces among the main control room, the technical support center and the emergency planning centers are the responsibility of the Combined License applicant.

Staffing of the emergency operations facility occurs consistent with current operating practice and with revision 1 of NUREG-0654/FEMA-REP-1 except for a loss of offsite power and loss of all onsite AC power. For this initiating condition, the Combined License applicant shall immediately activate the emergency operations facility rather than bringing it to a standby status.

13.3.1 Combined License Information Item

Combined License applicants referencing the AP600 certified design will address emergency planning including post-72 hour actions and its communication interface.

Combined License applicants referencing the AP600 certified design will address the activation of the emergency operations facility consistent with current operating practice and NUREG-0654/FEMA-REP-1 except for a loss of offsite power and loss of all onsite AC power. For this initiating condition, the Combined License applicant shall immediately activate the emergency operations facility rather than bringing it to a standby status.

To initially and continuously assess the course of an accident for emergency response purposes, Combined License applicants referencing the AP600 certified design will address the capability for promptly obtaining and analyzing grab samples of reactor coolant and containment atmosphere and sump in accordance with the guidance of Item II.B.3 of NUREG-0737.

13.4 Operational Review

This section is the responsibility of the Combined License applicant.

13.4.1 Combined License Information Item

Combined License applicants referencing the AP600 certified design will address each operational review.

13.5 Plant Procedures

Plant procedures are the responsibility of the Combined License applicant. References to applicable combined license information are included in Section 1.8. This includes, for example, reference to guidelines on inservice inspection in Chapters 3 and 6, and initial testing in Chapter 14. Operational experience and the resolution of generic issues to be considered in the preparation of plant procedures is outlined in Section 1.9.

Reference 1 provides input to the Combined License applicant for the development of plant operating procedures, including information on the development and design of the AP600 emergency response guidelines and emergency operating procedures. Also included in Reference 1 is information on the computerized procedure system, which is the human system interface that allows the operators to execute the plant procedures.

The computerized procedure system is not part of the AP600 design scope that the Nuclear Regulatory Commission is being asked to approve. The acceptability of the computerized procedure system, and its backup, for application to the AP600 design will be determined during the implementation of the AP600 verification and validation program (see DCD Section 18.8) and reviewed as part of an application for a combined license.

WCAP-14837 (Reference 4) provides input to the Combined License applicant for the development of plant specific refueling plans.

13.5.1 Combined License Information Item

Combined License applicants referencing the AP600 certified design will address plant procedures including the following:

- Normal operation
- Abnormal operation
- Emergency operation
- Refueling and outage planning
- Alarm response
- Maintenance, inspection, test and surveillance
- Administrative
- Operation of post-72 hour equipment

13.6 Security

13.6.1 Preliminary Planning

Objectives and functional requirements of the AP600 physical protection system and description of security features are provided in the AP600 Security Design Report, submitted under separate cover in accordance with 10 CFR 2.790(d), Rules of Practice. The report also includes the security boundary drawings and the listing of the vital equipment and components. A vulnerability analysis, which demonstrates that the AP600 certified security design is adequate to protect the AP600 from radiological sabotage, is also submitted under separate cover.

As demonstrated by the AP600 Security Design Vulnerability Analysis Report, reducing the protected area and eliminating the isolation zones results in a reduced requirement for security staffing when compared to current plants. Personnel screening, selection, performance evaluation, and training aspects of the physical security program will be addressed by the Combined License applicant.

13.6.2 Security Plan

The comprehensive physical security program is the responsibility of the Combined License applicant and will be addressed in the security plan, contingency plan, and guard training plan provided by the Combined License applicant.

13.6.3 Plant Protection System

13.6.3.1 Introduction

A physical protection system and security organization is provided to protect the AP600 from radiological sabotage, as required by 10 CFR 73.55. To achieve this objective, the physical protection system:

- Includes a security organization
- Locates vital equipment within vital areas
- Controls points of personnel, vehicle, and material access into the protected and vital areas
- Annunciates alarms in a continuously manned central alarm station and at least one other continuously manned alarm station that is physically separated from the central alarm station
- Provides for continuous communications between the security officers and the continuously manned alarm stations
- Provides for testing and maintenance of the alarms, communications, and physical barriers
- Responds to threats of radiological sabotage in accordance with a developed contingency plan

13.6.3.2 Design Basis

The physical protection system protects against radiological sabotage events, following the requirements of 10 CFR 73.55(a). The design basis and assumptions for the design are provided by the Security Design Report, Reference 2, and the Security Design Vulnerability Analysis Report, Reference 3. The following assumptions are made:

- The intrusion detection systems cannot be disabled without detection and timely response by the security force.
- Unless precluded by plant design features or prevented by the plant security system, insider sabotage can potentially result in an initiating event requiring actuation of safe

shutdown systems, disabling of safe shutdown systems, disabling of nonsafety-related systems (including offsite power), or any combination of these.

- In evaluating vulnerability to internal sabotage, onsite security system features, offsite resources or both are effective in preventing undetected penetration into the protected area by outsiders.

- While access to containment for maintenance and testing during operation at power is permitted, such access is controlled and typically nonroutine.

- The continuous presence of several employees precludes acts of sabotage in the control room. However, the control room is a vital area and will be protected in accordance with 10 CFR 73.55.

- Equipment and systems designated as vital for full power operation shall be maintained as vital in other modes of plant operation. However, during unit shutdown, a vital area can be declassified to nonvital if approved by the security plan.

- Sabotage events do not occur coincident with some other independent single failure or independently initiated event.

- The security restrictions for access to equipment and plant regions will be compatible with loss of site power, access requirements, fire protection, health physics, and local operator actions required for event mitigation. During operating modes, security access control restrictions will not excessively impede operator functions.

13.6.4 Physical Security Organization

The description of the site-specific physical security organization is the responsibility of the Combined License applicant. The size and capabilities of the physical security organization's armed response team are established by the vulnerability analysis that demonstrates the acceptability of the AP600 certified security design. The required manning for the security force armed response team is established in design certification and is contained in Reference 3.

13.6.5 Physical Barriers

13.6.5.1 Protected Area

The AP600 security design features a collapsed protected area boundary that does not require a perimeter fence such as those found in conventional security plans. Where there are portals for personnel or material access into the vital areas, protected areas surround the portals. Protected area barriers provide an outer boundary to prevent unauthorized access to the vital areas of the plant without detection. The protected area barriers are constructed, as a minimum, of chain link fence equivalent to the physical barrier defined in 10 CFR 73.2 for fences. The protected area barriers are constructed so that any attempt to penetrate into the

protected areas will activate counter measures in response to the threat. The protected area is equipped with CCTV and has intrusion detection equipment and alarms that annunciate upon detection of penetration to alert security response forces that the area has been breached. Descriptions of the protected areas and the drawings showing the location of the protected areas are provided in Reference 2.

13.6.5.2 Vital Areas

Vital equipment is located within designated vital areas. The AP600 vital areas are encompassed by the boundary formed by the shield building, a reinforced concrete and steel structure surrounding containment, and by portions of the reinforced concrete perimeter and interior walls of the auxiliary and annex buildings. Accessible and unmonitored portions of the boundary walls, floors, ceilings, windows, doors and penetrations are hardened for security. Accessible is defined as 18 feet above the base of a wall that can be reached by normal means of walking, climbing fixed ladders, or using hand-carried step up devices. Unmonitored is defined as not being visible to a continuously manned location or to intrusion detection alarms. The security hardened barriers are constructed of sufficient structural integrity to significantly delay a perpetrator trying to penetrate the boundary in order to gain access to vital equipment. The delay times of these barriers are sufficient to allow timely response by security and plant personnel to neutralize a sabotage attempt. Access points to vital areas are locked and alarmed with active intrusion detection systems. Protected areas that surround the access points to the vital areas are equipped with CCTV that is monitored at the alarm stations. The vital areas and a listing of the vital equipment are provided in Reference 2.

13.6.5.3 Bullet-Resisting Barriers

The doors, walls, floor, and ceiling of the control room and the continuously manned alarm stations are designed to meet the bullet-resisting criteria of UL-752, High Power Rifle Rating, including resistance to a level 4 round.

13.6.5.4 Vehicle Barrier System

The vital areas are surrounded by a vehicle barrier system that provides a barrier such that no location along the perimeter will permit forced entry of a vehicle. The vehicle barrier system is designed to stop the Design Basis Vehicle before it reaches the safe standoff distance for the vital equipment located inside the vital areas. No point along the perimeter of the vehicle barrier system is located closer than the minimum safe standoff distance for the vital area barrier. Vital equipment/components are not expected to be damaged to the extent that they are no longer able to maintain the plant in a safe condition as a result of detonation of a design basis bomb at the vehicle barrier system boundary. Active gates are located at the two vehicle portals that provide the only access for vehicles to enter the area enclosed by the vehicle barrier system. Vehicles that are authorized for access and that have a need to enter the area enclosed by the vehicle barrier system are searched at these gates for items that could be used for radiological sabotage. There is no general parking within the area enclosed by

the vehicle barrier system. A description of the vehicle barrier system and the drawings showing the location of the vehicle barrier system are provided in Reference 2.

13.6.6 Access Requirements

Positive control features are implemented to provide authorization for personnel and vehicles entering the protected and vital areas. The Combined License applicant is responsible for the following access control features:

- Means for positive identification of authorized personnel entering the protected and vital areas.
- Means for searching individuals, packages, and materials for firearms, explosives, and incendiary devices. This may be accomplished using detection devices such as metal detectors, explosive detectors, and x-ray machines.

The AP600 design certification scope includes:

- Access portals entering the protected and vital areas are identified and unmanned portals are provided with alarm annunciation in the continuously manned alarm stations.
- Protected and vital area ingress and egress are designed to interface with other plant requirements and not impair plant operations during emergency conditions.

13.6.7 Detection Aids

13.6.7.1 Perimeter

Except for the special provisions provided for the shield building, intrusion detection at the perimeter of the plant is not required. A description of the intrusion detection provisions provided for the shield building are provided in Reference 2.

13.6.7.2 Protected Area

An intrusion detection system is utilized to notify the security organization of any unauthorized attempt to gain access into the protected areas. CCTV is installed in unmanned protected areas. Doors entering a protected area are equipped with an alarm to detect tampering and unauthorized access into the protected area. A description of the intrusion detection provisions provided for the AP600 is provided in Reference 2.

13.6.7.3 Vital Area

Doors entering a vital area are hardened to provide significant delay time and are alarmed to detect tampering and unauthorized access into the vital area. The delay times for doors accessing the vital areas are sufficient to allow timely response by the security organization

to attempted penetrations. A description of the intrusion detection provisions provided for the AP600 is provided in Reference 2.

13.6.8 Security Lighting

Security lighting is provided for the alarm stations and the protected areas. A description of the security lighting provided for the AP600 is provided in Reference 2.

13.6.9 Security Power Supply System

Security equipment that supports critical monitoring functions, that is, intrusion detection, alarm assessment, and the security communication system, receive power from the security-dedicated uninterruptable power supply (UPS) system. Switchover to the uninterruptable power supply system is automatic and does not cause false alarms on annunciation modules. The uninterruptable power supply system is capable of sustaining operation for a minimum of 24 hours. A description of the security power supply system provided for the AP600 is provided in Reference 2.

13.6.10 Communications

A description of the AP600 Security Communication System is provided in Reference 2. Specific details for the security communication system will be addressed by the Combined License applicant.

Two two-way communications paths are provided between the control room and the alarm stations within the AP600. A single act of sabotage cannot sever both communication paths. Security force members with responsibilities to respond to acts of sabotage have the capability for continuous two-way communication with the alarm stations, and with each other. The centralized communication equipment and radio antenna are located in a controlled area so that they will remain operable during a radiological sabotage event.

Non-portable security communications equipment are fed from the security power supply system so that they remain operable in the event of the loss of normal power.

13.6.11 Testing and Maintenance

The Combined License applicant will address testing and maintenance aspects of the plant security system.

13.6.12 Response Requirements

The Combined License applicant will address response requirements of the plant security program.

13.6.13 Combined License Information Item

13.6.13.1 Security Plans, Organization, and Testing

Combined License applicants referencing the AP600 certified design will address site-specific information related to the security, contingency, and guard training plans. Those plans will include descriptions of the tests planned to show operational status, maintenance of the plant security system, the security organization, communication, and response requirements.

The Combined License applicant will develop the comprehensive physical security program which includes the security plan, contingency plan, and guard training plan. Each COL applicant will describe in its physical security plan how the requirements of 10 CFR Part 26 will be met. At least 60 days before loading fuel, the Combined License applicant will confirm that the security systems and programs described in its physical security plan, safeguards contingency plan, and training and qualification plan have achieved operational status and are available for the staff's inspection. Operational status means that the security systems and programs are functioning. The determination that operational status has been achieved will be based on tests conducted under realistic operating conditions of sufficient duration to demonstrate that:

- the equipment is properly operating;
- procedures have been developed, approved, and implemented; and
- personnel responsibility for security operations and maintenance have been appropriately trained and have demonstrated their capability to perform their assigned duties and responsibilities.

13.6.13.2 Vital Equipment

Combined License applicants referencing the AP600 certified design will verify that the as-built location of vital equipment is inside the vital areas.

13.6.13.3 Plant Security System

Combined License applicants referencing the AP600 certified design will address site-specific information related to the maintenance and testing of the plant security system including the intrusion detection and assessment system, the access control features specified in subsections 13.6.6, 13.6.7.2, and 13.6.7.3, and the vehicle barrier system. The Combined License applicant will address in its safeguards plans how the physical protection system will provide the protection stated in subsection 13.6.3.2.

13.7 References

1. WCAP 14690, "Designer's Input To Procedure Development for the AP600," Revision 1, June 1997.

2. AP600 Security Design Report, Revision 6, July 1998.

3. AP600 Security Design Vulnerability Analysis Report, Revision 3, July 1998.

4. WCAP 14837, "AP600 Shutdown Evaluation Report," Revision 3, March 1998.