protected area must be checked for proper authorization and visually searched for explosives before entry.

(10) Written response procedures must be established and maintained for addressing unauthorized penetration of, or activities within, the protected area including Category 5, ''Procedures,'' of appendix C to part 73. The licensee shall retain a copy of response procedures as a record for 3 years or until termination of the license for which the procedures were developed. Copies of superseded material must be retained for 3 years after each change or until termination of the license.

(11) All detection systems and supporting subsystems must be tamper indicating with line supervision. These systems, as well as surveillance/assessment and illumination systems, must be maintained in operable condition. Timely compensatory measures must be taken after discovery of inoperability, to assure that the effectiveness of the of the security system is not reduced.

(12) The physical protection program must be reviewed once every 24 months by individuals independent of both physical protection program management and personnel who have direct responsibility for implementation of the physical protection program. The physical protection program review must include an evaluation of the effectiveness of the physical protection system and a verification of the liaison established with the designated response force or LLEA.

(13) The following documentation must be retained as a record for 3 years after the record is made or until termination of the license. Duplicate records to those required under § 72.180 of part 72 and § 73.71 of this part need not be retained under the requirements of this section:

(i) A log of individuals granted access to the protected area;

(ii) Screening records of members of the security organization;

(iii) A log of all patrols;

(iv) A record of each alarm received, identifying the type of alarm, location, date and time when received, and disposition of the alarm; and

(v) The physical protection program review reports.

(e) A licensee that operates a GROA is exempt from the requirements of this section for that GROA after permanent closure of the GROA.

[63 FR 26962, May 15, 1998, as amended at 63 FR 49414, Sept. 16, 1998; 66 FR 55816, Nov. 2, 2001]

§ 73.54 Protection of digital computer and communication systems and networks.

By November 23, 2009 each licensee currently licensed to operate a nuclear power plant under part 50 of this chapter shall submit, as specified in § 50.4 and § 50.90 of this chapter, a cyber security plan that satisfies the requirements of this section for Commission review and approval. Each submittal must include a proposed implementation schedule. Implementation of the licensee's cyber security program must be consistent with the approved schedule. Current applicants for an operating license or combined license who have submitted their applications to the Commission prior to the effective date of this rule must amend their applications to include a cyber security plan consistent with this section.

(a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.

(1) The licensee shall protect digital computer and communication systems and networks associated with:

(i) Safety-related and important-to-safety functions;

(ii) Security functions;

(iii) Emergency preparedness functions, including offsite communications; and

(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

(2) The licensee shall protect the systems and networks identified in paragraph (a)(1) of this section from cyber attacks that would:

(i) Adversely impact the integrity or confidentiality of data and/or software;

(ii) Deny access to systems, services, and/or data; and

(iii) Adversely impact the operation of systems, networks, and associated equipment.

(b) To accomplish this, the licensee shall:

(1) Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks to satisfy paragraph (a) of this section,

(2) Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section; and

(3) Incorporate the cyber security program as a component of the physical protection program.

(c) The cyber security program must be designed to:

(1) Implement security controls to protect the assets identified by paragraph (b)(1) of this section from cyber attacks;

(2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks;

(3) Mitigate the adverse affects of cyber attacks; and

(4) Ensure that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber attacks.

(d) As part of the cyber security program, the licensee shall:

(1) Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.

(2) Evaluate and manage cyber risks.

(3) Ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained.

(e) The licensee shall establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of this section.

(1) The cyber security plan must describe how the requirements of this section will be implemented and must account for the site-specific conditions that affect implementation.

(2) The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will:

(i) Maintain the capability for timely detection and response to cyber attacks;

(ii) Mitigate the consequences of cyber attacks;

(iii) Correct exploited vulnerabilities; and

(iv) Restore affected systems, networks, and/or equipment affected by cyber attacks.

(f) The licensee shall develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

(g) The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.

(h) The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.

[74 FR 13970, Mar. 27, 2009]

§ 73.55 Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.

(a) *Introduction.* (1) By March 31, 2010, each nuclear power reactor licensee, licensed under 10 CFR part 50, shall implement the requirements of this section through its Commission-approved Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and Cyber Security Plan referred to collectively hereafter as ''security plans.'' Current applicants