U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

July 2007
Division 5

DRAFT REGULATORY GUIDE

Contact: P. Lee
(301) 415-8111

DRAFT REGULATORY GUIDE DG-5021

MANAGING THE SAFETY/SECURITY INTERFACE

A. INTRODUCTION

This draft regulatory guide provides an approach acceptable to the Nuclear Regulatory Commission (NRC) for managing the safety/security interface at nuclear power plants. Title 10, Section 73.58, of the *Code of Federal Regulations* (10 CFR 73), "Physical Protection of Plants and Materials," (Ref. 1) requires NRC licensees to assess and manage safety and security activities. If implemented by licensees, the approach and examples described in this guidance would provide reasonable assurance of adequate protection for the interface of safety and security, but are not intended to be all-inclusive, and licensees may employ alternative methods for implementing NRC regulations. This draft regulatory guide would be applicable to operating reactors licensed in accordance with 10 CFR Parts 50 (Ref. 2) and 52 (Ref. 3), and new applicants should consider this guidance in preparing an application for a combined license (COL) under 10 CFR Part 52. The licensee bears sole responsibility for ensuring that the potential for adverse affects on safety and security is managed and assessed to provide adequate protection of public health and safety, protection of the environment, and common defense and security. Licensee questions regarding regulatory requirements for the management of safety/security interface should be directed to the appropriate NRC Headquarters or Regional staff.

The proposed addition of Section 73.58 to Part 73 (Ref. 4) requires licensees to assess and manage safety and security activities to ensure that these activities do not adversely affect each other and that compliance with applicable security requirements in 10 CFR Part 73 or requirements in 10 CFR Part 50 or 52, and related regulations regarding the safety of the reactor and plant operations, are maintained. This requirement is intended to require licensees to coordinate and plan activities to prevent potential adverse conditions that could negatively impact either plant safety or security.

Section 10 CFR 73.58(a)(1) requires licensees to assess and manage the potential for adverse effects between safety and security (including the site emergency plan) before implementing changes to plant configurations, facility conditions, or security. Additionally, in accordance with 10 CFR 73.58(a)(2), the scope of changes to be assessed and managed must include planned and emergent activities such as, but not limited to, physical modifications, procedural changes, maintenance activities, system reconfigurations, access control modifications or restrictions, and security contingency or

emergency plans changes. In addition, 10 CFR 73.58(b) requires that when potential adverse interactions are identified, licensees must communicate them to the appropriate licensee personnel and take corrective or compensatory actions to maintain safety and security in accordance with applicable regulations, orders, license conditions, and requirements for nuclear operations and the protection of nuclear material.

To meet the requirements of 10 CFR 73.58, licensees should establish and implement controls necessary to inform and coordinate safety and security activities. The performance goal is to minimize the potential for unintended adverse impact on safety or security performance from changes to the site, facilities, programs, plans, or procedures, such as those related to engineering, operations, safety, security, or emergency preparedness, prior to their implementation. The intent includes assurance that security is actively and appropriately considered during the planning for design, construction, maintenance, and day-to-day operations. Similarly, interface and impact to safety should be considered during the planning and design of security-related activities. The changes or activities to be reviewed may be temporary or permanent. If the implementation is such that there is a potential for an adverse effect, licensees should take the appropriate compensatory or mitigating actions along with the implementation of the change. If the conclusion of the assessment is that the implementation would have an adverse effect on either safety or security, and no appropriate compensatory or mitigating action is possible, then it is the intent of the requirement in 10 CFR 73.58 that the proposed change should not be implemented, or it should be deferred until such a time when appropriate compensatory or mitigating actions are identified and can be implemented without degrading safety and security requirements. The exception is under extreme emergency conditions where it may not be possible to adequately consider all safety/security interfaces, as permitted in accordance with applicable regulations.

The NRC issues regulatory guides to describe methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants and licensees. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required.

This regulatory guide contains information collections that are covered by the requirements of 10 CFR Part 73 which the Office of Management and Budget (OMB) approved under OMB control number 3150-0002. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

Background

The performance goal for managing safety/security interface is to minimize the potential for adverse impact on safety or security performance while implementing changes. This may be accomplished by providing management controls or processes that effectively facilitate the interface between safety and security requirements for the conduct of plant operations that range from normal to emergency modes of operations and from the design of facilities, processes, or systems to routine surveillance, testing, and maintenance of structure, systems, and components (SSCs), and the implementation of programs and procedures at a nuclear power plant. NRC licensees should establish a means of communicating information to licensee management that supports informed decisions and

result in actions that preserve safety and security. The management controls or processes necessary for managing the safety/security interface should already be in place, within a licensee's established operating infrastructure for operations, safety, and security, and should not be new to an operating reactor licensee.

Following the events of September 11, 2001, the NRC issued Orders to licensees to enhance security at nuclear power plants and other locations. In implementing measures to meet the enhanced security requirements, NRC licensees instituted a significant number of security system upgrades and configuration changes, along with new and revised procedures. These activities highlighted the need for addressing plant activities (such as design, configuration control, construction, maintenance, and operations) that could compete or conflict with the licensees' obligations to provide high assurance of adequate protection of common defense and security. Conversely, these changes in the plant's security programs, systems, and operations also highlighted the need to address potential adverse effects on plant operations, safety-related SSCs, operator actions, or emergency responses necessary to prevent or mitigate postulated design basis accidents, and to protect public health and safety and the environment.

These changes in licensee security programs increased the potential for security goals, requirements, and implementing procedures to conflict or compete with safety goals, requirements, or procedures. Security should be balanced with operations or safety programs goals or requirements for safety (i.e., prevention, mitigation, or response) that manage the risk and consequences of postulated design basis accidents. Similarly, if a licensee's existing management controls or processes do not consider security early on in the planning stages, later changes in plant safety or operations could adversely impact security programs, systems, activities, and the bases and assumptions of the site's security protective strategies. A common example of security activities that could adversely affect safety is the securing of doors or other facility egress pathways which could impede operator actions in responding to or mitigating a safety-related emergency. Examples of adverse impact on security are (a) the removal of a barrier during construction or maintenance activities, defeating the performance and function of the barrier to delay the adversary and allowing easy passage into the protected area (PA) or vital area (VA), and (b) the introduction of construction scaffolding or demolition debris that delays a planned and credited security response that result in outcomes that have degraded effectiveness or capabilities of the physical protection system (PPS).

The licensee's efforts to manage interfaces between safety and security should ensure that security-related plans and implementing procedures are mutually supportive and balanced with operations, safety, and emergency plans and implementing procedures. A licensee's management controls or processes, such as engineering or design management, configuration management, work controls, construction, and maintenance, should be capable of reviewing and assessing the safety/security interface for nuclear operations, including resolution of issues. It should also be capable of addressing concerns during the planning of projects, activities, or work, thereby preventing unintended degradation to safety or security. The established management controls or processes that identify adverse effects should result in the implementation of appropriate corrective actions and equivalent compensatory measures, and should address root causes, providing an overall balance between conflicting or competing goals for safety and security.

This regulatory guide is being developed to provide guidance to an applicant or a licensee on the requirements of the proposed amendment to 10 CFR Part 73. This regulatory guide should assist an applicant or licensee in developing and implementing management controls or processes regarding the safety/security interface that will satisfy the requirements of the rule.

C. REGULATORY POSITION

1. Requirements and Applicability of Managing The Safety/Security Interface

The 10 CFR 73.58, "Safety/security interface requirements for nuclear power reactors," applies to all operating nuclear power reactors licensed under 10 CFR Parts 50 and 52. The proposed language for 10 CFR 73.58 is as follows:

- The regulations in 10 CFR 73.58(a)(1) state that "The licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to the plant configurations, facility conditions, or security."
- The regulations in 10 CFR 73.58(a)(2) state that "The scope of changes to be assessed and managed must include planned and emergent activities (such as, but not limited to physical modifications, procedural changes, changes to operator actions or security assignments, maintenance activities, system reconfiguration, access modification or restrictions, and changes to the security plan and its implementation)."
- The regulations in 10 CFR 73.58(b) state that "Where potential adverse interactions are identified, the licensee shall communicate them to appropriate licensee personnel and take compensatory and/or mitigative actions to maintain safety and security under applicable Commission regulations, requirements, and license conditions."

The purpose of the requirements is to:

- identify potential adverse effects on safety and security measures before implementing changes;
- assess proposed changes and manage potential adverse effects that could impact compliance with NRC regulations (the new requirements are not intended to substitute for existing requirements);
- communicate potential adverse interactions to the appropriate licensee personnel; and
- take appropriate compensatory and mitigating actions to maintain safety and security consistent with applicable NRC requirements.

In addition, 10 CFR Part 73.55 states the following requirements for managing the safety/security interface:

- The regulations in 10 CFR 73.55(n)(2)(ii) require that "onsite physical protection program reviews and audits must include, but are not limited to, an evaluation of the effectiveness of the approved security plans, implementing procedures, response commitments by local, State, and Federal law enforcement authorities, cyber-security program, safety/security interface, and the testing, maintenance, and calibration program."
- The regulations in Section 10 CFR 73.55(s) require that "in accordance with the requirements of §73.58, the licensee shall develop and implement a process to inform and coordinate safety and security activities to ensure that these activities do not adversely affect the capabilities of the security organization to satisfy the requirements of this section, or overall plant safety."
- In accordance with 10 CFR Part 73, Appendix C, Section II (f)(4), "licensees shall address safety/security interface issues in accordance with the requirements of §73.58 to ensure activities by the security organization, maintenance, operations, and other onsite entities are coordinated in a manner that precludes conflict during both normal and emergency conditions."

2. An Acceptable Approach for Meeting Requirements of 10 CFR 73.58

2.1 Introduction

Licensees (or applicants) should establish and implement controls or processes necessary to assess and manage the potential for adverse safety and security interactions that may result from changes to the configuration of the site, SSCs, and procedures. The objective of these controls or processes is for licensees to identify potential adverse interactions between safety and security activities prior to implementation of such activities, and where such adverse interfaces are identified during implementation, to consider appropriate compensatory or mitigative actions to maintain safety and security consistent with applicable NRC requirements.

2.2 Identify and Evaluate Safety/Security Significance Changes

Licensees should establish controls or processes to identify changes, from both planned and emergent activities, to the facility or procedures that could impact (a) the effectiveness, reliability, and availability of physical protection systems that protect target sets (i.e., systems, equipment, and people), (b) the effective implementation of the protective strategy against the Design Basis Threat (DBT) as required by 10 CFR 73.1, and (c) the effectiveness of security contingency responses and requirements that are described in the site security plans, implementing procedures, regulations, and license conditions. Similarly, licensees should establish controls or processes to identify and evaluate security-related changes, from both planned and emergent activities, that could impact safe plant operations, including emergency planning.

2.3 Use Existing Controls and Processes

The requirements for managing the safety/security interfaces in 10 CFR 73.58 may be met by already established management controls or processes such as the Plant Operations Review Committees, Plant Review Boards, Safety Review Committees, Independent Safety Reviews, Work Planning and Controls, Configuration Management, Review and Audit Program, Corrective Actions and Reporting Program, Engineering, Design, and Project Management, Maintenance, and other controls that exist at an operating nuclear power plant. These management controls or processes typically ensure that licensee personnel identify, describe, review, approve, monitor, implement, and/or document day-to-day and planned operations or activities.

It is the NRC's position that, because of other existing regulatory requirements, all licensees of operating power reactors currently have in place the necessary management controls or processes for reviewing, assessing, and managing plant activities or changes to provide continued assurance of adequate safety and security. Therefore, though existing programs may not explicitly require consideration of the safety/security interface, the NRC believes that these concerns have been addressed indirectly by the existing programs. However, Section 10 CFR 73.58 adds an express requirement to Part 73 for licensees to manage and assess these activities. As such, an acceptable approach is for licensees to explicitly address the requirement to assess and manage the safety/security interface in existing umbrella programs or process documents and associated implementing procedures that govern the plant engineering modifications, plant work control and planning, plant procedure modifications, and quality assurance program. Licensees may include other plant programs or processes deemed necessary, as the four identified are not limiting but instead establish a minimum for assuring an adequate safety/security

interface. Also, an alternative acceptable approach is that licensees may develop a single overriding or crosscutting procedure that is applicable to the four key programs or processes identified above and such a procedure would assure the flow-down of the requirements into the associated implementing procedures.

2.4 Incorporate Reviews in Plant Programs

Planned changes to the facility or procedures should be adequately addressed by current processes identified above in Section 2.3. Emergent activities, due to their nature, are more likely to result in conflicts between safety and security.

Listed below are plant programs, including implementing procedures, that should be considered, and examples of potential outcomes that may occur or may have been experienced at nuclear facilities as a result of a less than adequate consideration of safety/security interface. The examples provided are not intended to be either limiting or all-inclusive, but only illustrative of where adequate management controls or processes should minimize the likelihood of inadvertent degradation of safety or security performances.

2.4.1 Examples of Program Areas

The following are program areas that a licensee should pay particular attention to and review changes to in order to identify and assess possible safety/security interface concerns for NRC-regulated activities:

- Operations (includes maintenance, construction, work management, nuclear training)
- Nuclear engineering and support (includes nuclear safety and analysis, criticality safety)
- Radiation protection
- Emergency preparedness or planning
- Fire protection
- Chemical safety
- Environmental protection
- Industrial health and safety
- Security (physical, personnel and information)

2.4.2 Examples of Potential Safety/Security Interfaces

The following are examples of potential concerns for the safety/security interface that may occur due to conflicting performance goals or requirements between safety and security. Adequate management controls or processes should identify, prevent, and resolve undesired outcomes (actual or potential) that degrade the performance of plant safety or security for nuclear operations and related activities:

- Construction work that inadvertently causes a loss of primary power to multiple zones of the PA perimeter lighting systems needed for visual assessment and/or disrupts continuity of alarm

transmission by the PA perimeter intrusion detection and assessment system (PIDAS), resulting in an unplanned loss of detection and assessment capabilities

- Staging of construction trailers or heavy equipment for a refueling outage in the vicinity of PA perimeter security barriers, inadvertently providing cover and concealment by creating shadows and decreased illumination in the field of vision for assessment and the obstruction of lines of sight for security responders, impacting the site's security protective strategy
- Parking of an unsecured forklift near a roll-type door at a facility's shipping dock, inadvertently providing a means for an adversary to reduce task time for defeating security access delays for entry, invalidating planning assumptions regarding security force response time and decreasing the probability of interrupting or neutralizing adversaries
- Planned fire protection manual operator actions to mitigate postulated design basis accidents that fail to consider paths of travel through the security response team's established fields of fire for interrupting adversaries, resulting in the delay or unavailability of operator response to security-initiated events and invalidating safety assumptions and credit for operator actions
- Installation of security delay barriers or dispensable delays (locks, cages, or engineered delays) intended to control accesses that inadvertently reduce the availability of required exits and exit capacity for life safety, resulting in unacceptable increased travel distances and evacuation time or prevents occupants from escaping hazards in the event of a fire or a release of radioactive material due to a nuclear criticality
- Changing plant security procedures to require extensive inspections and searches prior to entry into the PA, without adequate consideration and accommodation for off-site emergency responders and vehicles coming to assist the site's fire brigade in mitigating a hazardous release that could inadvertently result in delays
- Construction for a reactor restart that did not consider additional security measures for controlling access to VA that inadvertently allow bypass of established access control points and results in a defeat of established plant PPS credited for mitigating potential insider threats.
- Installation of security barriers, such as PA PIDAS or delay fencing, that inadvertently prevent fire brigade or offsite firefighter access to hydrants for fire suppression or water spray containment of hazardous chemicals or radiological release in emergencies
- Construction of drainage for site environmental affluent runoffs that inadvertently provides a new pathway for an adversary to bypass the PA PIDAS, defeating PPS and creating a scenario that was not considered or evaluated when developing the site's protective strategy
- Installation of chemical storage tanks adjacent to a security defensive fighting position that inadvertently provides a means for adversaries to tactically defeat or disable security response by causing the release of the hazardous and/or flammable material from the tank
- Establishing a defensive fighting position with a field of fire that inadvertently could result in damage to unprotected SSCs important to safety (e.g., control panel and cables, diesel generators, remote shutdown panel, electrical transformers) from stray bullets fired in order to interrupt or neutralize adversaries
- Installation of temporary movable security barriers that could inadvertently blocks site evacuation routes identified in the site's emergency plan or implementing procedures

2.5 Review of Changes in Plant Areas

Management controls or processes should assess physical and administrative changes to site areas, SSCs, and activities that could affect elements of a licensee's security program, minimizing possible inadvertent degradation of required PPS credited for protection against the DBT and should meet the requirements of 10 CFR 73.55. Licensees may demonstrate protection against the DBT by establishing an effective, reliable, and available PPS, with assurance of reliability and availability, for implementation of the security plans, and maintaining sound and technically defensible bases and assumptions of a site's security protective strategy. Typical PPS at nuclear power plants begins at the owner-controlled area (OCA) to provide a concentric ring or layer of protection that interrupts adversary access or performance of tasks. Therefore, the licensee's established management controls or processes for the safety/security interface should review changes to the characteristics of the site's physical layout (including topographical changes), the configuration of facilities, SSCs, the site's operational procedures, and day-to-day or planned activities that could affect PPS functions and performance established within the OCA, PA, and VA. Where the changes are predominantly security-driven in nature, the review and assessment should address the potential impact to safety functions and performance to prevent inadvertent degradation to the safety of nuclear operations.

2.6 Review of Changes Impacting Physical Protection Systems, Functions, and Performances

Licensees should review the PPS and the elements of detection, delay, and response needed to successfully implement the site's security protective strategy before implementing changes or activities within the OCA, PA, and VA. Licensees should consider the following discussion of PPS functions and measures of effective performance:

- The PPS element of "Detection" typically serves the functions of sensing intrusion, communication of alarms, and alarm assessment. These functions may be carried out by engineered systems or people, or a combination of the two, in the OCA, PA, and VA to detect unauthorized activities. The effectiveness of detection is measured by the capability of exterior or interior detection sensors to sense an intrusion (i.e., detect and alarm), the time required to transmit the alarm to continuously monitored locations, and the time required to assess whether an alarm is valid. Security force patrols may also be used to detect intrusions, particularly in the OCA. Timely assessment by the licensee's security personnel at monitoring locations, security responders (on patrol or at fixed protected locations), or a roving security patrol is a prerequisite for initiating a contingency security response. The licensee's established management controls or processes should provide reviews and assessments of plant changes and activities to identify the potential impact on security SSCs and people credited to perform detection and assessment functions. The overall PPS effectiveness depends on timely assessment. The following specific components of the detection element of the PPS should be included in reviews and assessment of the safety/security interface:

  a. Exterior sensors
  b. Interior sensors
  c. Alarm assessment
  d. Alarm communications
  e. Access control systems

- The PPS element of "Delay" typically serves the functions of slowing down or stopping adversaries by installing barriers, locks, dispensable delays (e.g., sticky foam, cold smoke), and

people (e.g., response force in fixed protected positions). The effectiveness of the delay may be measured by the time required by the adversary to bypass or defeat the licensee's established delays. For example, the effectiveness of delay provided by vehicle barriers may be measured by the capability (including the assurance of reliability and availability) to prevent or stop a vehicle from penetrating beyond the required stand-off distance that protects the SSCs or people critical to the safety or security of the facility from an explosion. To provide assurance of adequate interface for safety and security, the licensee's established management controls or processes should screen and review changes affecting the following delay elements of the PPS:

a. Vehicle barriers (man-made or natural, active and passive)
b. Vehicle access control and channeling barriers
c. Access delay systems
d. Exterior (PA) delay barriers
e. Interior delay barriers (passive and activated or dispensable)

- The PPS element of "Response" typically provides the functions of interrupting or stopping the adversaries. The effectiveness of the response should be measured by the time required to respond to an adversarial attack by deploying a sufficient number of appropriately trained, armed, and protected security responders to interrupt or neutralize the adversary. The timely deployment of the security response force depends on the capability (including reliability and availability of equipment and personnel) to communicate information about an adversary attack after detection. To provide assurance of an adequate safety/security interface, the established management controls or processes should review changes affecting the following elements of the PPS that support the security response:

  a. Security response force communications
  b. Security response force (include response times and response pathways)
  c. Security response equipment and systems (include defensive fighting positions)

2.7 Examples of Physical Protection System Performance

Licensees should consider the following examples of effectiveness for detection, delay, and response elements of the PPS when reviewing and assessing changes:

- Availability of access routes to plant areas and facilities for security contingency response or the evacuation to safety and assembly of site personnel in a security event
- Availability of or access to security equipment or posts (e.g., an armored vehicle, defensive fighting positions) to timely respond to adversarial threats
- Continuity of active and passive (man-made or natural terrain features) vehicle barrier systems and vehicle access controls to delay or prevent unauthorized access by vehicles
- Capabilities of security barriers and access control systems to control personnel access into the PA and VA
- Ability to conduct security patrols for surveillance of PPS integrity or alarm assessment
- Ability to perform searches for contraband (i.e., prohibited or controlled items) at the PA access points
- Availability of lighting to allow observation of isolation zones, visual assessments of alarms, and response

- Availability of detection systems to sense intrusion and transmit alarm signals, including supervision of alarm transmission lines
- Reliability and availability of security cameras to provide surveillance and assessment
- Maintaining lines of sight for required fields of fire from defensive fighting positions
- Capabilities of central and secondary (or other) alarm stations to monitor and communicate alarms and initiate and monitor security response required at all areas of the site, from OCA to VA

2.8 Implementing Management Controls or Processes

Management controls or processes assessing changes may be qualitative, quantitative, or a combination of both, based on the complexity of the proposed changes or planned activity. When a potential adverse interaction is identified, the licensee should resolve the conflicts or competing issues, examine risks and alternatives, and take appropriate corrective or compensatory actions, to provide assurance of safety and security, consistent with the applicable regulations, requirements, and license conditions. Established management controls or processes should provide a means of communicating results to appropriate licensee personnel.

2.9 Screening Questions for Safety

Licensees should use the current change controls and processes for assessing and managing the impact of planned security activities on plant safety activities. For example, licensees established screening questions, representative of 10 CFR 50.59, "Changes, test, and experiments," such as Section 50.59(c)(1)(i) through (viii) and Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Test, and Experiments," (Ref. 5) and other screening of safety and non-security related regulatory requirements, could be applied to meet the objective of identifying potential adverse interactions between security and safety activities.

Specific attention should be given to screen changes effecting emergency plans in accordance with already established screening questions for 10 CFR 50.54(q) to maintain in effect emergency plans which meet the standards in 10 CFR 50.47(b) and the requirements in Appendix E to Part 50. For example, screening questions should identify plant changes that could result in the inability to meet emergency response requirements as outlined in the site's emergency plan or implementing procedures.

2.10 Screening Questions for Security

Licensees should review all operational and physical plant changes against the requirements of the regulations, site security plans, and the bases and assumptions previously evaluated for implementing an effective site protective strategy and licensing basis for security. The following are examples of questions that may be used for the screening of planned activities or changes to identify potential adverse effects on PPS (e.g., systems, equipment, procedures, or people):

- Could the proposed changes decrease the reliability or availability of a security protection systems to perform intended functions previously described or assumed?
- Could the proposed changes increase the likelihood of malfunctions or defeats of security protection system performance or functions previously evaluated?

- Could the proposed changes decrease the capabilities of security equipment or personnel to perform detection (i.e., sensing) functions previously evaluated?
- Could the proposed changes decrease the capabilities of security equipment or personnel to perform alarm communications previously evaluated?
- Could the proposed changes decrease the capabilities of security equipment and/or personnel to assess alarms previously evaluated?
- Could the proposed changes decrease the capabilities of security equipment and personnel to provide delays of adversary less than previously evaluated?
- Could the proposed changes increase response times of security response force (personnel and/or equipment) beyond that previously assumed or evaluated?
- Could the proposed changes decrease the capability of security personnel and/or equipment to neutralize adversaries previously evaluated?
- Could the proposed changes decrease adversary time lines previously evaluated?
- Could the proposed changes increase the likelihood of a different type of adversary sequence (i.e., approaches or attacks) not previously considered?
- Could the proposed changes increase the numbers of, change configurations of, or create new targets set(s) from those previously evaluated?
- Could the proposed changes or as-found condition result in an inadequate security plan or inadequate site protective strategy?
- Could the proposed changes or activities result in noncompliance with NRC's regulations?

The types of questions indicated above are not atypical of what licensees may already have in established controls or processes for assessing and managing security changes.

3. An Acceptable Approach for Implementing 10 CFR 73.55 (n)(2)(ii), Security Program Reviews and Audits

3.1 Frequency of Reviews and Audits

In accordance with 10 CFR 73.55(n)(2)(ii), licensees are required to perform reviews and audits as well as include an evaluation of the effectiveness of management controls or processes established for managing the safety/security interface. Licensees must establish a review/audit in accordance with current requirements of 10 CFR 73.55(g)(4)(i)(A) or (B) and 10 CFR 73, Appendix C, "Licensee Safeguards Contingency Plan." As specified therein, licensees must provide a review/audit by individuals independent of management and personnel who have direct responsibility for implementing management controls or processes on a schedule as follows:

- at an interval not to exceed 12 months, or
- as necessary, based on an assessment by the licensee against performance indicators, and as soon as reasonably practical after changes occur in personnel, procedures, equipment, or facilities that potentially could adversely affect safety/security, but no longer than 12 months after the change.

In all cases, licensees must review each element of safety/security interfaces at least every 24 months.

3.2 Reviews of Implementing Procedures

The licensee should conduct reviews to confirm that procedures established to control any changes to the plant configuration, including emergencies, comply with the licensee's security program. The review and audit should encompass plant operations, modifications, and safety programs, processes, and procedures. The following may be audited: engineering and design, safety analysis, work controls, construction, maintenance, and other activities. The procedures governing these and other activities should include security reviews to identify (1) safety activities or conditions that could affect security, (2) security activities or conditions that could affect safety, and (3) provide a means for resolving conflicting or competing safety and security interests.

3.3 Results of Reviews and Audits

To prevent reoccurrence, the required corrections to specific or programmatic issues should be managed through the site's corrective action program for tracking, communications, and completion.

4. Implementing 10 CFR 73.55 (s) to Manage the Safety/Security Interface

The regulation in 10 CFR 73.55(s) requires that "in accordance with the requirements of §73.58, the licensee shall develop and implement a process to inform and coordinate safety and security activities to ensure that these activities do not adversely affect the capabilities of the security organization to satisfy the requirements of this section, or overall plant safety." The guidance provided for implementing 10 CFR 73.58 addresses this requirement and no additional guidance is needed.

5. Implementing 10 CFR 73, Appendix C, Section II (f)(4), Responsibility Matrix

The regulations in 10 CFR Part 73, Appendix C, Section II (f)(4), requires licensees to "address safety/security interface issues in accordance with the requirements of § 73.58 to ensure activities by the security organization, maintenance, operations, and other onsite entities are coordinated in a manner that precludes conflict during both normal and emergency conditions." The guidance provided for implementing 10 CFR 73.58 addresses this requirement and no additional guidance is needed.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants and licensees regarding the NRC staff's plans for using this draft regulatory guide. Except in those cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the NRC staff will use the methods described in this guide to evaluate the licensee performance and abilities to adequately review, assess, and account for safety/security interfaces in the planning, design, development, and implementation of physical, systems, programs, and/or procedures changes intended to meet the NRC regulatory requirements.

The NRC has issued this draft guide to encourage public participation in its development. Except in those cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the methods to be described in the final guidance, which will reflect public comments, will be used in evaluating (1) submittals in connection with applications for construction permits, standard plant design certifications, operating licenses, early site permits, and combined licenses; and (2) submittals from operating reactor licensees who voluntarily propose or are required to initiate system modifications if there is a clear nexus between the proposed modifications and the subject for which guidance is provided herein.

A backfit analysis was prepared for proposed § 73.58 for which this regulatory guide provides guidance. The NRC has determined that, per 10 CFR 50.109(a)(3), there is a substantial increase in the overall protection of the public health and safety or the common defense and security to be derived from the backfit (associated with proposed § 73.58) and that the direct and indirect costs of implementation are justified in view of this increased protection.

REGULATORY ANALYSIS

The regulatory analysis prepared for the amendment of 10 CFR 73.55 and 73.58 examines the costs and benefits associated with implementing the rule as described in this guide. The regulatory analysis was published by the U.S. Nuclear Regulatory Commission, and is available electronically through the Rulemaking-RuleForum on the NRC's public Web site, at http://www.nrc.gov/about-nrc/regulatory/rulemaking.html. A copy of that regulatory analysis is available for inspection and copying (for a fee) at the NRC's Public Document Room (PDR), which is located at 11555 Rockville Pike (first floor), Rockville, Maryland, 20852. The PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4209, by fax at (301) 415-3548, and by email to PDR@nrc.gov.

REFERENCES

1. 10 CFR 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.[1]

2. 10 CFR 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

3. 10 CFR 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.

4. 71 FR 62664, "Power Reactor Security Requirements," Proposed Rule, *Federal Register*, Vol. 71, No. 207, Part II , October 26, 2006, pp. 62664–62874.[2]

5. Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Test, and Experiments," U.S. Nuclear Regulatory Commission, Washington, DC.[3]

---

[1] All NRC regulations listed herein are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/cfr/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov.

[2] All *Federal Register* notices listed herein were issued by the U.S. Nuclear Regulatory Commission, and are available electronically through the *Federal Register* Main Page of the public GPOAccess Web site, which the U.S. Government Printing Office maintains at http://www.gpoaccess.gov/fr/index.html. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room at 11555 Rockville Pike, Rockville, MD; the PDR's mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; email PDR@nrc.gov.

[3] All regulatory guides listed herein were published by the U.S. Nuclear Regulatory Commission. Most are available electronically through the Public Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/. Active guides may also be purchased from the National Technical Information Service (NTIS) on a standing order basis. Details on this service may be obtained by contacting NTIS at 5285 Port Royal Road, Springfield, Virginia 22161, online at http://www.ntis.gov, by telephone at (800) 553-NTIS (6847) or (703)605-6000, or by fax to (703) 605-6900. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room (PDR), which is located at 11555 Rockville Pike, Rockville, Maryland; the PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4209, by fax at (301) 415-3548, and by email to PDR@nrc.gov.