Department of Energy
Washington, DC 20585

July 31, 2003

The Honorable John T. Conway
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, D.C. 20004

Dear Mr. Chairman:

By letter dated July 14, 2003, you accepted the Department of Energy's Implementation Plan for the Defense Nuclear Facilities Safety Board Recommendation 2002-3, Requirements for the Design, Implementation, and Maintenance of Administrative Controls. Commitment 4.1 of the Implementation Plan is:

"The Office of Nuclear and Facility Safety Policy has reviewed and analyzed existing requirements and guidance and assessed the need for expanded or more focused requirements and guidance. A draft report has been prepared and will be finalized."

The Office of Nuclear and Facility Safety Policy within the Office of the Assistant Secretary of Environment, Safety and Health prepared the final report and it is provided with this transmittal.

If you have any questions, please call me at 301-903-0104.

Sincerely,

Richard L. Black

Richard L. Black, Director
Office of Nuclear and Facility Safety Policy
Environment, Safety and Health

cc:
M. Whitaker

DOE Requirements and Guidance
Use of Administrative Controls for Specific Safety Functions

I. Introduction

DNFSB Recommendation 2002-3 concerns the use at some DOE sites of administrative controls to perform specific safety functions equivalent in importance to safety class and safety significant Structures Systems, and Components (SSCs). (For convenience, these will be referred to in this report as Safety ACs.) The Board has observed that often these administrative controls are not provided an equivalent (to Safety SSCs) level of assurance that they will be effective and reliable to provide their function when called upon and recommended that DOE enhance requirements and guidance in this area. Specifically, the Board recommended that requirements and guidance should address:

a. Specific design attributes to assure effectiveness and reliability;
b. Specific TSRs and limiting conditions of operation;
c. Specific training and qualifications to ensure that the appropriate facility operators, maintenance and engineering personnel, plant management, and other staff properly implement each control;
d. Periodic reverification that each control remains effective, and
e. Root cause and failure analysis, similar to those required upon a failure of an engineered system.

DOE accepted the Board's Recommendation and committed to finalize a preliminary review of existing DOE requirements and guidance applicable to the Safety ACs to determine where consolidation or clarification is needed, as stated in commitment 4.1 of DOE's Implementation Plan for Recommendation 2002-3. This report is the deliverable for that commitment.

Section II of this report describes what was done to assess the current applicable requirements and guidance documents, and also provides conclusions as to their adequacy and the planned actions to resolve inadequacies in the requirements and guidance documents.

Section III contains summarizations that characterize the applicable requirements and guidance in the most directly applicable documents (10 CFR 830 Subpart B Implementation Guides and DOE-STD-3009).

Attachment A contains quoted excerpts from the 10 CFR 830 Subpart B Implementation Guides and from DOE-STD-3009 that support the characterizations in Section III.

Attachment B provides a correlation of a more complete set of applicable existing requirements and guidance for Safety ACs to DNFSB recommendation 1, items a through e, as listed above, which support the conclusions of the assessment of Section II.

II. Assessment

In DOE, rules establish requirements of general applicability. Acceptable methods or approaches to meet the general rule requirements are established in underlying DOE guidance documents. The nuclear safety management rule (10 CFR 830, Subparts A and B), and Implementation Guides (IGs) for Documented Safety Analyses (DSAs) and Technical Safety Requirements (TSRs), DOE G 421.1-2 and DOE G 423.1-1, and DOE-STD-3009 were reviewed to identify requirements and guidance applicable to the Safety AC issue.

Attachment A to this report is a compilation of pertinent excerpts from the guidance documents. Attachment B is a correlation of both the requirements (in the nuclear safety management rule) and DOE Directives and guidance documents to the DNFSB's list of issues that requirements should address for Safety ACs, as stated in the Board's recommendation 1, items (a) through (e). This correlation shows that there are abundant relevant statements of requirements and guidance that are applicable to Safety ACs in the areas the Board recommended to be addressed.

The review indicated that no additional 10 CFR Part 830 QA or Safety Basis Requirements rulemaking is warranted to address the Board's primary concerns. Section III describes the applicable requirements and the bases for this conclusion.

Review of existing guidance in documents such as rule Implementation Guides DOE G 421.1-2 and DOE G 423.1.1 and in DOE-STD-3009 as well as the existing requirements of 10 CFR 830 indicates that the appropriate DOE expectations for the treatment of Safety ACs are included, but are not as explicitly stated or focused as those for Safety SSCs.

The guidance documents and standards referenced as safe harbor methodologies for safety analyses currently in place did not anticipate the utilization of Safety ACs to the extent they have been used. Accordingly, there are not clear and focused statements of DOE expectations for Safety ACs. Commitment 4.2 of the DOE Implementation Plan for Recommendation 2002-3 provides for the development of a Nuclear Safety Technical Position and more formal statements in DOE rule guidance and standards (e.g., a new standard on administrative controls, and additional guidance in DSA and TSR rule Implementation Guides for Safety ACs) to serve as interim guidance to support consistent interpretation, and effective application and implementation of DOE's expectations for Safety ACs.

These more focused versions of rule guidance and the new standard will be developed, and then will be formally incorporated into appropriate DOE Guidance Directives or Technical Standards, with coordinated Program Office review, comment and formal issuance in conjunction with Commitment 4.8. Commitment 4.8 is to review the interim guidance developed for Commitment 4.2 and, based on the comments received and the lessons learned from the implementation reviews by the program and field offices under Commitments 4.5 and 4.6, and develop revisions to DOE standards, rule guidance, and directives, as appropriate.

III. Existing Requirements and Guidance

Requirements

Applicable requirements can be found in 10 CFR 830, Subparts A and B. Specifically, 10 CFR 830.202 requires the establishment of hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment. Title 10 CFR 830.204 requires that a DSA include the derivation of hazard controls necessary to ensure adequate protection from hazards, demonstrate the adequacy of these controls, and define the process for maintaining the hazard controls current at all times and controlling their use.

In 10 CFR 830.3, hazard controls are defined to include TSRs as well as other controls necessary to provide adequate protection from hazards. TSRs are defined to include administrative controls, and administrative controls are defined as the provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of a facility. Title 10 CFR 830.205 requires that TSRs be derived from the documented safety analysis.

These requirements and descriptors are sufficiently broad to cover both safety SSCs and specific operator actions derived from hazard analyses of specific accident scenarios, including Safety ACs.

Additionally, 10 CFR 830, Subpart B, Appendix A provides DOE's expectations for the safety basis requirements and specifies DOE Guide 423.1-1 (TSR Implementation Guide) as the complete description of what technical safety requirements should contain and how they should be developed and maintained.

Title 10 CFR 830, Subpart A also has provisions that are applicable. This subpart is applicable to contractors performing services that affect, or may affect, nuclear safety. The use of administrative controls for accident preventive or mitigative functions qualifies as services that

affect, or may affect nuclear safety. Specifically, 10 CFR 830.122, quality assurance criteria, includes several criteria directly applicable to implementing critical administrative controls in safety basis documents and in operating facilities. Attachment B shows how the criteria are applicable to the DNFSB's list of issues that requirements should address for Safety ACs, as stated in the Board's recommendation 1, sub items (a) through (e).

The DOE nuclear safety management rule requirements in 10 CFR 830 are sufficient at the level of detail intended for the rule (general and high-level).

Guidance

Administrative Controls as addressed in the Documented Safety Analysis Implementation Guide for the rule (DOE G 421.1-2) and the TSR Implementation Guide (DOE G 423.1-1)

These guides encourage design and engineered safety SSCs over administrative controls for safety. However, they further say selection of appropriate controls is a judgment call, and considerations should include: high consequence events preferably should have safety SSCs, while lower consequence events may have administrative controls playing a more prominent role; reliability and effectiveness favor engineered SSCs, but there are attributes such as independent verification, human factor analysis, training, drills, etc. that can increase the reliability and effectiveness of administrative controls. Administrative controls should be considered for defense in depth rather than for primary or redundant controls. Administrative controls necessary to meet specific "safety criteria" need to be described in the hazard analysis and any limiting parameters should be described in the DSA chapter on Derivation of TSRs.

With two exceptions, administrative controls that perform specific safety functions are addressed in the level of detail in the TSR Implementation Guide that the Board's recommendation (items a. through e.) would imply, appropriate to this document. The two areas not addressed are the classification of administrative controls as safety class and safety significant and the development of limiting conditions of operations for administrative controls. The DSA Implementation Guide contains a section that addresses the hierarchy of hazard controls and their selection, but it addresses only SSCs, not administrative controls.

Extracts from the Implementation Guides that are most relevant are included in Attachment A to this paper. Especially relevant material is bolded.

Administrative Controls as addressed in DOE-STD-3009

The guidance in DOE-STD-3009 can be summarized as calling for hazard analysis to define any specific administrative controls necessary to prevent or mitigate accident scenarios and the rationale for them. Most of the discussion of how to handle such controls in a TSR is to the effect that they should not be described in detail; instead, they should be implemented through commitments to the relevant Safety Management Programs when possible. However, any explicit discussion of these controls in a DSA constitutes a commitment to implement them in order to be in compliance with the safety basis.

It can be inferred from the wording that specific controls needed to satisfy safety criteria should be explicitly included in administrative controls in the TSR. This is related to the practice in the field to define so-called "directive action administrative controls."

The most relevant specific guidance for administrative controls that perform a specific safety function is from Chapter 5 (Derivation of TSRs) guidance:

> Derivation of TSRs consists of summaries and references to pertinent sections of the DSA in which design (i.e., SSCs) and administrative features (i.e., non SSCs) are needed to prevent or mitigate the consequences of accidents. Design and administrative features

addressed include ones which: (1) provide significant defense in depth in accordance with TSR screening criteria; (2) provide for significant worker safety; or (3) maintain consequences of facility operations below Evaluation Guidelines. Expected products of this chapter, as applicable based on the graded approach, include: Information with sufficient basis from which to derive TSR administrative controls for specific control features or to specify specific programs necessary to perform institutional safety functions.

And from the Introduction section:

> When TSR administrative controls are used for purposes other than generic coverage of safety management programs, descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why. Beyond safety-significant SSCs designated for worker safety and their associated TSR coverage, additional worker safety issues should be covered in TSRs only by administrative controls on overall safety management programs.

Specific quotes from the Standard that are most relevant are attached at the end of this paper. Especially relevant material is bolded.

Other Relevant Directives

Finally, there are several DOE Directives that relate to aspects of the DNFSB recommendation.

- DOE O 210.1: Performance Indicators and Analysis of Operations Information
  Gather, verify, analyze, trend, and disseminate ES&H performance indicator data, including narrative data, which can help assess performance; where appropriate, perform root cause analyses.
- DOE O 225.1A: Accident Investigations
  Prescribes requirements for conducting investigations of accidents, including root cause and lessons learned to prevent the recurrence of such accidents.
- DOE O 5480.20A: Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities
  Operator training on TSRs and operating procedures.
- DOE Manual 232.1-1A: Occurrence Reporting and Processing of Operations Information
  Reporting of TSR violations
  Reporting of use of inadequate procedures that result in adverse effects on safety.
- DOE O 425.1C (and DOE-STD-3006) Startup and Restart of Nuclear Facilities
  Training, safety basis implementation, adequate procedures in place.

ATTACHMENT A

Specific Relevant Quotes from Guidance Documents (Rule Implementation Guides and DOE-STD-3009)

Note: Particularly relevant material is bolded.

DOE G 421.1-2 (DSA Implementation Guide)

From section 4.1.1:

For the design and construction of a new facility or activity, it is imperative that safety be addressed early so that it can be "designed-in" instead of "added-on." To achieve this integration of safety into design, there needs to be continuous interaction between safety analysts and the designers throughout the design process, as described in DOE O 420.1 and the related Implementation Guides. (See DOE G 420.1-1, DOE G 420.1-2, DOE G 440.1-5, and the criticality design standards ANSI/ANS 8.1, 8.2, 8.3, 8.5, 8.6, 8.7, 8.9, 8.10, 8.12, 8.15, 8.17, 8.19 and 8.21.) All of these hazards (nuclear, explosive, natural phenomena, fire, criticality, etc.) should be addressed as early as possible in the design of new nuclear facilities and major modifications so that passive and active design concepts can be economically incorporated into the design. **DOE encourages the use of design and safety features rather than procedural and administrative controls to address worker and public safety. (See Section 5.2.1)**

From Section 4.3:

DOE line managers, including NNSA line managers, supported by safety professionals, must satisfy themselves that all the hazards associated with a nuclear facility have been identified and appropriate controls have been put in place to prevent accidents and mitigate consequences of accidents associated with those hazards. Generally, it is most effective for DOE reviewers to be engaged and interact with the contractor during the DSA development process so that the reviewers know the safety issues and how they were resolved. **Judgments must be made regarding what constitutes appropriate controls. These judgments should consider the level of the hazard and potential consequences, the practicality and effectiveness of possible control options, the importance of the mission of the facility, and other relevant factors, if any.** These are all elements of the graded approach.

From section 5.2.1.1:

All safety-related controls (criticality related or otherwise) are identified and characterized during the course of the hazards and accident analyses performed in support of the DSA. A subset of all controls will get safety class or safety significant designation, and some of these may be related to control of criticality accidents. Controls that are identified and discussed in CSEs may or may not end up as safety class or safety significant depending on the basis for these designations derived from the hazards analysis and accident analysis in the DSA. **Depending on the situation, criticality derived TSRs would usually be limiting conditions of operation, design features, or administrative controls (approved written procedures).** Procedures are not generally described in detail in a DSA. TSR-level controls should be identified on a case-by-case basis and should be graded according to the guidance in DOE-STD-3009-94, Change Notice No. 1 or successor document with regard to the classification of controls.

From section 5.2.2:

The DSA requirements for a Hazard Category 3 nuclear facility are not as extensive as those for higher hazard facilities. A contractor with a DOE nonreactor, Hazard Category 3 nuclear facility can apply the methods defined in Chapters 2, 3, 4, and 5 of DOE-STD-3009-94, Change Notice

No. 1 or successor document to address the following topics, as applicable, in the DSA and the TSRs (See Table 1):

facility description and operation, including safety SSCs;

process hazards analysis; and

the hazard controls (consisting primarily of inventory limits and safety management programs) and their bases.

For sitewide safety management programs (for example, radiation protection), the DSA should explain the features of those programs that are important to the facility safety basis and can refer to the sitewide program documentation for the details.

DOE G 423.1-1 (TSR Implementation Guide)

From section 2:

Contractors, in the preparation of DSAs, identify how the safety requirements of the Safety Management Rule apply to a specific facility, and describe how the contractor undertakes to design, build, and operate the facility to be in conformance with the applicable statutes, DOE rules and Directives to ensure facility safety. **The analysis of operations and accidents defines the limits of safe operations, identifies the required performance of safety class and safety significant structures systems and components (SSCs), and describes any ACs or procedures that are necessary to meet the specific safety criteria for the facility. These limiting parameters are described in the DSA under "Derivation of Technical Safety Requirements" and provide the principal bases for the TSRs required by 10 CFR 830.205.** The Department reviews the TSRs and decides whether or not to approve the TSRs as part of the nuclear safety basis for the facility. Facility operation is required to be in compliance with the safety basis established and described in the approved DSA and the operating conditions and limitations contained in the TSRs. The TSR document is a controlled document and should be maintained with an authorized users list and is maintained under change control. The users list should be defined in the TSR and should include operations and support personnel, as necessary, and the DOE approval authority.

From section 4:

TSRs define the performance requirements of SSCs and identify the safety management programs used by personnel to ensure safety. TSRs are aimed at confirming the ability of the SSCs and personnel to perform their intended safety functions under normal, abnormal, and accident conditions. These requirements are identified through hazard analysis of the activities to be performed and identification of the potential sources of safety issues. Safety analyses to identify and analyze a set of bounding accidents that take into account all potential causes of releases of radioactivity also contribute to development of TSRs.

From section 4.2:

The DSA required by 10 CFR 830.204 furnishes the technical basis for TSRs. For some facilities, other documentation such as the SER may provide additional safety controls or operating restrictions that should be reflected in the TSRs. **The TSR derivation section in the DSA is intended to provide a link between the safety analysis and the list of variables, systems, components, equipment, and administrative procedures that must be controlled or limited in some way to ensure safety.**

From section 4.7:

DOE must ensure its facilities are operated in a manner that protects workers. Safety significant SSCs can be identified for worker safety, as discussed in DOE-STD-3009-94, Change Notice 1, or successor document. TSRs are intended to ensure the availability of these features. **TSRs can also be established to require the implementation of ACs that have importance to worker safety.**

From section 4.10:

Even after the control parameters for TSRs have been chosen, several levels of TSRs may be selected to control a given parameter. **There is a hierarchy to the selection process, with SLs providing protection against potentially high consequence events and ACs providing protection against lower consequence events and providing for safety management programs.** Guidance for the use of various TSR elements, by facility type, is provided in the following discussion and in Table 4 of the Nuclear Safety Management rule.

From section 4.10.7:

ACs are the provisions relating to organization and management, procedures, record keeping, reviews, and audits necessary to ensure safe operation of the facility. ACs may include reporting deviations from TSRs (i.e., exceeding LCOs, LCSs, or SRs, or violation of a TSR), staffing requirements for facility positions important to safe operation of the facility, ACs of the criticality safety program (see Section 4.13), and commitments to safety management programs important to worker safety.

In general, the ACs should document all those administrative functions that are required to meet facility safety criteria as identified in the DSA, including commitments to safety management programs. It is expected that the ACs will be tailored to the facility activities and the hazards identified in the DSA. This tailoring should be a direct result of the DSA, but it may also result from institutional requirements that address many facilities. **As a general practice, safety controls for individual accident scenarios based on engineered SSCs are preferred to ACs because they are usually more reliable and more predictable.**

The tendency to use ACs as an expedient alternative to an LCO or LCS should be avoided when possible. Efforts should be made to use engineered SSCs whenever possible for controlling the likelihood and consequences of accidents. ACs should be considered for defense in depth rather than the primary or redundant controls. While ACs may be acceptable for ensuring safe operation, their generally lower reliability, compared with engineered controls, should be evaluated carefully when choosing safety measures for long-term hazardous activities.

Human actions, taken either in response to an event or taken proactively to establish desired conditions, are subject to errors of omission or commission. **Sets of ACs are prone to common cause failure. The following attributes, which can be tailored as appropriate, can increase reliability:**

use of reader/worker/checker systems;
independent verification;
positive feedback systems;
human factor analysis;
operator training and certification;
continuing training and requalification;
abnormal event response drills; and
ergonomic considerations in procedures.

When invoking ACs for control of accident scenarios, the preceding attributes, appropriate to the consequences of the accidents they are intended to prevent, should be considered and also invoked.

From section 4.11:

Failure to comply with an AC statement is a TSR violation when either the AC is directly violated, as would be the case with not meeting minimum staffing requirements for example, or the intent of a referenced program is not fulfilled. To qualify as a TSR violation, the failure to meet the intent of the referenced program would need to be significant enough to render the DSA summary invalid.

From section 5.2.4 (Administrative Controls):

This section should impose administrative requirements necessary to control operation of the facility such that it meets the TSR. The paragraphs that follow discuss some of the ACs that should be placed in this section. Where information is provided by reference, the specific ACs relied upon in the safety analyses should be identified and summarized.

1. Contractor Responsibility. The facility or plant manager is responsible for overall operation of the nuclear facility and should delegate in writing the succession to this responsibility during his or her absence. The shift supervisor is responsible for the local command function. During any absence of the shift supervisor from the area, a designated, qualified individual should be assigned the command function.

2. Contractor Organization. On-site and off-site organizations should be described for facility operation and contractor management. The on-site and off-site organizations should be described in terms of the lines of authority, responsibility, and communication for the highest management levels through intermediate levels to and including all operating organization positions. The individuals who train the operating staff and those who carry out health physics and quality assurance functions may report to the appropriate on-site manager; however, they should have sufficient organizational freedom to ensure their independence from operating pressures.

3. **Procedures**. Operations procedures should provide sufficient direction to ensure that the facility is operated within its design basis and supports safe operation of the facility. This should include emergency operating procedures; operating procedures for all phases of operation, maintenance, procedures for all surveillances required by TSR; Security Plan implementation; Emergency Plan implementation; fire protection; procedures for all programs listed in paragraph (4) below; and procedures governing the administrative aspects of operation of the facility. A system should be developed to control all procedures that provide assurance of safe operation. **Procedures that are important to safety need to be identified for special attention to ensure that such procedures are given proper attention in proportion to the hazard that they control and that they are performed reliably (see the discussion in Section 4.10.7).** The system should include the mechanism for review, approval, revision, control, and temporary changes to the procedures. The TSR should include appropriate identification and summary of or reference to the procedures.

4. Programs. Programs developed to ensure the safe operation of the facility should be discussed here and thereby committed to by reference. These programs should include as appropriate but not be limited to in-service inspection of components, pumps, and valves as per ASME Boiler and Pressure Vessel Code Section XI; worker protection such as radiation protection programs; in-plant radiation, process control programs; ventilation filter testing program; explosive gas and storage tank radioactivity monitoring programs; radiological effluent control; quality programs; configuration control programs; and document control. The basic elements of these programs should be described in this section but should be separate controlled volumes and are not to be included in the TSR. The detailed Nuclear Criticality Safety Program may be presented in this subsection of the TSR.

5. Minimum Operations Shift Complement. This section of the ACs should include the maximum daily working hours and maximum number of consecutive days on duty. The required staffing of operating shifts for nonreactor nuclear facilities and the members of the shift staff required to be present in the control room or control area for different operating conditions should be specified in the AC section on the basis of relevant safety analyses.
6. Operating Support. A list of facility support personnel by name, title, and work and home telephone number must be kept up to date. The list should include management, radiation safety, and technical support personnel. The list, itself should not be in the TSR, but should be referenced in the TSR and is required to be readily accessible.
7. Facility Staff Qualifications and Training. Minimum qualifications for members of the facility staff in positions affecting safety should conform to the requirements of DOE 5480.20A or successor document and should be provided in the AC section.
8. Record Keeping. Records need to be kept of all information supporting the implementation of the TSR, including operational logs of modes changes, entering actions, surveillances, deviations, procedures, programs, meetings, recommendations, etc.
9. Reviews and Audits. Describe the methods established to conduct independent reviews and audits. The methods may take a range of forms acceptable to DOE. These may include creating an organizational unit, a standing or ad hoc committee, or assigning individuals capable of conducting these reviews and audits. When an individual performs a review function, a cross-disciplinary review determination is necessary. If deemed necessary, such reviews will be performed by the review personnel of the appropriate discipline. Individual reviewers should not review their own work or work for which they have direct responsibility. Regardless of the method used, management should specify the functions, organizational arrangement, responsibilities, appropriate ANSI/ANS 3.1-1981 qualifications, and reporting requirements of each functional element or unit that contributes to these processes. **Reviews and audits of activities affecting facility safety have two distinct elements. The first of these is the review performed by facility personnel to ensure that day-to-day activities are conducted in a safe manner. The second of these is the review and audit of facility activities and programs affecting nuclear safety that is performed independently of the facility staff. The independent review and audit should provide for the integration of the reviews and audits into a cohesive program to provide senior level facility operation and recommend actions to improve nuclear safety and facility reliability. It should include an assessment of the effectiveness of reviews conducted by facility staff**. Facility staff reviews should include USQ determinations; proposed tests and experiments; procedures; programs; facility changes and modifications; TSR changes; facility operation, maintenance, and testing; DOE and industry issues of safety significance; and any other safety- related items. Reviews by the off-site safety organization should include: USQ determinations; proposed changes to the TSR; violations of codes, orders, and procedures that have safety and health significance; Occurrence Reports; staff performance; unanticipated deficiencies of SSCs that could affect nuclear safety; significant, unplanned radiological or toxic material releases; and significant operating abnormalities. Audits by the off-site safety organization should include conformance with TSR; training and qualification of facility staff; program implementation; deficiency corrective actions; quality program adherence; and other activities of safety significance.
10. Deviations from Technical Safety Requirements. State the actions and reporting to be taken for deviations from TSRs.

DOE-STD-3009 DSA Safe Harbor

Introduction section, Technical Safety Requirements:

When TSR administrative controls are used for purposes other than generic coverage of safety management programs, descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why. Beyond safety-significant SSCs designated for worker safety and their associated TSR coverage, additional worker safety issues

should be covered in TSRs only by administrative controls on overall safety management programs.

Section 3.3.2.3.2, Defense in Depth (under section 3.3.2, Hazard Analysis Results:

Administrative features are typically linked to the overall safety management programs that directly control operations. Administrative features include the following aspects of operator interfaces:

- Procedural restrictions or limits imposed
- Manual monitoring of critical parameters
- Equipment support functions
- Responses or actions counted on to limit abnormal conditions, accident progression, or potential personnel exposure.

If there is a procedural requirement for the operator to perform an action if a parameter is exceeded, it is not necessary to identify the exact procedure, the exact phrasing of the requirement, the specific details of how the operator accomplishes that action, etc. Stating the action, providing a brief summary of its rationale, and noting that both procedures and training needed to cover that action are sufficient.

Safety-Significant SSCs (under section 3.3.2.3.2):

This Standard maintains that all SSCs with a safety function do not require categorization as equipment requiring detailed description in the SAR (i.e., safety-class SSCs and safety-significant SSCs). As noted in the Intoduction, this is one of the principle reasons for the emphasis on programmatic commitments.

TSRs (under section 3.3.2.3.2:

TSRs may also be provided for safety management programs in the form of TSR administrative controls to support adequate defense in depth. Such all encompassing TSRs should be used in lieu of individual TSRs for numerous specific aspects of programs.

Section 3.3.2.3.3, Worker Safety:

This section summarizes the major features protecting workers from the hazards of facility operation, exclusive of standard industrial hazards. Summary products germane to worker safety typically include:

- General overview of worker safety in terms of SSCs and administrative features
- Identification of any safety-significant SSCs
- **Identification of any safety management programs that will be assigned TSR coverage in the form of administrative controls for adequate worker safety.**

The safety features to be addressed in this section fall into one of two categories:

- Structures, systems, and components
- Administrative features.

Categorize administrative features in terms of the programmatic elements covered in later chapters of the SAR. With the exception of safety-significant SSCs, TSR designation is made in the form of administrative controls for overall programs only for worker safety. Typical safety-management programs include criticality protection, radiation protection, hazardous material protection, institutional safety provisions, procedures and training, operational safety, and emergency preparedness. **Specifically note programs that will be provided TSR coverage as administrative controls in Chapter 5, Derivation of Technical Safety Requirements.**

Section 3.4.2.X.5, Summary of Safety-Class SSCs and TSR Controls:

This subsection identifies the safety-class SSCs and assumptions judged to require TSR coverage to meet Evaluation Guidelines. Any TSR assumption not directly related to exceeding Evaluation Guidelines should be defined in section 3.3.2.3.2, Defense in Depth.

Chapter 5, Derivation of Technical Safety Requirements, Purpose and Graded Approach sections:

Derivation of TSRs consists of summaries and references to pertinent sections of the SAR in which design (i.e., SSCs) and administrative features (i.e., non SSCs) are needed to prevent or mitigate the consequences of accidents. Design and administrative features addressed include ones which: (1) provide significant defense in depth in accordance with TSR screening criteria; (2) provide for significant worker safety; or (3) maintain consequences of facility operations below Evaluation Guidelines). Expected products of this chapter, as applicable based on the graded approach, include: Information with sufficient basis from which to derive TSR administrative controls for specific control features or to specify specific programs necessary to perform institutional safety functions.

Section 5.5.X.3, Administrative Controls:

This section is the only applicable section for those features that are provided with only TSR administrative controls. The rationale for assigning TSR administrative controls needs to be clearly and briefly stated.

A special type of TSR administrative control is that covering a safety management program. The administrative controls section of the TSR document will contain commitments to establish, maintain, and implement these programs at the facility and, as appropriate, facility staffing requirements.

Section 6.4.2, Administrative Controls (Criticality):

This section summarizes the administrative controls used to prevent accidental criticality. Include in the discussion the administrative controls on nuclear material safety limits such as mass, moderators, changes in geometry configurations, and procedures for handling, storing, and transporting fissile materials. Discuss also the administrative controls for reviewing and approving changes to process or system configurations.

Chapter 7, Radiation Protection:

This chapter is not intended to be the vehicle for review and approval of the radiation protection program. It is intended to describe the essential features of the program as it relates to facility safety.
Expected products of this chapter, as applicable based on the graded approach include: Description of radiation controls including administrative limits, radiological practices, dosimetry, and respiratory protection.

Section 7.6.1 Administrative Limits:

This section summarize administrative control levels and dose limits, including process for planned special exposures.

Note 1: Chapter 8, Hazardous Material Protection, contains similar wording, including references to administrative control levels and exposure limits.

Note 2: Chapters 6 through 17 are for "Safety Management Programs," as referred to in the previous extracts from Chapters 1 through 5. Other than the explicit mentions of Administrative

Controls and Administrative Limits in the notes above for Chapters 6 through 8, there are no discussions of Administrative Controls.

ATTACHMENT B

Correlation of Existing Requirements and Guidance to DNFSB Recommendation 1, Items (a) Through (e)

a. Specific design attributes to assure effectiveness and reliability

10 CFR 830.122, criterion 6:

1. Design items and processes using sound engineering/scientific principles and appropriate standards.
2. Incorporate applicable requirements and design bases in design work and design changes.
3. Identify and control design interfaces.

10 CFR 830.122 criterion 4:

1. Prepare, review, approve, issue, use, and revise documents to prescribe processes, specific requirements, or establish design.
2. Specify, prepare, review, approve, and maintain records.

DOE G 423.1-1, section 4.10.7:
Human actions, taken either in response to an event or taken proactively to establish desired conditions, are subject to errors of omission or commission. Sets of ACs are prone to common cause failure. The following attributes, which can be tailored as appropriate, can increase reliability:

use of reader/worker/checker systems;
independent verification;
positive feedback systems;
human factor analysis;
operator training and certification;
continuing training and requalification;
abnormal event response drills; and
ergonomic considerations in procedures.

When invoking ACs for control of accident scenarios, the preceding attributes, appropriate to the consequences of the accidents they are intended to prevent, should be considered and also invoked.

b. Specific TSRs and limiting conditions of operation

DOE-STD-3009, Introduction section, Technical Safety Requirements:
When TSR administrative controls are used for purposes other than generic coverage of safety management programs, descriptions should be sufficiently detailed that a basic understanding is provided of what is controlled and why.

DOE-STD-3009, Section 3.3.2.3.2, Defense in Depth (under section 3.3.2, Hazard Analysis Results:
Administrative features are typically linked to the overall safety management programs that directly control operations. Administrative features include the following aspects of operator interfaces:

- Procedural restrictions or limits imposed
- Manual monitoring of critical parameters
- Equipment support functions
- Responses or actions counted on to limit abnormal conditions, accident progression, or potential personnel exposure.

If there is a procedural requirement for the operator to perform an action if a parameter is exceeded, it is not necessary to identify the exact procedure, the exact phrasing of the requirement, the specific details of how the operator accomplishes that action, etc. Stating the action, providing a brief summary of its rationale, and noting that both procedures and training needed to cover that action are sufficient.

DOE-STD-3009, Chapter 5, Derivation of Technical Safety Requirements, Purpose and Graded Approach sections:
Derivation of TSRs consists of summaries and references to pertinent sections of the DSA in which design (i.e., SSCs) and administrative features (i.e., non SSCs) are needed to prevent or mitigate the consequences of accidents. Design and administrative features addressed include ones which: (1) provide significant defense in depth in accordance with TSR screening criteria; (2) provide for significant worker safety; or (3) maintain consequences of facility operations below Evaluation Guidelines). Expected products of this chapter, as applicable based on the graded approach, include: Information with sufficient basis from which to derive TSR administrative controls for specific control features or to specify specific programs necessary to perform institutional safety functions.

DOE-STD-3009, Section 5.5.X.3, Administrative Controls:
This section is the only applicable section for those features that are provided with only TSR administrative controls. The rationale for assigning TSR administrative controls needs to be clearly and briefly stated.

DOE G 423.1-1, Section 2:
The analysis of operations and accidents defines the limits of safe operations, identifies the required performance of safety class and safety significant structures systems and components (SSCs), and describes any ACs or procedures that are necessary to meet the specific safety criteria for the facility. These limiting parameters are described in the DSA under "Derivation of Technical Safety Requirements" and provide the principal bases for the TSRs required by 10 CFR 830.205.

DOE G 423.1-1, Section 4:
TSRs define the performance requirements of SSCs and identify the safety management programs used by personnel to ensure safety. TSRs are aimed at confirming the ability of the SSCs and personnel to perform their intended safety functions under normal, abnormal, and accident conditions. These requirements are identified through hazard analysis of the activities to be performed and identification of the potential sources of safety issues. Safety analyses to identify and analyze a set of bounding accidents that take into account all potential causes of releases of radioactivity also contribute to development of TSRs.

DOE G 423.1-1, Section 4.2:
The DSA required by 10 CFR 830.204 furnishes the technical basis for TSRs. For some facilities, other documentation such as the SER may provide additional safety controls or operating restrictions that should be reflected in the TSRs. The TSR derivation section in the DSA is intended to provide a link between the safety analysis and the list of variables, systems, components, equipment, and administrative procedures that must be controlled or limited in some way to ensure safety.

DOE G 423.1-1, Section 4.10.7:
In general, the ACs should document all those administrative functions that are required to meet facility safety criteria as identified in the DSA, including commitments to safety management programs. It is expected that the ACs will be tailored to the facility activities and the hazards identified in the DSA. This tailoring should be a direct result of the DSA, but it may also result from institutional requirements that address many facilities. As a general practice, safety controls for individual accident scenarios based on engineered SSCs are preferred to ACs because they are usually more reliable and more predictable.

DOE G 423.1-1, Section 5.2.4:
Procedures that are important to safety need to be identified for special attention to ensure that such procedures are given proper attention in proportion to the hazard that they control and that they are performed reliably (see the discussion in Section 4.10.7).

c. Specific training and qualifications to ensure that the appropriate facility operators, maintenance and engineering personnel, plant management, and other staff properly implement each control

10 CFR 830.122 criterion 2:
Train and qualify personnel to be capable of performing their assigned work.

DOE O 5480.20A: Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities
(Operator training on TSRs and operating procedures)

d. Periodic reverification that each control remains effective

Should be handled under TSR provisions. If an LCO is used, either in the LCO section of the TSR or in the AC section, the associated Surveillance Requirement (SR) would be the periodic reverification.

10 CFR 830.122 criterion 3, subitems (1) and (4):
(1) Establish and implement processes to detect and prevent quality problems.
(4) Review item characteristics, processes implementation, and other quality-related information to identify items, services, and processes that need improvement.

10 CFR 830.122 criterion 5, subitems (2) and (3):
(2) Identify and control items to ensure their proper use.
(3) Maintain items to prevent their damage, loss, or deterioration.

e. Root cause and failure analysis, similar to those required upon a failure of an engineered system

10 CFR 830.122 criterion 3, subitems 3
Identify the causes of problems and work to prevent recurrence as a part of correcting the problem.

10 CFR 830.122 criterion 9:
Ensure managers assess their management processes and identify and correct problems that hinder the organization from achieving its objectives.

10 CFR 830.122 criterion 10:
Plan and conduct independent assessments to measure item and service quality, to measure the adequacy of work performance, and to promote improvement.

DOE O 232.1A and DOE M 232.1-1A, Occurrence Reporting and Processing of Operations Information
Requires categorization of occurrences related to nuclear safety; notification of DOE; and development and submission of follow-on reports covering description of event, significance, causal factors, and corrective actions. Events that might qualify related to critical administrative controls might fall under Group 1, Facility Condition (under nuclear criticality safety, fire and explosions, or safety status degradation (TSR violations)); Group 6, Transportation; or Group 9, Nuclear Explosive Safety.

DOE O 225.1A: Accident Investigations

Prescribes requirements for conducting investigations of accidents, including root cause and lessons learned to prevent the recurrence of such accidents.

DOE-NE-STD-1004, Root Cause Analysis Guidance Document
A guide for root cause analysis and causal factors to identify program control deficiencies and guide early corrective actions.