not been paid within sixty calendar days after the assessment has been issued, the DOE shall institute an action in the appropriate District Court of the United States for an order affirming the assessment of the civil penalty.

§ 824.15 Collection of civil penalties.

If any person fails to pay an assessment of a civil penalty after it has become a final order or after the appropriate District Court has entered final judgment for DOE under § 824.14, DOE shall institute an action to recover the amount of such penalty in an appropriate District Court of the United States.

§ 824.16 Direction to NNSA contractors.

(a) Notwithstanding any other provision of this part, the NNSA Administrator, rather than the Director, signs, issues, serves, or takes the following actions that direct NNSA contractors or subcontractors.

(1) Subpoenas;

(2) Orders to compel attendance;

(3) Disclosures of information or documents obtained during an investigation or inspection;

(4) Preliminary notices of violation; and

(5) Final notices of violations.

(b) The Administrator shall act after consideration of the Director's recommendation. If the Administrator disagrees with the Director's recommendation, and the disagreement cannot be resolved by the two officials, the Director may refer the matter to the Deputy Secretary for resolution.

APPENDIX A TO PART 824—GENERAL STATEMENT OF ENFORCEMENT POLICY

I. INTRODUCTION

a. This policy statement sets forth the general framework through which DOE will seek to ensure compliance with its classified information security regulations and rules and classified information security-related compliance orders (hereafter collectively referred to as classified information security requirements).

The policy set forth herein is applicable to violations of classified information security requirements by DOE contractors and their subcontractors (hereafter collectively referred to as DOE contractors). This policy statement is not a regulation and is intended only to provide general guidance to those persons subject to the classified information security requirements. It is not intended to establish a formulaic approach to the initiation and resolution of situations involving noncompliance with these requirements. Rather, DOE intends to consider the particular facts of each noncompliance situation in determining whether enforcement penalties are appropriate and, if so, the appropriate magnitude of those penalties. DOE reserves the option to deviate from this policy statement when appropriate in the circumstances of particular cases.

b. Both the Department of Energy Organization Act, 42 U.S.C. 7101, and the Atomic Energy Act of 1954 (the Act), 42 U.S.C. 2011, require DOE to protect and provide for the common defense and security of the United States in conducting its nuclear activities, and grant DOE broad authority to achieve this goal.

c. The DOE goal in the compliance arena is to enhance and protect the common defense and security at DOE facilities by fostering a culture among both DOE line organizations and contractors that actively seeks to attain and sustain compliance with classified information security requirements. The enforcement program and policy have been developed with the express purpose of achieving a culture of active commitment to security and voluntary compliance. DOE will establish effective administrative processes and incentives for contractors to identify and report noncompliances promptly and openly and to initiate comprehensive corrective actions to resolve both the noncompliances themselves and the program or process deficiencies that led to noncompliance.

d. In the development of the DOE enforcement policy, DOE believes that the reasonable exercise of its enforcement authority can help to reduce the likelihood of serious security incidents. This can be accomplished by providing greater emphasis on a culture of security awareness in existing DOE operations and strong incentives for contractors to identify and correct noncompliance conditions and processes in order to protect classified information of vital significance to this nation. DOE wants to facilitate, encourage, and support contractor initiatives for the prompt identification and correction of problems. These initiatives and activities will be duly considered in exercising enforcement discretion.

e. Section 234B of the Act provides DOE with the authority to impose civil penalties and also with the authority to compromise, modify, or remit civil penalties with or without conditions. In implementing section 234B, DOE will carefully consider the facts of each case of noncompliance and will exercise appropriate judgment in taking any enforcement action. Part of the function of a sound

enforcement program is to assure a proper and continuing level of security vigilance. The reasonable exercise of enforcement authority will be facilitated by the appropriate application of security requirements to nuclear facilities and by promoting and coordinating the proper contractor attitude toward complying with those requirements.

II. PURPOSE

The purpose of the DOE enforcement program is to promote and protect the common defense and security of the United States by:

a. Ensuring compliance by DOE contractors with applicable classified information security requirements.

b. Providing positive incentives for a DOE contractor's:

(1) Timely self-identification of security deficiencies,

(2) Prompt and complete reporting of such deficiencies to DOE,

(3) Root cause analyses of security deficiencies,

(4) Prompt correction of security deficiencies in a manner which precludes recurrence, and

(5) Identification of modifications in practices or facilities that can improve security.

c. Deterring future violations of DOE requirements by a DOE contractor.

d. Encouraging the continuous overall improvement of operations at DOE facilities.

III. STATUTORY AUTHORITY

Section 234B of the Act subjects contractors, and their subcontractors and suppliers, to civil penalties for violations of DOE regulations, rules and orders regarding the safeguarding and security of Restricted Data and other classified information.

IV. PROCEDURAL FRAMEWORK

a. 10 CFR part 824 sets forth the procedures DOE will use in exercising its enforcement authority, including the issuance of notices of violation and the resolution of contested enforcement actions in the event a DOE contractor elects to adjudicate contested issues before an administrative law judge.

b. Pursuant to §824.6, the Director initiates the civil penalty process by issuing a preliminary notice of violation that specifies a proposed civil penalty. The DOE contractor is required to respond in writing to the preliminary notice of violation, either admitting the violation and waiving its right to contest the proposed civil penalty and paying it; admitting the violation, but asserting the existence of mitigating circumstances that warrant either the total or partial remission of the civil penalty; or denying that the violation has occurred and providing the basis for its belief that the preliminary notice of violation is incorrect. After evaluation of the DOE's contractor response, the Director may determine that no violation has occurred; that the violation occurred as alleged in the preliminary notice of violation, but that the proposed civil penalty should be remitted in whole or in part; or that the violation occurred as alleged in the preliminary notice of violation and that the proposed civil penalty is appropriate notwithstanding the asserted mitigating circumstances. In the latter two instances, the Director will issue a final notice of violation or a final notice of violation with proposed civil penalty.

c. An opportunity to challenge a proposed civil penalty either before an administrative law judge or in a United States District Court is provided in 42 U.S.C. 2282a(c). Part 824 sets forth the procedures associated with an administrative hearing, should the contractor opt for that method of challenging the proposed civil penalty.

V. SEVERITY OF VIOLATIONS

a. Violations of classified information security requirements have varying degrees of security significance. Therefore, the relative importance of each violation must be identified as the first step in the enforcement process. Violations of classified information security requirements are categorized in three levels of severity to identify their relative security significance. Notices of violation are issued for noncompliance and propose civil penalties commensurate with the severity level of the violation(s) involved.

b. Severity Level I has been assigned to violations that are the most significant and Severity Level III violations are the least significant. Severity Level I is reserved for violations of classified information security requirements which involve actual or high potential for adverse impact on the national security. Severity Level II violations represent a significant lack of attention or carelessness toward responsibilities of DOE contractors for the protection of classified information which could, if uncorrected, potentially lead to an adverse impact on the national security. Severity Level III violations are less serious, but are of more than minor concern: *i.e.*, if left uncorrected, they could lead to a more serious concern. In some cases, violations may be evaluated in the aggregate and a single severity level assigned for a group of violations.

c. Isolated minor violations of classified information security requirements will not be the subject of formal enforcement action through the issuance of a notice of violation. However, these minor violations will be identified as noncompliances and tracked to assure that appropriate corrective/remedial action is taken to prevent their recurrence, and evaluated to determine if generic or specific problems exist. If circumstances demonstrate that a number of related minor noncompliances have occurred in the same time

frame (*e.g.*, all identified during the same assessment), or that related minor noncompliances have recurred despite prior notice to the DOE contractor and sufficient opportunity to correct the problem, DOE may choose in its discretion to consider the noncompliances in the aggregate as a more serious violation warranting a Severity Level III designation, a notice of violation and a possible civil penalty.

d. The severity level of a violation will depend, in part, on the degree of culpability of the DOE contractor with regard to the violation. Thus, inadvertent or negligent violations will be viewed differently from those in which there is gross negligence, deception or willfulness. In addition to the significance of the underlying violation and level of culpability involved, DOE will also consider the position, training and experience of the person involved in the violation. Thus, for example, a violation may be deemed to be more significant if a senior manager of an organization is involved rather than a foreman or non-supervisory employee. In this regard, while management involvement, direct or indirect, in a violation may lead to an increase in the severity level of a violation and proposed civil penalty, the lack of such involvement will not constitute grounds to reduce the severity level of a violation or mitigate a civil penalty. Allowance of mitigation in such circumstances could encourage lack of management involvement in DOE contractor activities and a decrease in protection of classified information.

e. Other factors which will be considered by DOE in determining the appropriate severity level of a violation are the duration of the violation, the past performance of the DOE contractor in the particular activity area involved, whether the DOE contractor had prior notice of a potential problem, and whether there are multiple examples of the violation in the same time frame rather than an isolated occurrence. The relative weight given to each of these factors in arriving at the appropriate severity level will depend on the circumstances of each case.

f. DOE expects contractors to provide full, complete, timely, and accurate information and reports. Accordingly, the severity level of a violation involving either failure to make a required report or notification to DOE or an untimely report or notification will be based upon the significance of, and the circumstances surrounding, the matter that should have been reported. A contractor will not normally be cited for a failure to report a condition or event unless the contractor was actually aware or should have been aware of the condition or event which it failed to report.

VI. Enforcement Conferences

a. Should DOE determine, after completion of all assessment and investigation activities associated with a potential or alleged violation of classified information security requirements, that there is a reasonable basis to believe that a violation has actually occurred, and the violation may warrant a civil penalty, DOE will normally hold an enforcement conference with the DOE contractor involved prior to taking enforcement action. DOE may also elect to hold an enforcement conference for potential violations which would not ordinarily warrant a civil penalty but which could, if repeated, lead to such action. The purpose of the enforcement conference is to assure the accuracy of the facts upon which the preliminary determination to consider enforcement action is based, discuss the potential or alleged violations, their significance and causes, and the nature of and schedule for the DOE contractor's corrective actions, determine whether there are any aggravating or mitigating circumstances, and obtain other information which will help determine the appropriate enforcement action.

b. DOE contractors will be informed prior to a meeting when that meeting is considered to be an enforcement conference. Such conferences are informal mechanisms for candid pre-decisional discussions regarding potential or alleged violations and will not normally be open to the public. In circumstances for which immediate enforcement action is necessary in the interest of the national security, such action will be taken prior to the enforcement conference, which may still be held after the necessary DOE action has been taken.

VII. Enforcement Letter

a. In cases where DOE has decided not to issue a notice of violation, DOE may send an enforcement letter to the contractor signed by the Director. The enforcement letter is intended to communicate the basis of the decision not to pursue further enforcement action for a noncompliance. The enforcement letter is intended to point contractors to the desired level of security performance. It may be used when the Director concludes the specific noncompliance at issue is not of the level of significance warranted for issuance of a notice of violation. The enforcement letter will typically describe how the contractor handled the circumstances surrounding the noncompliance and address additional areas requiring the contractor's attention and DOE's expectations for corrective action. The enforcement letter notifies the contractor that, when verification is received that corrective actions have been implemented, DOE will close the enforcement action. In the case of NNSA contractors or subcontractors, the enforcement letter will take the form of advising the contractor or subcontractor that the Director has consulted with the NNSA Administrator who

agrees that further enforcement action should not be pursued if verification is received that corrective actions have been implemented by the contractor or subcontractor.

b. In many investigations, an enforcement letter may not be required. When DOE decides that a contractor has appropriately corrected a noncompliance or that the significance of the noncompliance is sufficiently low, it may close out an investigation without such enforcement letter. A closeout of a noncompliance with or without an enforcement letter may only take place after the Director has issued a letter confirming that corrective actions have been completed. In the case of NNSA contractors or subcontractors, the Director's letter will take the form of confirming that corrective actions have been completed and advising that the Director has consulted with the NNSA Administrator who agrees that no enforcement action should be pursued.

VIII. Enforcement Actions

The nature and extent of the enforcement action is intended to reflect the seriousness of the violation involved. For the vast majority of violations for which DOE assigns severity levels as described previously, a notice of violation will be issued, requiring a formal response from the recipient describing the nature of and schedule for corrective actions it intends to take regarding the violation.

1. Notice of Violation

a. A Notice of Violation (preliminary or final) is a document setting forth the conclusion that one or more violations of classified information security requirements have occurred. Such a notice normally requires the recipient to provide a written response which may take one of several positions described in Section IV of this policy statement. In the event that the recipient concedes the occurrence of the violation, it is required to describe corrective steps which have been taken and the results achieved; remedial actions which will be taken to prevent recurrence; and the date by which full compliance will be achieved.

b. DOE will use the notice of violation as the standard method for formalizing the existence of a possible violation and the notice of violation will be issued in conjunction with the proposed imposition of a civil penalty. In certain limited instances, as described in this section, DOE may refrain from the issuance of an otherwise appropriate notice of violation. However, a notice of violation normally will be issued for willful violations, for violations where past corrective actions for similar violations have not been sufficient to prevent recurrence and there are no other mitigating circumstances.

c. DOE contractors are not ordinarily cited for violations resulting from matters not within their control, such as equipment failures that were not avoidable by reasonable quality assurance measures, proper maintenance, or management controls. With regard to the issue of funding, however, DOE does not consider an asserted lack of funding to be a justification for noncompliance with classified information security requirements. Should a contractor believe that a shortage of funding precludes it from achieving compliance with one or more of these requirements, it may request, in writing, an exemption from the requirement(s) in question from the appropriate Secretarial Officer (SO). If no exemption is granted, the contractor, in conjunction with the SO, must take appropriate steps to modify, curtail, suspend or cease the activities which cannot be conducted in compliance with the classified information security requirement(s) in question.

d. DOE expects the contractors which operate its facilities to have the proper management and supervisory systems in place to assure that all activities at DOE facilities, regardless of who performs them, are carried out in compliance with all classified information security requirements. Therefore, contractors normally will be held responsible for the acts or omissions of their employees and subcontractor employees in the conduct of activities at DOE facilities.

2. Civil Penalty

a. A civil penalty is a monetary penalty that may be imposed for violations of applicable classified information security requirements, including compliance orders. Civil penalties are designed to emphasize the need for lasting remedial action, deter future violations, and underscore the importance of DOE contractor self-identification, reporting and correction of violations.

b. Absent mitigating circumstances as described below, or circumstances otherwise warranting the exercise of enforcement discretion by DOE as described in this section, civil penalties will be proposed for Severity Level I and II violations. Civil penalties also will be proposed for Severity Level III violations which are similar to previous violations for which the contractor did not take effective corrective action. "Similar" violations are those which could reasonably have been expected to have been prevented by corrective action for the previous violation. DOE normally considers civil penalties only for similar Severity Level III violations that occur over an extended period of time.

c. DOE will impose different base level civil penalties considering the severity level of the violation(s). Table 1 shows the daily base civil penalties for the various categories of severity levels. However, as described in Section V, the imposition of civil

penalties will also take into account the gravity, circumstances, and extent of the violation or violations and, with respect to the violator, any history of prior similar violations and the degree of culpability and knowledge.

d. Regarding the factor of ability of DOE contractors to pay the civil penalties, it is not DOE's intention that the economic impact of a civil penalty is such that it puts a DOE contractor out of business. Contract termination, rather than civil penalties, is used when the intent is to terminate a contractor's management of a DOE facility. The deterrent effect of civil penalties is best served when the amount of such penalties takes this factor into account. However, DOE will evaluate the relationship of entities affiliated with the contractor (such as parent corporations) when it asserts that it cannot pay the proposed penalty.

e. DOE will review each case involving a proposed civil penalty on its own merit and adjust the base civil penalty values upward or downward appropriately. As indicated in paragraph 2.c of this section, Table 1 identifies the daily base civil penalty values for different severity levels. After considering all relevant circumstances, civil penalties may be escalated or mitigated based upon the adjustment factors described below in this section. In no instance will a civil penalty for any one violation exceed the $110,000 statutory limit per violation. However, it should be noted that if a violation is a continuing one, under the statute, each day the violation continued constitutes a separate violation for purposes of computing the civil penalty. Thus, the per violation cap will not shield a DOE contractor that is or should have been aware of an ongoing violation and has not reported it to DOE and taken corrective action despite an opportunity to do so from liability significantly exceeding $110,000. Further, as described in this section, the duration of a violation will be taken into account in determining the appropriate severity level of the base civil penalty.

TABLE 1—SEVERITY LEVEL BASE CIVIL PENALTIES

Severity level	Base civil penalty amount (percentage of maximum civil penalty per violation per day)
I	100
II	50
III	10

3. Adjustment Factors

a. DOE's enforcement program is not an end in itself, but a means to achieve compliance with classified information security requirements, and civil penalties are not assessed for revenue purposes, but rather to emphasize the importance of compliance and to deter future violations. The single most important goal of the DOE enforcement program is to encourage early identification and reporting of security deficiencies and violations of classified information security requirements by the DOE contractors themselves rather than by DOE, and the prompt correction of any deficiencies and violations so identified. With respect to their own practices and those of their subcontractors, DOE believes that DOE contractors are in the best position to identify and promptly correct noncompliance with classified information security requirements. DOE expects that these contractors should have in place internal compliance programs which will ensure the detection, reporting and prompt correction of security-related problems that may constitute, or lead to, violations of classified information security requirements before, rather than after, DOE has identified such violations. Thus, DOE contractors are expected to be aware of and to address security problems before they are discovered by DOE. Obviously, protection of classified information is enhanced if deficiencies are discovered (and promptly corrected) by the DOE contractor, rather than by DOE, which may not otherwise become aware of a deficiency until later on, during the course of an inspection, performance assessment, or following an incident at the facility. Early identification of classified information security-related problems by DOE contractors can also have the added benefit of allowing information which could prevent such problems at other facilities in the DOE complex to be shared with other appropriate DOE contractors.

b. Pursuant to this enforcement philosophy, DOE will provide substantial incentive for the early self-identification, reporting and prompt correction of problems which constitute, or could lead to, violations of classified information security requirements. Thus, application of the adjustment factors set forth below may result in no civil penalty being assessed for violations that are identified, reported, and promptly and effectively corrected by the DOE contractor.

c. On the other hand, ineffective programs for problem identification and correction are unacceptable. Thus, for example, where a contractor fails to disclose and promptly correct violations of which it was aware or should have been aware, substantial civil penalties are warranted and may be sought, including the assessment of civil penalties for continuing violations on a per day basis.

d. Further, in cases involving factors of willfulness, repeated violations, patterns of systematic violations, flagrant DOE-identified violations or serious breakdown in management controls, DOE intends to apply its full statutory enforcement authority where

such action is warranted. Based on the degree of such factors, DOE may escalate the amount of civil penalties up to the statutory maximum of $110,000 per violation per day for continuing violations.

4. Identification and Reporting

Reduction of up to 50% of the base civil penalty shown in Table 1 may be given when a DOE contractor identifies the violation and promptly reports the violation to the DOE. In weighing this factor, consideration will be given to, among other things, the opportunity available to discover the violation, the ease of discovery and the promptness and completeness of any required report. No consideration will be given to a reduction in penalty if the DOE contractor does not take prompt action to report the problem to DOE upon discovery, or if the immediate actions necessary to restore compliance with classified information security requirements or place the facility or operation in a safe configuration are not taken.

5. Self-Identification and Tracking Systems

a. DOE strongly encourages contractors to self-identify noncompliances with classified information security requirements before the noncompliances lead to a string of similar and potentially more significant events or consequences. When a contractor identifies a noncompliance through its own self-monitoring activity, DOE will normally allow a reduction in the amount of civil penalties, regardless of whether prior opportunities existed for contractors to identify the noncompliance. DOE normally will not allow a reduction in civil penalties for self-identification if DOE intervention was required to induce the contractor to report a noncompliance.

b. Self-identification of a noncompliance is possibly the single most important factor in considering a reduction in the civil penalty amount. Consideration of self-identification is linked to, among other things, whether prior opportunities existed to discover the violation, and if so, the age and number of such opportunities; the extent to which proper contractor controls should have identified or prevented the violation; whether discovery of the violation resulted from a contractor's self-monitoring activity; the extent of DOE involvement in discovering the violation or in prompting the contractor to identify the violation; and the promptness and completeness of any required report. Self-identification is also considered by DOE in deciding whether to pursue an investigation.

6. Self-Disclosing Events

a. DOE expects contractors to demonstrate acceptance of responsibility for security of classified information and to pro-actively identify noncompliance conditions in their programs and processes. In deciding whether to reduce any civil penalty proposed for violations revealed by the occurrence of a self-disclosing event (*e.g.* belated discovery of the disappearance of classified information or material subject to accountability rules), DOE will consider the ease with which a contractor could have discovered the noncompliance, *i.e.* failure to comply with classified information accountability rules, that contributed to the event and the prior opportunities that existed to discover the noncompliance. When the occurrence of an event discloses noncompliances that the contractor could have or should have identified before the event, DOE will not generally allow a reduction in civil penalties for self-identification. If a contractor simply reacts to events that disclose potentially significant consequences or downplays noncompliances which did not result in significant consequences, such contractor actions do not lead to the improvement in protection of classified information contemplated by the Act.

b. The key test is whether the contractor reasonably could have detected any of the underlying noncompliances that contributed to the event. Failure to utilize events and activities to address noncompliances may result in higher civil penalty assessments or a DOE decision not to reduce civil penalty amounts.

7. Corrective Action To Prevent Recurrence

The promptness (or lack thereof) and extent to which the DOE contractor takes corrective action, including actions to identify root causes and prevent recurrence, may result in up to a 50% increase or decrease in the base civil penalty shown in Table 1. For example, very extensive corrective action may result in reducing the proposed civil penalty as much as 50% of the base value shown in Table 1. On the other hand, the civil penalty may be increased as much as 50% of the base value if initiation or corrective action is not prompt or if the corrective action is only minimally acceptable. In weighing this factor, consideration will be given to, among other things, the appropriateness, timeliness and degree of initiative associated with the corrective action. The comprehensiveness of the corrective action will also be considered, taking into account factors such as whether the action is focused narrowly to the specific violation or broadly to the general area of concern.

8. DOE's Contribution to a Violation

There may be circumstances in which a violation of a classified information security requirement results, in part or entirely, from a direction given by DOE personnel to a DOE contractor to either take, or forbear from taking an action at a DOE facility. In such cases, DOE may refrain from issuing a notice

of violation, and may mitigate, either partially or entirely, any proposed civil penalty, provided that the direction upon which the DOE contractor relied is documented in writing, contemporaneously with the direction. It should be emphasized, however, that no interpretation of a classified information security requirement is binding upon DOE unless issued in writing by the General Counsel. Further, as discussed in this section of this policy statement, lack of funding by itself will not be considered as a mitigating factor in enforcement actions.

9. Exercise of Discretion

Because DOE wants to encourage and support DOE contractor initiative for prompt self-identification, reporting and correction of problems, DOE may exercise discretion as follows:

a. In accordance with the previous discussion, DOE may refrain from issuing a civil penalty for a violation which meets all of the following criteria:

(1) The violation is promptly identified and reported to DOE before DOE learns of it;

(2) The violation is not willful or a violation that could reasonably be expected to have been prevented by the DOE contractor's corrective action for a previous violation;

(3) The DOE contractor, upon discovery of the violation, has taken or begun to take prompt and appropriate action to correct the violation; and

(4) The DOE contractor has taken, or has agreed to take, remedial action satisfactory to DOE to preclude recurrence of the violation and the underlying conditions which caused it.

b. DOE may refrain from proposing a civil penalty for a violation involving a past problem that meets all of the following criteria:

(1) It was identified by a DOE contractor as a result of a formal effort such as an annual self assessment that has a defined scope and timetable which is being aggressively implemented and reported;

(2) Comprehensive corrective action has been taken or is well underway within a reasonable time following identification; and

(3) It was not likely to be identified by routine contractor efforts such as normal surveillance or quality assurance activities.

c. DOE will not issue a notice of violation for cases in which the violation discovered by the DOE contractor cannot reasonably be linked to the conduct of that contractor, provided that prompt and appropriate action is taken by the DOE contractor upon identification of the past violation to report to DOE and remedy the problem.

d. DOE may refrain from issuing a notice of violation for an act or omission constituting noncompliance that meets all of the following criteria:

(1) It was promptly identified by the contractor;

(2) It is normally classified at a Severity Level III;

(3) It was promptly reported to DOE;

(4) Prompt and appropriate corrective action will be taken, including measures to prevent recurrence; and

(5) It was not a willful violation or a violation that could reasonably be expected to have been prevented by the DOE contractor's corrective action for a previous violation.

e. DOE may refrain from issuing a notice of violation for an act or omission constituting noncompliance that meets all of the following criteria:

(1) It was an isolated Severity Level III violation identified during an inspection or evaluation conducted by the Office of Independent Oversight, or a DOE security survey, or during some other DOE assessment activity;

(2) The identified noncompliance was properly reported by the contractor upon discovery;

(3) The contractor initiated or completed appropriate assessment and corrective actions within a reasonable period, usually before the termination of the onsite inspection or integrated performance assessment; and

(4) The violation was not willful or one which could reasonably be expected to have been prevented by the DOE contractor's corrective action for a previous violation.

f. In situations where corrective actions have been completed before termination of an inspection or assessment, a formal response from the contractor is not required and the inspection or integrated performance assessment report serves to document the violation and the corrective action. However, in all instances, the contractor is required to report the noncompliance through established reporting mechanisms so the noncompliance issue and any corrective actions can be properly tracked and monitored.

g. If DOE initiates an enforcement action for a violation at a Severity Level II or III and, as part of the corrective action for that violation, the DOE contractor identifies other examples of the violation with the same root cause, DOE may refrain from initiating an additional enforcement action. In determining whether to exercise this discretion, DOE will consider whether the DOE contractor acted reasonably and in a timely manner appropriate to the security significance of the initial violation, the comprehensiveness of the corrective action, whether the matter was reported, and whether the additional violation(s) substantially change the security significance or character of the concern arising out of the initial violation.

h. The preceding paragraphs are solely intended to be examples indicating when enforcement discretion may be exercised to forego the issuance of a civil penalty or, in

some cases, the initiation of any enforcement action at all. However, notwithstanding these examples, a civil penalty may be proposed or notice of violation issued when, in DOE's judgment, such action is warranted on the basis of the circumstances of an individual case.

[70 FR 3607, Jan. 26, 2005, as amended at 71 FR 68733, Nov. 28, 2006; 74 FR 66033, Dec. 14, 2009]

PART 830—NUCLEAR SAFETY MANAGEMENT

Sec.
830.1 Scope.
830.2 Exclusions.
830.3 Definitions.
830.4 General requirements.
830.5 Enforcement.
830.6 Recordkeeping.
830.7 Graded approach.

Subpart A—Quality Assurance Requirements

830.120 Scope.
830.121 Quality Assurance Program (QAP).
830.122 Quality assurance criteria.

Subpart B—Safety Basis Requirements

830.200 Scope.
830.201 Performance of work.
830.202 Safety basis.
830.203 Unreviewed safety question process.
830.204 Documented safety analysis.
830.205 Technical safety requirements.
830.206 Preliminary documented safety analysis.
830.207 DOE approval of safety basis.

APPENDIX A TO SUBPART B OF PART 830—GENERAL STATEMENT OF SAFETY BASIS POLICY

AUTHORITY: 42 U.S.C. 2201; 42 U.S.C. 7101 *et seq.*; and 50 U.S.C. 2401 *et seq.*

SOURCE: 66 FR 1818, Jan. 10, 2001, unless otherwise noted.

§ 830.1 Scope.

This part governs the conduct of DOE contractors, DOE personnel, and other persons conducting activities (including providing items and services) that affect, or may affect, the safety of DOE nuclear facilities.

§ 830.2 Exclusions.

This part does not apply to:

(a) Activities that are regulated through a license by the Nuclear Regulatory Commission (NRC) or a State under an Agreement with the NRC, including activities certified by the NRC under section 1701 of the Atomic Energy Act (Act);

(b) Activities conducted under the authority of the Director, Naval Nuclear Propulsion, pursuant to Executive Order 12344, as set forth in Public Law 106–65;

(c) Transportation activities which are regulated by the Department of Transportation;

(d) Activities conducted under the Nuclear Waste Policy Act of 1982, as amended, and any facility identified under section 202(5) of the Energy Reorganization Act of 1974, as amended; and

(e) Activities related to the launch approval and actual launch of nuclear energy systems into space.

§ 830.3 Definitions.

(a) The following definitions apply to this part:

Administrative controls means the provisions relating to organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility.

Bases appendix means an appendix that describes the basis of the limits and other requirements in technical safety requirements.

Critical assembly means special nuclear devices designed and used to sustain nuclear reactions, which may be subject to frequent core and lattice configuration change and which frequently may be used as mockups of reactor configurations.

Criticality means the condition in which a nuclear fission chain reaction becomes self-sustaining.

Design features means the design features of a nuclear facility specified in the technical safety requirements that, if altered or modified, would have a significant effect on safe operation.

Document means recorded information that describes, specifies, reports, certifies, requires, or provides data or results.

Documented safety analysis means a documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers,