SAFETY AND SECURITY ENFORCEMENT COORDINATOR HANDBOOK

APRIL 2015

Office of Enforcement
Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

Ensure use of the current version of this document by checking the Office of Enterprise Assessments website at: http://energy.gov/ea/services/enforcement/enforcement-program-and-process-guidance-and-information

Acronyms

C.F.R.	Code of Federal Regulations
CSO	Cognizant Security Officer
DART	Days Away, Restricted, or Transferred
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
EA	Office of Enterprise Assessments
EFCOG	Energy Facility Contractors Group
EGS	Enforcement Guidance Supplement
EOC	Extent of Condition
EPO	Enforcement Process Overview
IDLH	Immediately Dangerous to Life and Health
IOSC	Incidents of Security Concern
NNSA	National Nuclear Security Administration
NTS	Noncompliance Tracking System
OGC	Office of General Counsel
ORPS	Occurrence Reporting and Processing System
OSR	Operational Safety Requirement
QA	Quality Assurance
RAM	Radioactive Material
S&S	Safeguards and Security
SSIMS	Safeguards and Security Information Management System
SSC	Structures, Systems, and Components
TSR	Technical Safety Requirement

Definitions

Contractor Assurance System: Encompasses all aspects of the processes and activities designed to identify deficiencies and opportunities for improvement, report deficiencies to the responsible managers, complete corrective actions, and share lessons learned effectively across all aspects of operation.

Compliance Assurance: The set of actions that a contractor should take to ensure that it operates DOE's facilities and conducts work in a manner that complies with applicable requirements.

Director: Refers to the Director of the Office of Enforcement, who is also referred to as the Director of Enforcement.

Enforcement Action: Refers to a Preliminary Notice of Violation, Final Notice of Violation, or Compliance Order; does not refer to a Consent Order, Settlement Agreement, Enforcement Letter, or Special Report Order.

Enforcement Coordinator: A DOE or contractor individual assigned to serve as an organization's principal interface with the Office of Enforcement for issues related to rule implementation, noncompliances, and enforcement proceedings.

Enforcement Outcome: A general term referring to the result of an enforcement evaluation or investigation of an event or condition involving noncompliances.

Enforcement Sanction: A general term referring collectively to Enforcement Actions (see above), Consent Orders, Settlement Agreements, and Special Report Orders.

Noncompliance: A condition that does not meet a DOE regulatory requirement.

Notice of Violation: Either a Preliminary Notice of Violation or a Final Notice of Violation.

Programmatic Problem: Generally involves some weakness in administrative or management controls, or their implementation, to such a degree that a broader management or process control problem exists.

Repetitive Problems: Two or more events or conditions, separated in time, that have comparable causes/circumstances and involve substantially similar work activities, locations, equipment, or individuals, so that it would be reasonable to assume that the contractor's corrective actions for the first occurrence should have prevented the subsequent event/condition.

Violation: A Department of Energy determination that a contractor has failed to comply with an applicable safety or security regulatory requirement.

I. Purpose of Enforcement Coordinator Handbook

The Enforcement Coordinator Handbook is intended to serve as a ready reference and source of guidance for use by U.S. Department of Energy (DOE) and contractor enforcement coordinators to facilitate the day-to-day performance of their regulatory compliance assurance responsibilities. This handbook is a companion document to the Safety and Security Enforcement Process Overview (EPO). It provides detailed information on such topics as Noncompliance Tracking System (NTS) and Safeguards and Security Information Management System (SSIMS) reporting thresholds that are beyond the scope of the EPO document, but nevertheless are key elements for meeting DOE's expectations for effective regulatory compliance assurance. Adherence to the expectations outlined in this document can benefit contractors by providing the Office of Enforcement with a level of confidence in a contractor's compliance assurance processes such that the Office of Enforcement may elect to exercise regulatory discretion and/or mitigate the possible sanctions associated with an enforcement proceeding.

As described in the EPO, the Office of Enforcement, within DOE's independent Office of Enterprise Assessments (EA), implements the safety and security enforcement program in accordance with 10 C.F.R. Part 820, *Procedural Rules for DOE Nuclear Activities*; Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*; and Part 851, *Worker Safety and Health Program*. The requirements that are enforceable under these procedural regulations include 10 C.F.R. Part 830, *Nuclear Safety Management*; Part 835, *Occupational Radiation Protection*; Part 850, *Chronic Beryllium Disease Prevention Program*; Part 851; Part 708, *DOE Contractor Employee Protection Program*; Part 1016, *Safeguarding of Restricted Data*; Part 1045, *Nuclear Classification and Declassification*; Section 820.11, *Information Requirements*, of Part 820; and DOE security directives and National Nuclear Security Administration (NNSA) policies that include language as to their enforceability under Part 824. For a current list of those security directives and policies, see http://energy.gov/ea/enforcement-regulations-and-directives-security.

This handbook is updated periodically based on feedback from DOE and contractor enforcement coordinators and others who have responsibilities for regulatory compliance. The most current version is available from the EA website at http://energy.gov/ea/services/enforcement/enforcement-program-and-process-guidance-and-information.

II. Enforcement Coordinator Roles and Responsibilities

DOE Enforcement Coordinator

A key step in overseeing and improving contractor performance, enhancing compliance with safety and security requirements, and interfacing with the Office of Enforcement is the designation of an enforcement point of contact from each DOE organization. Each DOE organization with responsibility for management or oversight of contractor activities that come under the DOE safety and security rules should identify an enforcement coordinator. The DOE coordinator's roles and responsibilities include:

- Being knowledgeable of safety and security requirements and DOE's enforcement process.
- Maintaining a broad understanding of the activities and operations undertaken by their contractor/site/organization.
- Acting as the focal point to promote effective communications within DOE and with the contractor on DOE regulatory compliance matters.
- Identifying and openly communicating concerns and adverse trends to senior DOE and contractor management.
- Informing the Headquarters Program Office enforcement coordinator and Office of Enforcement before a contract fee reduction or similar contract action is administered because of a safety- or classified information security-related event or issue.
- Ensuring that Federal managers have a working knowledge of DOE's enforcement program and the site's regulatory compliance program.
- Being knowledgeable of reporting thresholds, with a keen sensitivity to identifying programmatic issues, negative trends, and repetitive issues.
- Collecting information or coordinating with personnel to provide information, and collaborating with the Office of Enforcement in evaluating noncompliances reported into NTS and SSIMS.
- Coordinating periodic reviews of noncompliances that the contractor is tracking locally.
- Conducting routine oversight of the contractor's program for identifying, screening, trending, reporting, and correcting noncompliances, and closing noncompliance reports.
- Communicating to the Office of Enforcement any noncompliances that appear to meet the NTS or SSIMS reporting criteria but that the contractor declined to report into those systems.

- Verifying the proper and timely completion of corrective actions (with the assistance of Facility Representatives and subject matter experts) for items reported into NTS and (with the assistance of designated security professionals) compliance-related classified information security items reported into SSIMS.

- Reviewing contractor effectiveness reviews performed for NTS-reported noncompliances and SSIMS-reported classified information security noncompliances, and ensuring appropriate follow-up actions.

- Entering verification/validation results into NTS with clear recommendations for closure.

- Coordinating the Program Office or Field Element's input to the enforcement process (e.g., preliminary investigation discussions, enforcement conferences, and post-conference deliberations) and providing Federal perspective on any proposed enforcement outcome.

- Participating in dialogues between DOE and the contractor in any investigation or regulatory assistance review.

- Maintaining regular communications and sharing lessons learned among the DOE enforcement coordinators within their respective organizations (DOE Program Office or Field Element Coordinator).

- Assisting with resolving requests for investigation submitted directly to the Office of Enforcement.

Contractor Enforcement Coordinator

The contractor enforcement coordinator is pivotal in monitoring and improving safety and security performance. As the primary interface with the Office of Enforcement and the DOE Field Element and Headquarters Program Office enforcement coordinators, and with support from senior management, the coordinator can positively influence his/her organization's attention to and assurance of compliance with requirements. To achieve these benefits, each contractor organization should formally designate a contractor enforcement coordinator. Desired roles and responsibilities include:

- Being knowledgeable of the general safety and security regulatory requirements and the enforcement process. In some organizations, it may be appropriate to designate information security, worker safety and health, and nuclear safety leads to support the enforcement coordinator.

- Maintaining a broad understanding of the activities and operations undertaken by their contractor/organization.

- Serving as the focal point for issues related to safety and security regulatory enforcement implementation and compliance, and championing excellence in the organization's compliance assurance and continuous improvement efforts.

- Through broad awareness of safety and security issues and performance across the organization, identifying and reporting to management areas of weakness or systemic problems not otherwise recognized by the organization.

- Maintaining a "questioning attitude" about worker safety and health, nuclear safety, and classified information security issues.

- Ensuring that contractor managers have a working knowledge of DOE's enforcement program.

- Monitoring contractor compliance assurance program effectiveness and progress in moving toward a culture of critical self-evaluation and continuous improvement.

- Managing or overseeing screening of problems, issues, findings, and conditions to identify noncompliances.

- Ensuring timely screening of a broad set of issues from a variety of sources (e.g., events, performance assessment reports, nonconformance reports, radiological deficiency reports, security assessment reports, incident of security concern reports, inspections, audits, and employee concerns) for potential regulatory noncompliances.

- Being knowledgeable of reporting thresholds, with a keen sensitivity to identifying programmatic issues, negative trends, and repetitive issues.

- Regularly performing, or ensuring regular performance of, assessments to evaluate implementation of the contractor's processes for noncompliance screening and reporting into NTS, SSIMS, and internal systems.

- Ensuring proper and timely reporting of noncompliances into NTS, SSIMS[1], and local tracking systems.

- Ensuring validation of NTS and SSIMS corrective actions prior to closure; verifying that corrective actions address the causes, are comprehensive, and have been completed; and marking NTS and SSIMS reports as "complete" or "closed" (as applicable) only when all actions have been validated.

- Ensuring that effectiveness reviews are conducted for NTS and SSIMS issues when corrective actions have been completed.

- Facilitating coordination of responses to Office of Enforcement requests for information and documents, and scheduling of investigations, inspections, fact-finding visits, and enforcement conferences.

- Serving as the liaison between DOE and the contractor during an enforcement investigation to ensure that the facts and technical issues are fully understood.

[1] Includes mandatory SSIMS reporting in accordance with DOE Order 470.4B, Attachment 5, *Incidents of Security Concern*.

- Maintaining an awareness of enforcement activity and enforcement issues at other sites in the DOE complex, with appropriate follow-up to ensure that similar issues do not exist at the coordinator's own site.

- Regularly informing senior management of compliance issues, safety and security performance issues elsewhere in the DOE complex, and the status of the site's noncompliance screening and reporting program.

III. Noncompliance Reporting Criteria

All noncompliant conditions are expected to be documented, and certain conditions are also expected to be reported to DOE through NTS or SSIMS, consistent with the guidance provided in this section. As discussed in Chapter IV, *Contractor Noncompliance Identification and Reporting*, of the EPO, reporting of worker safety and health and nuclear safety noncompliances into NTS is voluntary; however, the Office of Enforcement views such reporting positively when considering options for an enforcement outcome and possible mitigation of a civil penalty. Reporting to SSIMS is mandatory for certain noncompliant classified information security conditions. Noncompliances that are not reported into either NTS or SSIMS should be tracked in local issues management systems.

NTS reporting thresholds in the worker safety and health and nuclear safety areas are established as shown in Tables III-1 through III-4 on the next several pages. The application of these thresholds is discussed generally in Chapter IV of the EPO and more specifically in the remainder of this document.

Worker Safety and Health Noncompliance Reporting Criteria

Table III-1
Worker Safety and Health Noncompliances Associated With Occurrences
(DOE Order 232.2, *Occurrence Reporting and Processing of Operations Information*)
Consult this Order for the full text of each occurrence criterion.[1]
Notes for Tables III-1 and III-2 are provided after Table III-2.

Reporting Criteria Group	Subgroup	Occurrence Category and Summary Description[2]
1. Operational Emergencies[3]	N/A	(1) Operational Emergency (2) Alert (3) Site Area Emergency (4) General Emergency
2. Personnel Safety and Health	A. Occupational Injuries	(1) Fatality/terminal injury (2) Inpatient hospitalization of $\geq$ 3 personnel (3) Inpatient hospitalization $\geq$ 5 days (4) $\geq$ 3 personnel having Days Away, Restricted, or Transferred (DART) cases (5) Serious occupational injury
	B. Occupational Exposure	(1) Fatality/terminal illness or inpatient hospitalization of $\geq$ 3 personnel (2) Inpatient hospitalization $\geq$ 5 days or $\geq$ 3 personnel having DART cases (3) Personnel exposure > 10X limits or > immediately dangerous to life and health (IDLH) (4) Personnel exposure > limits but < IDLH requiring medical treatment

Reporting Criteria Group	Subgroup	Occurrence Category and Summary Description[2]
		(5) Exposure resulting in serious occupational injury (6) Personnel exposure > limits but < IDLH
	C. Fires	(1) Fire within primary confinement/containment (2) Fire in a nuclear facility (3) Fire in a non-nuclear facility
	D. Explosions	(1) Unplanned explosion within primary confinement/containment (2) Unplanned explosion in a nuclear facility (3) Unplanned explosion in a non-nuclear facility
	E. Hazardous Electrical Energy	(1) Unexpected/unintended personal contact (2) Unexpected discovery of uncontrolled energy source
	F. Hazardous Energy (other than electrical)	(1) Unexpected/unintended personal contact (2) Unexpected discovery of uncontrolled energy source
4. Facility Status	B. Operations	(1) Stop Work Order from DOE
10. Management Concerns/Issues	N/A	(1) Initiation of a Federal Accident Investigation (3) Near miss

Table III-2
Other Worker Safety and Health Conditions Reportable to NTS

Reporting Threshold	Notes[4]
Severity Level I noncompliance(s) with Parts 850 or 851 (Refer to Part 851, Appendix B, *General Statement of Enforcement Policy*, Section VI(b)(1))	Conditions of noncompliance (not otherwise reported into NTS) that are identified by any method or means (e.g., assessments, inspections, observations, employee concerns, event evaluation) that represent a condition or hazard that has the potential to cause death or serious physical harm (injury or illness). These conditions include imminent danger situations.

Reporting Threshold	Notes[4]
Programmatic deficiencies involving noncompliances	Generally involves some weakness in administrative or management controls, or their implementation, to such a degree that a broader management or process control problem exists and requires broad corrective actions.
Repetitive noncompliances	Two or more related noncompliances associated with events/conditions that involve substantially similar work activities, locations, or equipment.
Intentional violation or misrepresentation	Also known as willful noncompliance; may involve record falsification.
Substantiated management reprisal(s) against worker(s) for raising safety issues associated with 851.20(a)(6) or (9)	Customarily referred to as worker retaliation.

Notes for Tables III-1 and III-2

1 The simple occurrence of an event or discovery of a condition in any of the listed categories is not by itself sufficient to warrant NTS reporting. NTS reporting requires the identification of a 10 C.F.R. Part 850 or 851 noncompliance in conjunction with the event or discovery. Contractors identifying a significant worker safety and health noncompliance in association with an event/discovery type or category not listed in the table should evaluate the event for NTS reportability, particularly under the "Severity Level I Noncompliances" category.

2 These summary descriptions are a brief characterization of the related criteria. Use the full statement of the criteria contained in DOE Order 232.2 to determine NTS reportability of occurrence-related worker safety and health noncompliances.

3 Report worker safety and health noncompliances associated with any of the DOE Order 232.2 Operational Emergency categories (Operational Emergency, Alert, Site Area Emergency, General Emergency).

4 Refer to Chapter IV for more information about these types of noncompliances.

Nuclear Safety Noncompliance Reporting Criteria

Table III-3
Nuclear Safety Noncompliances Associated With Occurrences (DOE Order 232.2)
Consult this Order for the full text of each occurrence criterion.[1]
Notes for Tables III-3 and III-4 are provided after Table III-4.

Reporting Criteria Group	Subgroup	Occurrence Category and Summary Description[2]
1. Operational Emergencies[3]	N/A	(1) Operational Emergency (2) Alert (3) Site Area Emergency (4) General Emergency
2. Personnel Safety and Health	C. Fires	(1) Fire within primary confinement/containment (2d) Self-extinguishing fires
	D. Explosions	(1) Unplanned explosion within primary confinement/containment
3. Nuclear Safety Basis	A. Technical Safety Requirement (TSR) Violations	(1) Violation of TSR/Operational Safety Requirement (OSR) Safety Limit (2) Violation of other TSR/OSR requirement (3) Violation of DSA hazard control
	B. Documented Safety Analysis (DSA) Inadequacies	(1) Positive unreviewed safety question
	C. Nuclear Criticality Safety	(1) Criticality accident (2) Loss of all valid criticality controls
4. Facility Status	A. Safety Structure/ System/Component (SSC) Degradation	(1) SSC performance degradation[4]
	B. Operations	(1) Stop Work Order from DOE (2) Actuation of Safety Class SSC (4) Facility evacuation
5. Environmental	A. Releases	(1) Radionuclide release
6. Contamination/ Radiation Control	A. Loss of Control of Radioactive Material (RAM)	(1) Offsite RAM exceeding DOE limits (2) Loss of RAM (>100X limits specified in 10 C.F.R. 835 App. E)
	B. Spread of Radioactive Contamination	(1) Offsite radioactive contamination[5]
	C. Radiation Exposure	(1) Exceedance of DOE dose limits (2) Unmonitored exposure (3) Single exposure > thresholds
	D. Personnel Contamination	(1) Offsite medical assistance (2) Offsite personnel/clothing contamination

Reporting Criteria Group	Subgroup	Occurrence Category and Summary Description[2]
		(3) Onsite personnel/clothing contamination[6]
7. Nuclear Explosive Safety	N/A	(1) Damaged nuclear explosive (2a) Introduction of electrical energy (2b) Safety feature compromise (2c) Inadvertent substitution (2d) Violation of a safety rule
10. Management Concerns/Issues	N/A	(1) Initiation of a Federal Accident Investigation (3) Near miss

Table III-4
Other NTS Nuclear Safety Reportable Conditions

Reporting Threshold	Notes[7]
Programmatic deficiencies involving noncompliances	Generally involves some weakness in administrative or management controls, or their implementation, to such a degree that a broader management or process control problem exists and requires broad corrective actions.
Repetitive noncompliances	Two or more related noncompliances associated with events/conditions that involve substantially similar work activities, locations, equipment, or individuals.
Intentional violation or misrepresentation	Also known as willful noncompliance; may involve record falsification.
Substantiated management reprisal(s) against worker(s) for raising safety issues involving 10 C.F.R. 830/835 noncompliances	Customarily referred to as worker retaliation.[8]

Notes for Tables III-3 and III-4

1 The simple occurrence of an event or discovery of a condition in any of the listed categories is not by itself sufficient to warrant NTS reporting. NTS reporting requires the identification of a 10 C.F.R. Part 830 or 835 (or any other nuclear safety rule) noncompliance in conjunction with the event or discovery. Contractors identifying a significant nuclear safety noncompliance (i.e., one with the potential to cause radiological harm) in association with an event/discovery type or category not listed in the table should evaluate the condition for NTS reportability.

2 These summary descriptions are a brief characterization of the related criteria. Use the full statement of the criteria contained in DOE Order 232.2 to determine NTS reportability of occurrence-related nuclear safety noncompliances.

3 Report nuclear safety noncompliances associated with any of the DOE Order 232.2 Operational Emergency categories (Operational Emergency, Alert, Site Area Emergency, General Emergency).

4 Report noncompliances associated with a degradation of Safety Class SSC preventing satisfactory performance of its design function when required to be operable or in operation.

5 Report noncompliances associated with the offsite spread of contamination where a contamination level exceeds 100 times the applicable value identified in 10 C.F.R. Part 835, Appendix D, *Surface Contamination Values*.

6 Report noncompliances associated with a personnel/personal clothing contamination where a contamination level exceeds 100 times the applicable total contamination value identified in 10 C.F.R. Part 835, Appendix D.

7 Refer to Chapter IV for more information about these types of noncompliances.

8 Worker retaliation as defined in 10 C.F.R. Part 708.

Classified Information Security Noncompliance Reporting Criteria

Noncompliances with classified information security requirements include actions, inactions, or incidents of security concern (IOSC) that have occurred at a site that:

1. Pose threats to the national security
2. Create potentially serious or dangerous classified information security situations
3. Could endanger the health and safety of the workforce or public (excluding safety-related items)
4. Degrade the effectiveness of the safeguards and classified information security programs
5. Adversely impact an organization's ability to protect classified information.

DOE uses a graded approach for identifying and categorizing classified information security noncompliances. This approach provides a structure for reporting timelines and the level of detail for inquiries into, and root cause analysis of, specific classified information security noncompliances.

There are two categories of security incidents, designated A and B, that are based on the relative severity of a security incident and the potential impact on the national security. Classified information security noncompliances are categorized A or B depending on whether the classified matter at risk is determined to be lost or compromised or is suspected of having been compromised. The two significance level categories are then further subdivided into three types based on the type of interest associated with an incident or noncompliance; i.e., security, management, or procedural (see Table III-5 below).

> (NOTE: Security incidents involving the protection and control of classified matter categorized as B require documented evidence to support the determination that no compromise has occurred or the likelihood of potential compromise is remote.)

Table III-5
Classified Information Security Reportable Noncompliances
(DOE Order 470.4B, *Safeguards and Security Program*)

This table identifies reportable noncompliances involving classified information security. Consult DOE Order 470.4B for the full text of each IOSC criterion.

Significance Level Category	
A Category A incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require notification to the DOE/NNSA Cognizant Security Officer (CSO) and the contractor CSO, and reporting in SSIMS.	**B** Category B incidents, which do not meet the Category A criterion, are managed and resolved by the contractor CSO; however, the DOE/NNSA CSO retains his/her oversight responsibility and authority. Monitoring of Category B incidents by the contractor CSO is essential as it allows management to proactively address recurring incidents, thereby minimizing the occurrence of potentially more significant incidents. Category B incidents must be reported in a locally approved system or may be reported in SSIMS.
Incident Type	
Security Interest (SI) This type of incident results in the loss, theft, compromise, or suspected compromise of classified matter.	**Security Interest (SI)** Not applicable to Part 824. Incidents in this significance category/incident type should not involve classified matter.
Management Interest (MI) Not applicable to Part 824. Incidents in this significance category/incident type should not involve classified matter.	**Management Interest (MI)** Not applicable to Part 824. Incidents in this significance category/incident type should not involve classified matter.
Procedural Interest (PI) Not applicable to Part 824. Incidents in this significance category/incident type should not involve classified matter.	**Procedural Interest (PI)** This type of incident is associated with a failure to adhere to security procedures that does not result in the loss, theft, compromise, or suspected compromise of classified matter, and all evidence surrounding the incident suggests the classified matter was not compromised or the likelihood of compromise is remote.

Contractor Tracking of Non-NTS/SSIMS Reportable Noncompliances

For enforcement purposes, reporting a noncompliance that is below an NTS or SSIMS reporting threshold into a contractor's tracking system also constitutes formal reporting to DOE. The Office of Enforcement expects these noncompliances to be tracked and managed to resolution by the contractor's internal issues management or corrective action process. The Office of Enforcement could later choose to take action on these issues if, for example, a regulatory assistance review shows that the contractor is not taking effective action to correct the issue or the issue should have been reported into a DOE tracking system.

Contractors are also expected to use their internal tracking processes to capture, track, and trend nuclear safety, worker safety and health, and classified information security noncompliance conditions. An adequate noncompliance reporting process should, at a minimum:

- In some form, annotate those problems or issues that are noncompliances
- Indicate how the noncompliance was discovered
- Reference the specific Rule section(s) or requirement(s) violated
- Ensure proper resolution (development and completion of corrective actions) of the noncompliance
- Allow retrieval of the noncompliances for review and trending by the contractor and DOE
- Be readily accessible by DOE Field Element and Program Office coordinators, as well as Office of Enforcement staff when on site.

As noted, contractor issue resolution processes should provide a means for trending and evaluating data to identify adverse trends, dominant problems, and potential repetitive problems. The Office of Enforcement has observed that effective screening and reporting processes include provisions for reviewing, trending, and evaluating internally tracked noncompliance conditions.

IV. Contractor Noncompliance Screening and Reporting Guidance

Noncompliance Screening

Contractors' processes for self-identifying problems may identify issues ranging from serious conditions, with corresponding underlying programmatic problems and noncompliances, to relatively minor issues that may need attention but do not represent noncompliances. To determine which are noncompliances and what reporting is appropriate, contractors need to have effective processes for screening issues.

Such screening processes should be under the purview of the contractor's enforcement coordinator, be governed by one or more formal procedures, and receive input from a broad range of noncompliance identification mechanisms. Sources of information to be screened for noncompliances include:

- Internal management and independent assessment findings
- External assessment findings
- Internal issues management or deficiency reporting systems
- Nonconformance reports
- Radiological event or radiological deficiency reports
- Injury reports
- Computerized Accident/Incident Reporting System reports
- Occupational Safety and Health Administration 300 logs
- Occurrence Reporting and Processing System (ORPS) reports
- Operating logs (for issues involved in non-ORPS events)
- Protective force daily event logs
- Security incident notification and inquiry reports
- SSIMS reports
- Security inspection, survey, self-assessment, and special reports
- Employee concerns
- Subcontractor deficiency resolution processes analogous to those listed above.

Reporting a Programmatic or Repetitive Noncompliance

DOE incentivizes the reporting of programmatic and repetitive noncompliances. A programmatic problem is typically discovered through a review of multiple events or conditions with a common cause, but may also be found through causal analysis of a single event. A programmatic problem generally involves some weakness in administrative or management controls, or their implementation, to such a degree that a broader management or process control problem exists. When management determines that a problem or series of events or conditions dictates the need for broad corrective actions to improve management or process controls, this determination indicates that the problem is programmatic. For example, the absence of required worker exposure assessments, or working outside the limits established by radiation work

permits across multiple organizational divisions or facilities, indicates programmatic deficiencies.

Repetitive problems are different events or conditions that involve substantially similar work activities, locations, equipment, or individuals. These problems tend to be narrower in scope than a programmatic problem, and it is reasonable to assume that they should have been prevented by a contractor's corrective actions for a previous noncompliant condition. Repetitive problems typically involve similar circumstances or root causes, separated by a period of time, that suggest the possibility of a common solution.

DOE's expectations for safety and security management and quality improvement dictate that when problems are identified, the potential scope of the problem should be considered. Further, assessment and trending activities should be in place to identify potential programmatic and repetitive problems in a timely manner. Enforcement coordinators' database reviews may provide an additional avenue for identifying programmatic and repetitive noncompliance conditions. Programmatic or repetitive deficiencies identified through such processes are normally placed in a corrective action management process, and should be subject to the screening process to identify any noncompliances.

Reporting a Willful Noncompliance or Misrepresentation

A willful violation refers to a determination that an employee intentionally violated, or was aware of a violation of, a safety or security requirement and attempted to conceal the violation or made no reasonable attempt to eliminate or abate the conditions that gave rise to the violation. DOE expects contractors to report any willful noncompliance involving worker safety and health, nuclear safety, or classified information security regulatory requirements. An intentional or willful noncompliance may involve records that are falsified intentionally, such as indicating that work or surveys occurred in circumstances in which the worker knows that such an activity did not occur. The determination that a record is false provides the basis for categorizing the condition as an intentional noncompliance or misrepresentation that should be reported into NTS or SSIMS, as appropriate. An NTS/SSIMS report is warranted, irrespective of the significance of the activity involving a false record; the act of falsifying the record and providing inaccurate information is serious and warrants significant DOE and contractor management attention.

As another example, an intentional noncompliance may involve a case in which a worker is warned by a co-worker that a certain contemplated action would violate requirements, and then proceeds to take the action anyway. The co-worker's admonition and observation of the action becomes the evidence that the noncompliance was willful. Similarly, an event investigation may reveal that a worker intentionally deviated from or overrode a safety control or security requirement, thereby constituting a willful noncompliance.

The Office of Enforcement expects a matter to be treated as a willful noncompliance and reported into NTS or SSIMS whenever there is evidence of intention or willfulness. The determination of intention requires careful consideration.

A worker's failure to perform a required action, for example, is not necessarily evidence of an intentional disregard of requirements. Such a failure could result from many reasons (e.g., inadequate training, or a lapse in recalling the training) that do not necessarily indicate an intentional disregard of safety or security requirements. A noncompliance should be reported as intentional or willful only if there is supporting evidence that the individual intentionally or negligently falsely reported or otherwise disregarded requirements.

Reporting Worker Retaliation

The Office of Enforcement has established an explicit NTS reporting criterion for reporting retaliation against any worker who raises worker safety and health or nuclear safety concerns.

Enforcement staff have received several inquiries about reporting a worker retaliation. Questions raised include the appropriate time to report; whether noncompliance reporting would serve as an admission and undermine a contractor's defense if the contractor challenges allegations of worker retaliation or an underlying noncompliance; and whether an allegation of reprisal must be filed in accordance with 10 C.F.R. Part 708 or 29 C.F.R. Part 24, *Procedures For The Handling Of Retaliation Complaints Under The Employee Protection Provisions Of Six Environmental Statutes And Section 211 Of The Energy Reorganization Act Of 1974, as amended*, as a condition for asserting that a retaliation occurred.

The Office of Enforcement's general guidance for reporting worker retaliation is as follows:

- The standard NTS reporting expectation – reporting within 20 calendar days of the date of noncompliance determination – also applies to retaliation issues. In such cases, the nuclear safety or worker safety and health linkage is typically clear, and the issue is the point at which the retaliation is "determined." For NTS reporting purposes, "determination" refers to the date when an authoritative body makes an initial decision that retaliation has occurred. The authoritative body can be either the contractor's employee concerns program or similar organization, or an outside organization, such as the DOE Office of Hearings and Appeals or the Department of Labor. Although a contractor may disagree with and challenge or appeal an initial determination, these decisions are authoritative. Forgoing NTS reporting until the appellate process is complete is not considered timely and would preclude potential mitigation for timely reporting if a Notice of Violation is issued.

- The Office of Enforcement recognizes contractor concerns that reporting initial determinations of worker retaliation may undermine the contractor's defense in subsequent appeals. To resolve these concerns, the NTS report can simply acknowledge that such a decision was issued, and may also include information about the contractor's planned path forward.

- A worker need not file a claim under 10 C.F.R. Part 708 or 29 C.F.R. Part 24 for retaliation to have occurred. If a worker raises a retaliation claim to the contractor employee concerns program, which subsequently decides in favor of the employee, then retaliation did occur and would be reportable to NTS. Contractor corrective actions that

provide an appropriate and satisfactory remedy to the worker (e.g., reinstatement) do not affect the existence of the noncompliance, but may be a consideration when evaluating mitigating factors.

NTS and SSIMS Report Content and Closure

For worker safety and health and nuclear safety enforcement purposes, prompt reporting is generally considered to be within 20 calendar days after determining that a noncompliance exists. Some of the noncompliance conditions may be evident when an event occurs, and the NTS report should be filed in a timely manner for those noncompliances.

The initial description of a noncompliance may be limited. DOE does not require or expect contractors to complete a full investigation and causal analysis before reporting a noncompliance or a security incident, nor does DOE pursue a Preliminary Notice of Violation based solely on the initial description of a noncompliance or the initial Security Incident Notification Report. However, DOE expects the contractor to update the NTS/SSIMS report as additional information becomes available.

In general, NTS reports should summarize the noncompliance, along with appropriate information so that Office of Enforcement staff have sufficient information to understand the circumstances of the noncompliance or the events that led to an incident. If there is a corresponding ORPS report, the NTS report may simply refer to the specific ORPS report to enable enforcement staff to locate further details about the event.

For classified information security noncompliances, the contractor must complete a security notification report for an event and a subsequent inquiry report, and enter them into SSIMS. These reports should contain appropriate information so that enforcement staff can understand the circumstances surrounding the incident. Submission of these reports is not required for security self-assessments; however, contractors should consider entering assessment findings into SSIMS.

An NTS or SSIMS report should provide more noncompliance-related information specifically relevant to the noncompliance(s) or circumstances surrounding the event than is covered in the ORPS or initial security incident report. The NTS or SSIMS report should also identify all of the noncompliances associated with the event or condition – not just those that are considered the most significant or that caused an event. Additionally, the NTS and SSIMS reports should state the principal corrective actions needed to address the noncompliance conditions; these may be a subset of or differ from those listed in the ORPS or security incident report. Examples of the level of detail that contractors provide for these reports can be viewed in NTS and SSIMS.

DOE expects NTS and SSIMS reports to be submitted based simply on the established reporting thresholds and security incident significance categorization requirements, as described in the previous chapter. A decision to report should not be based on the contractor's evaluation of safety or security significance, or a prediction of whether the Office of Enforcement would pursue an investigation after receiving the report. However, contractors may include their

preliminary assessment of a noncompliance's significance in the "Description of Noncompliance Condition" portion of an NTS report or in the narrative portion of the SSIMS report.

Contractors are expected to identify and implement as many corrective actions as needed to resolve a noncompliance and provide reasonable assurance that recurrences will be prevented. As discussed in Appendix A, *Contractor Corrective Action Processes and Assessments*, the level of effort the contractor devotes to the investigation and corrective actions should be commensurate with the significance and complexity of the problem – that is, the contractor should apply a graded approach. For example, not every NTS report will require a full root cause analysis or a complete extent-of-condition determination.

The Office of Enforcement expects the corrective action section of an NTS or SSIMS report to include the principal corrective actions related to the noncompliance(s), not just a single corrective action indicating the intent to conduct a causal analysis or develop a corrective action plan. When the corrective actions have been completed and all completion dates entered into NTS or SSIMS, the contractor should mark the report "Completed" or "Closed," as applicable.

At this point, it is essential that the cognizant DOE Field Element validate that the corrective actions were completed effectively. The Field Element enforcement coordinator subsequently indicates in NTS either that the Field Element is satisfied with all corrective actions completed and report closure is recommended, or that a discrepancy remains and further contractor action is needed. After the Field Element indicates that all corrective actions have been completed and verified and recommends report closure, the DOE enforcement coordinator marks the report "Ready for Closure" in NTS; Office of Enforcement staff then review the NTS report closure status and the Field Element recommendation/response. Barring any concerns, the Office of Enforcement closes the report.

For classified information security noncompliances, inquiry officials must verify that corrective actions have been completed and forward a final report to line management and to DOE's Office of Security. The contractor typically closes the inquiry report in SSIMS after the cognizant Program Office concurs with site management's recommendation to do so.

ORPS Occurrence Associated with a Noncompliance

A number of ORPS event categories have significant safety implications, but not all ORPS occurrences involve regulatory noncompliances. Contractors are expected to report into NTS any noncompliances associated with an event or condition that meets any of the ORPS criteria listed in Chapter III and the corresponding notes.

NTS reporting is in the contractor's best interest when a worker safety and health or nuclear safety noncompliance is identified in association with an ORPS-reportable event in the specified categories. NTS reporting is not necessary if the event lacks an associated noncompliance.

Additional Guidance Unique to Worker Safety and Health Enforcement

Multiple Employer Worksite

Many DOE sites have multiple contractors and subcontractors performing work at the same workplace, so managing worker safety and health can be challenging. Title 10 C.F.R. Part 851, Subpart B, *Program Requirements*, and Subpart C, *Specific Program Requirements*, contain comprehensive requirements that each contractor must follow to protect its employees. However, given the complexity of working with other contractors and subcontractors on site, coordination of work planning and execution to ensure worker safety and health is especially important.

When investigating a matter involving risk to workers from multiple contractors, the Office of Enforcement determines the full extent of each contractor's responsibility in exposing employees to hazards. In such cases, the enforcement investigation will include determining which contractor(s): (1) created the hazard; (2) had responsibility for correcting and controlling the hazard; and (3) exposed the employees to the hazard.

To establish the extent of contractor responsibility, enforcement staff review available records and procedures that describe roles and responsibilities, determine whether responsible employees have received appropriate training, and ascertain the actual practices and conditions in the workplace. The Office of Enforcement may cite any contractor found responsible, whether or not the contractor's own employees were exposed to the hazard in question.

Before issuing an enforcement sanction, the Office of Enforcement also considers both mitigating and aggravating circumstances for each contractor involved, in accordance with the enforcement process described in the EPO and this handbook. At a minimum, DOE would expect a contractor whose workers are exposed to a hazard to promptly correct the hazard (if it has the authority to do so) or to remove its workers from the exposure in a timely manner; adequately protect its employees; and promptly notify the responsible contractor to correct the hazard.

General Duty Clause

DOE may pursue an enforcement case against a contractor that fails to provide a place of employment that is free from recognized hazards that are causing, or have the potential to cause, death or serious physical harm to workers, in accordance with 10 C.F.R. Section 851.10(a). The intent of Section 851.10(a) is to parallel the requirements set forth in the Occupational Safety and Health Administration general duty clause, Section 5(a)(1) of the *Williams-Steiger Occupational Safety and Health Act of 1970* (29 U.S.C. 654).

Contractors have a clear obligation to protect workers from death and serious physical harm resulting from recognized workplace hazards, even when:

- There is no existing standard that covers the hazard.

- There is doubt whether a particular standard applies to the hazard.

- A particular safety and health standard is inadequate to protect the contractor's workers against the specific hazard that the standard addresses, and the contractor is aware of the inadequacy.

In such situations, contractors must undertake any feasible actions to eliminate or abate such hazards. If all four of the following questions can be answered in the affirmative, a contractor will be considered to be noncompliant with Section 851.10(a) and may be subject to the issuance of a Notice of Violation, which may include the imposition of a civil penalty:

1. *Are workers being exposed to a hazard?* This means that the hazard exists, workers are exposed to the hazard, and the contractor has failed to remove the hazard. A hazard is defined as a "danger which threatens physical harm to employees." The contractor is not expected to follow any pre-defined abatement method, step, or precaution but to use any and all feasible means to protect employees from the hazard.

   It is also important to attempt to identify, as early as possible, any general workplace hazards that could lead to a condition that creates another hazard or may result in an event. An undetected hazard may become apparent after an event, especially if it results in an injury or fatality. Contractors must be constantly vigilant to detect and correct any existing hazard, as well as any new hazard—for example, those that may result from a change in a process or work practice, or from the use of new or additional equipment.

2. *Is the hazard a recognized hazard?* This means that the contractor knew (or should have known) about the hazard, the hazard is obvious, or the hazard is recognized within the contractor's industry (i.e., it is identified and addressed in a recognized industry consensus standard, or other credible industry guidance or documentation). Contractors should be particularly sensitive to use of a work practice that is contrary to an accepted industry practice or standard, that is contrary to a supplier's standard for use, or that safety experts in the industry acknowledge creates a particular hazard.

   A contractor's recognition of a hazard is also evidenced by the contractor documenting or reporting any injury related to the hazard, as well as by workers calling the contractor's attention to the hazard. Any written or oral statements made by the contractor or a supervisor that relate to the hazard also establish knowledge of the hazard.

   If the hazard is unrecognized within the industry, DOE would still hold a contractor responsible for recognizing and correcting the hazard if DOE concludes that a reasonable person should have recognized the hazard.

3. *Is the hazard causing, or does it have the potential to cause, death or serious physical harm?* If so, the hazard must be classified as Severity Level I or "serious," meaning that there is a potential for serious injury, illness, or death if the hazard is not eliminated or controlled. Potential effects can include any acute or chronic impairment of the body that affects life functioning on or off the job (usually requiring treatment by a medical

doctor), whether temporary or permanent. They also include illnesses that significantly reduce physical or mental efficiency (e.g., occupational asthma).

4. *Do feasible and useful methods exist to correct the hazard?* The hazard must be correctable, i.e., there must be a known, feasible way for the employer to correct, eliminate, or at least significantly reduce the hazard, either by applying an appropriate control or having workers use adequate personal protective equipment.

Coordinating Application of Civil Penalty and Contract Fee Reduction

Title 10 C.F.R. Section 851.5, *Enforcement*, states that contractors indemnified under the Atomic Energy Act are subject to either civil or contract penalties, but not both, for worker safety and health violations.[1] Most DOE contractors are indemnified under Section 170d of the Atomic Energy Act. Those that are not indemnified are subject to the contract remedy provisions of the Rule. The DOE Acquisition Regulation clause at 48 C.F.R. 923.7002, *Worker Safety and Health*, requires the cognizant DOE contracting officer to coordinate with the Office of Enforcement before pursuing a contract fee reduction in the event of a violation by the contractor of any Departmental regulation relating to worker safety and health. To provide for adequate coordination, the Office of Enforcement has built certain steps into its enforcement process (see EPO Chapter VI, *Investigation Process*) to ensure that DOE Program Office and Field Element perspectives are considered throughout the enforcement process, including the impact of any contract actions relating to an enforcement case under consideration.

Offsite Support for Emergencies

Part 851 applies to services provided under contract to DOE on a DOE site. In some cases, the Office of Enforcement may determine that Part 851 applies to emergency response support. In any evaluation for potential enforcement, the following points will be of primary consideration:

- Whether the agreement for services is a contractual relationship and thus falls within the scope of the Rule

- Where the activities took place.

Contractors are expected to conduct appropriate baseline needs assessments to ensure that Part 851 program requirements are addressed. Except for unusual or egregious deficiencies, the Office of Enforcement generally exercises discretion in evaluating noncompliances occurring during an emergency or event response involving offsite municipal fire-fighting or emergency response agencies, even when contractual relationships bring them under the scope of Part 851. Enforcement normally focuses on the operating or management/integrating contractor in

[1] Parts 820 and 824 do not specifically allow or prohibit both a contract fee reduction and civil penalty for the same violations. However, for purposes of consistent enforcement program implementation, the Office of Enforcement will consider reducing or forgoing a civil penalty for Preliminary Notices of Violation issued under Parts 820 and 824 when a fee reduction is levied for and clearly linked to an event and noncompliances that are the subject of the enforcement action. See Chapter VI, *Enforcement Outcomes*, of the EPO.

evaluating whether applicable program requirements are met. As in any potential enforcement situation, the Office of Enforcement will evaluate the situation based on its specific merits.

Additional Guidance Unique to Nuclear Safety Enforcement

To better support and describe implementation of the Department's nuclear safety enforcement program, over the years the Office of Enforcement has developed guidance (in the form of Enforcement Guidance Supplements, or EGSs) to address emerging situations or specific questions relating to enforcement. Where appropriate, the information contained in those EGSs has been incorporated into the body of the EPO or this handbook. However, the following EGSs are still viewed as containing relevant information, but deal with topics or situations too specific for inclusion in this general guide.

- **EGS 99-01**: Enforcement of 10 C.F.R. Section 830.120 (Quality Assurance Rule) for Facilities Below Hazard Category III (07/01/99)
- **EGS 99-02**: DOE Enforcement Activities of Internal Dosimetry Program Requirements (07/16/1999)
- **EGS 00-01**: Enforcement Position Relative to the Discovery/Control of Legacy Contamination (05/04/2000)
- **EGS 00-03**: Specific Issues on Applicability of 10 C.F.R. Part 830 (09/12/2000)
- **EGS 01-01**: Nuclear Weapons Program Enforcement Issues (10/15/2001)

The above EGSs are available at http://energy.gov/ea/enforcement-regulations-and-directives-nuclear-safety.

Additional Guidance Unique to Classified Information Security Enforcement

One of the goals of the Department's classified information security enforcement program is to encourage contractors to develop self-assessment processes that can identify security noncompliances. Contractors should report self-identified security deficiencies and provide the status of corrective actions to the Office of Security Enforcement. Contractors may report self-identified classified information security noncompliances in SSIMS. This voluntary reporting is in addition to the mandatory security incident reporting requirements of DOE Order 470.4B, Attachment 5, *Incidents of Security Concern*.

SSIMS Background and Reporting

For security enforcement purposes, SSIMS is the means for contractors to promptly identify and report certain classified information security noncompliances to DOE, including events and self-assessment results, as well as the resulting corrective actions. Event reporting timeframes are

based on security significance and are identified in DOE Order 470.4B, Attachment 5. In event cases, additional noncompliances that led to the event may not be identified until the root cause analysis and preliminary inquiry have been completed; these are identified in the inquiry report.

The Office of Security Enforcement recommends that contractor organizations, in coordination with the enforcement coordinator, review the results of any self-assessments or other internal reviews and trending data for classified information security deficiencies. Any identified noncompliances should be reported into SSIMS under the "SA" (self-assessment) survey type in the SSIMS survey screens, along with associated corrective actions developed from the causal/root cause analysis.

To ensure consistent contractor reporting of security noncompliances, the Office of Security Enforcement has developed the following list of thresholds:

- **Programmatic Noncompliance:** Programmatic issues are typically discovered through a review of multiple events or conditions with a common cause; however, they may also be identified through a causal analysis or a single security event/incident. Programmatic issues usually involve weaknesses in administrative or management controls (i.e., security plans, standard operating procedures, physical security configuration) or the implementation of those controls. Additionally, when management determines that conditions require broad corrective actions to improve management or process controls, this determination indicates that the problem is programmatic.

- **Repetitive Noncompliance:** Generally, repetitive noncompliances involve two or more different security deficiencies that include substantially similar conditions, locations, organizations, programs, classification levels, classified information/matter, or individual(s). It is reasonable to assume that the contractor's corrective actions for a previous noncompliance should have appropriately averted the deficiencies.

- **Intentional/Willful Noncompliance or Misrepresentation:** An intentional/willful noncompliance or misrepresentation may involve inventory records or inventory results that are falsified intentionally. A noncompliance should be reported as intentional or willful only if there is supporting evidence that the individual intentionally or negligently falsely reported, or otherwise disregarded, classified information security requirements.

The finding comments section of the SSIMS report should reflect the specific noncompliance threshold, along with a description of the self-identified security concern.

Other Guidance

Applicability of Enforceable Requirements to Strategic Partnership Projects (formerly known as Work for Others)

Questions have been raised as to whether enforcement would apply to safety or classified information security issues that involve workers performing strategic partnership project work or work for others using DOE facilities (see DOE Order 481.1C, *Strategic Partnerships Projects*

(formerly known as Work for Others (Non-Department of Energy Funded Work)). With respect to 10 C.F.R. Part 851, DOE's Office of General Counsel (OGC) has developed guidance on applying Part 851 to work for others, as well as general guidance on the issues of who is a DOE contractor and what work is in furtherance of a DOE mission. This OGC guidance has been incorporated into DOE Guide 440.1-1B, *Worker Safety and Health Program for DOE (Including the National Nuclear Security Administration) Federal and Contractor Employees*, which is available through the DOE directives website at: https://www.directives.doe.gov/.

Similarly, because strategic partnership project / work for others activities are performed by DOE contractors under their existing contracts with DOE, these activities are also subject to the enforcement provisions of 10 C.F.R. Parts 820 and 824 for noncompliances involving DOE nuclear safety or classified information security regulatory requirements.

Common Deficiencies in Contractor Screening Processes

Historically, the Office of Enforcement has observed a number of common weaknesses or errors in contractors' processes for screening information for potential noncompliance conditions. Although contractors should structure their processes to meet all of the objectives and guidance in this chapter, the following common weaknesses or errors should be considered as lessons learned that warrant particular management attention:

- Failure to consider all appropriate sources for screening (e.g., assessment reports, employee concerns, subcontractor events or deficiencies)
- Screening out issues because they were corrected promptly
- Screening out issues that are noncompliant with requirements, but are judged to be of low significance
- Establishing criteria that are not stipulated in the safety and security regulations, with the effect of limiting the applicability of the regulations; for example, treating as noncompliances *only* matters covered specifically in the safety basis, or *only* violations of work controls for work involving direct handling of nuclear material, or *only* violations of procedures specifically listed in Rule-required program plans.

Appendix A

Contractor Corrective Action Processes and Assessments

This appendix provides supplemental information about contractor compliance assurance and corrective action processes. It complements the Enforcement Process Overview and Enforcement Coordinator Handbook by providing additional details on these processes, and particularly by identifying areas in which the Office of Enforcement has observed programmatic weaknesses, which can be useful in reviewing quality assurance (QA) activities and the effectiveness of contractor corrective actions. The information may also be useful in understanding how mitigation is assessed during enforcement activities.

As part of the investigation of potential noncompliances in nuclear safety, worker safety and health, or classified information security, the Office of Enforcement routinely reviews contractors' investigations of events and noncompliances, preliminary inquiry reports, and associated causal analyses, and the corrective actions developed to resolve the noncompliances and prevent recurrence. During these reviews, the Office of Enforcement has noted several common deficiencies. Additionally, an enforcement case is typically pursued for recurrent events or deficiencies, which indicate weaknesses in contractor processes for developing, implementing, or sustaining effective corrective actions. The Office of Enforcement provides this information as potential lessons learned for the DOE contractor community.

Investigation, Causal Analysis, and Corrective Action Processes

Relevant Requirements and Regulatory Drivers

Specifically for nuclear safety, 10 C.F.R. Section 830.122(c), *Criterion 3 – Management/Quality Improvement*, establishes DOE requirements for investigating identified nuclear safety deficiencies, determining underlying causes, and developing and implementing effective corrective actions to correct the deficiencies and prevent recurrence. Additionally, Part 820, Appendix A, *General Statement of Enforcement Policy*, delineates incentives for contractors' timely and comprehensive corrective actions for noncompliances, including the application of regulatory discretion and/or penalty mitigation if the outcome is a Notice of Violation.

Although the worker safety and health and classified information security rules do not mandate a quality improvement process, the enforcement provisions of Parts 824 and 851, and their accompanying enforcement policy statements (Appendix A to Part 824 and Appendix B to Part 851), establish incentives for crediting contractors' timely and comprehensive investigative and corrective actions as one of the factors in applying enforcement discretion and possible mitigation.

When the Office of Enforcement's investigation activities identify deficiencies that the contractor should have self-identified and corrected, or that were previously identified by another entity and not corrected, or represent recurring problems or repetitive events, the office cannot make a favorable judgment regarding compliance with the QA Rule requirements or discretion

or mitigation as delineated in the enforcement policies referenced above. It is hoped that contractors will evaluate and improve their processes in these areas and avoid these types of deficiencies.

General Principles

The Office of Enforcement generally expects a contractor conducting an investigation/causal analysis to ensure that (1) the personnel who conduct the investigation are sufficiently independent of involvement in the event and adequately trained and qualified; (2) the investigation includes appropriate scope and depth; and (3) the corrective actions are timely and clearly relate to the identified causes. The level of effort devoted to the contractor investigation and corrective actions should be commensurate with the significance and complexity of the problem—that is, a graded approach should be applied that is consistent with the causal analysis criteria delineated in the DOE Order for occurrence reporting (DOE Order 232.2). For example, identification of apparent causes may be an appropriate endpoint when investigating less significant problems, while a root cause analysis would be appropriate for more significant or complex issues.

Scope of Investigation

After a deficiency or quality problem has been identified, the contractor must fully evaluate and characterize it so that it can be corrected. As part of its review of a contractor's investigation of a worker safety and health, nuclear safety, or security problem, the Office of Enforcement typically questions whether the investigation included the following elements:

- Extent-of-condition (EOC) review
- Precursor or historical review (including the effectiveness of prior corrective actions)
- Evaluation of assessment performance.

1. EOC Review

After a significant safety or security problem has been identified, the contractor should perform an EOC review to determine the full extent and generic implications of the problem—for example, determining whether the same problem/condition exists elsewhere (transportability of condition) and whether the same root or underlying causes of the problem/condition may be affecting performance in other applications (transportability of cause). Effective EOC reviews may address many areas, depending on the specifics of the identified problem, but they generally include:

- Looking for the same problem in applications, locations, or facilities other than where originally found

- Looking for other manifestations of the identified root cause or underlying causes of the problem (sometimes referred to as extent-of-cause)

- Looking for similar or related problems or problems that can be expected, based on the identified problem

- Reviewing prior applications of the deficient process or procedure to see whether earlier deficiencies might have gone unnoticed.

The approach to conducting an EOC review may also vary with the details and significance of the identified problem (i.e., a graded approach). Typically, an EOC review includes a series of focused field observations or assessments in conjunction with document reviews; a simple review of site trending data or issue tracking systems rarely provides the information needed to adequately assess the scope of the problem.

The most common performance deficiency in EOC conduct is the simple failure to perform an EOC review when identified deficiencies are indicative of a programmatic deficiency or otherwise have a clear potential for general applicability. In addition, contractors sometimes simply search event databases for similar prior events or for general negative performance trends, and call such searches EOC reviews. Although the Office of Enforcement understands that database reviews have value (e.g., as a precursor/historical review), they do not constitute an effective EOC review. Inappropriate use of this terminology and approach may give senior management false confidence that an identified problem is limited in scope.

2. Precursor/Historical Review

A contractor's investigation and analysis of an identified quality problem should include a review to determine whether the same or a similar problem has occurred previously. This determination addresses both the problem condition and the underlying causes to determine whether the problem is recurrent. If a problem is found to be recurrent, the contractor's analysis should determine why prior corrective actions were not effective in preventing recurrence. The results of that evaluation should be factored into the corrective actions for the current event or problem. Unlike an EOC review, a precursor or historical review is retrospective in nature and can usually be conducted effectively using site database information for such items as events and assessment results.

3. Evaluation of Assessment Performance

When evaluating an event or condition for possible investigation and when conducting investigation and assistance activities, the Office of Enforcement consistently focuses on the implementation and effectiveness of contractors' assessment programs in improving safety and security performance. Experience indicates that self-identification of issues through implementation of an effective internal assessment program (rather than by reacting to events) is a cost-effective way to improve performance in worker safety and health, nuclear safety, and classified information security.

Consequently, when conducting an investigation, the Office of Enforcement typically evaluates whether the subject safety or security noncompliance should have reasonably been identified through the contractor's assessment program. Based on an initial determination, follow-up

questions can help identify deficiencies in assessment topic selection and scope, scheduling, method of conduct, or implementation quality. The effectiveness of tools for tracking and trending deficiencies may also be evaluated, along with corrective action development processes and procedures for independent validation of the effectiveness of the corrective actions. The Office of Enforcement recommends that, where appropriate, contractors perform a similar evaluation as part of their investigation of an event or other worker safety and health, nuclear safety, or classified information security problem.

Causal Analysis

An effective causal analysis is essential in developing appropriate corrective actions for an identified safety or security problem.

1. Depth of Analysis

The depth of the contractor's causal analysis should reflect the significance and complexity of the noncompliance/incident of security concern or event under analysis. Some problems may be easily understood, while others may require considerable in-depth analysis.

Based on review of a large number of contractor causal analyses, the Office of Enforcement considers the most frequent deficiency in this area to be the tendency to truncate analyses before getting to the underlying issues; that is, the analyses do not go "deep" enough. In particular, the Office of Enforcement has found that contractors often end their analyses at some failure condition (e.g., failure to follow procedures, inadequate training, inadequate administrative controls) and then identify that condition as the root or underlying cause. Although convenient for binning and trending purposes, these failure conditions do not always represent satisfactory endpoints. A more detailed causal analysis should go further and ask, for example, why the procedure was not followed, why the training was inadequate, or why there was an inadequate administrative control.

2. Cultural/Organizational Factors

"Worker failure to follow procedures" is often cited as an underlying cause, with corrective actions focusing on retraining or disciplining the worker, or revising the procedure or process. Although such actions may be appropriate in some cases, contractors should also investigate whether organizational and management issues contributed to the failure. The cultural or organizational factors that may underlie worker procedural compliance issues may include:

- Perceived differences in management's actions versus their words
- Local supervisory influences contrary to management's stated expectations
- Emphasis on production or schedule
- Inconsistent application of standards across the institution
- Longstanding organizational practices conflicting with procedures and becoming the default process
- Examples set by fellow workers
- Desire for a successful experiment or evolution.

A comprehensive investigation of a safety problem or incident of security concern should attempt to identify all of the particular influences that caused the problem, including the management or supervisory influences that affect workers' behavior. These underlying factors may be difficult to identify or "get to" in an investigation and may require a senior-level effort, special expertise, or a number of one-on-one interviews.

3. Breadth of Analysis

The Office of Enforcement has also noted that some causal analyses do not identify all significant issues associated with an event. For example, the Office of Enforcement is just as interested in the reasons why a longstanding noncompliance persisted without being identified or corrected, as in the specific causes of the original noncompliance. Often, causal analyses do not address such questions, but tend to focus on the specific failure condition.

Corrective Actions

The Office of Enforcement evaluates contractor corrective action plans as part of the routine review of Noncompliance Tracking System (NTS) and Safeguards and Security Information Management System reports and as part of an enforcement investigation. The Office of Enforcement uses the general criteria outlined below to evaluate corrective actions, and also relies on the judgment of the cognizant DOE Program Office and Field Element representatives when evaluating the adequacy of contractor corrective actions:

- Clear linkage to the causal analysis – identifying whether the contractor has developed corrective actions for all root and significant contributing/underlying causes identified through the causal analysis process.

- Appropriateness of corrective actions – verifying that stated corrective actions make sense and appear appropriate for the problem being addressed (e.g., behavioral or cultural issues are not being addressed by a procedure revision) and that deliverables are clearly stated and achievable.

- Timeliness of corrective actions – verifying that schedules for corrective action completion reflect an appropriate priority and do not extend past a reasonable timeframe. The Office of Enforcement expects that any delays in corrective action completion will be justified by the contractor and limited in number and extent.

- Verification of effectiveness – determining whether the contractor included a verification of effectiveness (described below) as a planned corrective action for significant or complex safety or security problems.

Many contractors conduct "effectiveness reviews" as a corrective action for significant issues. These reviews, typically performed several months after the other corrective actions are completed, are intended to assess workplace performance in the subject area and to determine whether the corrective actions have been effective. Effectiveness reviews can also be performed as an element of the independent assessment process.

The Office of Enforcement views the practice of conducting an effectiveness review as a positive one that should reduce the incidence of recurrent events. For noncompliances reported into NTS, the contractor may either list the planned effectiveness review as one of the NTS report's formal corrective actions (which may involve keeping the NTS report open for a longer period of time) or track it separately. Implementing an effectiveness review approach does not alter the Office of Enforcement's expectation that the contractor and local DOE personnel will verify the completion of corrective actions before recommending closure of an NTS report.

The results of a contractor's effectiveness review for an NTS-reported noncompliance may require supplemental NTS reporting. If the review concludes that corrective actions have been ineffective in resolving the noncompliance, then the contractor should either update the existing NTS report (if still open) or submit a new NTS report. Updated information should include the results of the effectiveness review and newly-developed corrective actions.

Contractor Assessment Program Weaknesses

Background

Title 10 C.F.R. Section 830.121(a) requires that contractors conducting activities that affect, or may affect, the nuclear safety of DOE nuclear facilities must conduct work in accordance with the QA criteria in Section 830.122, *Quality Assurance Criteria*. Section 830.122(i), *Criterion 9 – Assessment/Management Assessment*, identifies criteria specific to the conduct of management assessments, and Section 830.122(j), Criterion 10 – *Assessment/Independent Assessment*, identifies criteria for independent assessments. Both assessment functions are required but, where appropriate, must be implemented in a graded approach consistent with Section 830.7, *Graded Approach*. DOE Order 470.4B, Attachment 2, Section 2, *Survey, Review and Self-Assessment Programs*, requires an assessment of all applicable safeguards and security (S&S) topical areas at a contractor facility or site, conducted by contractor security personnel at intervals consistent with risk management principles, to determine the overall status of the S&S program at that location and verify that S&S objectives are met. Additionally, in the worker safety area (as in the nuclear safety and classified information security areas), failure to discover problems (e.g., by having an ineffective assessment process) can lead to loss of mitigation in an enforcement action.

Supplemental DOE guidance specific to assessments is set out in DOE Guide 414.1-1C, *Management and Independent Assessments Guide*. This guide provides significant detail on assessment program purpose, objectives, and implementation. In addition, the Energy Facility Contractors Group (EFCOG) has issued an assessment guide, *Implementing the Assessment Process at the Department of Energy Facilities*, that describes the types of assessments, steps in the assessment process, obstacles to implementing an effective assessment program, and ways to overcome these obstacles. The EFCOG assessment guide can be found at: http://www.efcog.org/wg/ec/documents.htm

When conducted effectively, contractor assessment activities are a significant part of the performance feedback loop, allowing the proactive identification and correction of deficiencies in safety and classified information security that might otherwise result in events. However, over

the past several years, DOE enforcement activities have indicated a need for improvement in the conduct of contractor assessment programs, based on the following observations:

- A lack of assessment activity in significant safety and classified information security related areas

- Ineffective assessments, as evidenced by the absence of assessment findings in areas where programmatic problems have been disclosed through other means (e.g., operational history, events)

- Weaknesses in the effective correction and closure of assessment issues, resulting in recurrent and longstanding deficiencies.

During investigations of potential regulatory noncompliances, the Office of Enforcement typically reviews contractor assessment performance and results as they specifically relate to the subject area of the investigation.

Commonly Observed Assessment Weaknesses

- Procedural expectations for assessment scoping and scheduling are unclear or do not exist.

- Management and independent assessment processes have not been evaluated for effectiveness.

- A poor rationale (or none at all) is provided to explain failure to complete scheduled assessments.

- Assessments are not planned, conducted, and reported in accordance with procedural requirements.

- Management is not involved in completing the assessment (involvement may include participation in data collection or evaluation of results).

- Personnel performing the assessment are not trained in the assessment process or knowledgeable of the program, system, or process being assessed.

- Quality problems and noncompliances identified during the assessment are not evaluated and entered into a formal corrective action system consistent with site procedures.

- Causal analyses do not adequately evaluate the EOC, and corrective actions do not address causes or appear appropriate to prevent recurrence.

- Corrective actions are not assigned to specific “owners,” do not have associated milestone dates, and are not completed/closed in a timely fashion.

- Closure documentation is not consistent with the identified corrective actions, and the documented evidence is not adequate to support closure.

- The organization has not determined whether findings identified during assessments represent longstanding or recurring problems or whether assessment results are consistent with other indicators of performance.