



---

# ***SAFETY AND SECURITY ENFORCEMENT COORDINATOR HANDBOOK***

***August 2012***

***Office of Enforcement and Oversight  
Office of Health, Safety and Security  
U.S. Department of Energy***

## Table of Contents

*Ensure use of the proper version by checking with the Office of Enforcement and Oversight website at: [www.hss.doe.gov/enforce/process\\_guidance.html](http://www.hss.doe.gov/enforce/process_guidance.html).*

**Acronyms and Definitions..... iii**

**I. Purpose of Enforcement Coordinator Handbook..... 1**

**II. Enforcement Coordinator Roles and Responsibilities ..... 2**

- DOE Enforcement Coordinator .....2
- Contractor Enforcement Coordinator.....3

**III. Noncompliance Reporting Criteria ..... 5**

- Worker Safety and Health Noncompliance Reporting Criteria (Tables III-1 & III-2) .....5
- Nuclear Safety Noncompliance Reporting Criteria (Tables III-3 & III-4) .....8
- Classified Information Security Noncompliance Reporting Criteria (Table III-5) ..... 11
- Contractor Tracking of Non-NTS/SSIMS Reportable Noncompliances..... 13

**IV. Contractor Noncompliance Screening and Reporting Guidance ..... 14**

- Noncompliance Screening..... 14
- Reporting a Programmatic or Repetitive Noncompliance ..... 14
- Reporting a Willful Noncompliance or Misrepresentation..... 15
- Reporting a Worker Retaliation ..... 16
- NTS and SSIMS Report Content and Closure..... 17
- ORPS Occurrence Associated with a Noncompliance ..... 19
- Additional Guidance Unique to Worker Safety and Health Enforcement..... 19
  - Multiple Employer Worksite..... 19
  - General Duty Clause ..... 20
  - Coordinating Application of Civil Penalty and Contract Fee Reduction ..... 21
  - Applicability of Part 851 and “Work for Others” ..... 22
  - Offsite Support for Emergencies..... 22
- Additional Guidance Unique to Nuclear Safety Enforcement ..... 22
- Additional Guidance Unique to Classified Information Security Enforcement ..... 23
  - SSIMS Background and Reporting ..... 23

- 
- 
- **Common Deficiencies in Contractor Screening Processes .....24**

**Appendix A: Contractor Corrective Action Processes and Assessments**

**Contractor Investigation, Causal Analysis, and Corrective Action .....26**

- **Investigation, Causal Analysis, and Corrective Action Process.....26**
  - **Relevant Requirements and Other Regulatory Drivers .....26**
  - **General Principles .....27**
  - **Scope of Investigation.....27**
  - **Causal Analysis .....29**
  - **Corrective Actions .....30**

**Contractor Assessment Program Weaknesses .....31**

- **Background .....31**
- **Commonly Observed Assessment Weaknesses.....32**

## Acronyms and Definitions

### 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
EFCOG	Energy Facility Contractors Group
EGS	Enforcement Guidance Supplement
EOC	Extent of Condition
EPO	Enforcement Process Overview
FNOV	Final Notice of Violation
HSS	Office of Health, Safety and Security
HS-40	Office of Enforcement and Oversight
IDLH	Immediately Dangerous to Life and Health
IOSC	Incidents of Security Concern
MI	Management Interest
NNSA	National Nuclear Security Administration
NOV	Notice of Violation
NTS	Noncompliance Tracking System
OGC	Office of General Counsel
ORPS	Occurrence Reporting and Processing System
OSR	Operational Safety Requirement
PI	Procedural Interest
PNOV	Preliminary Notice of Violation
QA	Quality Assurance
RAM	Radioactive Material
S&S	Safeguards and Security
SI	Security Interest
SSIMS	Safeguards and Security Information Management System
SSC	Structures, Systems, and Components
TSR	Technical Safety Requirement
WSHP	Worker Safety and Health Program

## Definitions

**Contractor Assurance Systems:** 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:** Refers to 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 and Oversight.

**Enforcement Action:** Refers to a Preliminary Notice of Violation (PNOV), Final Notice of Violation (FNOV), or Compliance Order, and does not include a Consent Order, Settlement Agreement, Enforcement Letter, or Special Report Order.

**Enforcement Coordinator:** Refers to the DOE and/or contractor personnel assigned to serve as the principal interface in an organization for issues related to rule implementation, noncompliances, and enforcement proceedings.

**Enforcement Outcome:** The general term used to refer to the result of an enforcement evaluation or investigation of an event or condition involving noncompliances.

**Enforcement Sanction:** The general term used to refer collectively to Enforcement Actions (see above), Consent Orders, Settlement Agreements, and Special Report Orders.

**Noncompliance:** Refers to a condition that does not meet a DOE regulatory requirement.

**Notice of Violation:** Refers to either a PNOV or a FNOV.

**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 different events or conditions separated in time with comparable causes/circumstances and which involve substantially similar work activities, locations, equipment, or individuals where it would be reasonable to assume that the contractor's corrective actions for the first occurrence should have prevented the subsequent event/condition.

**Violation:** Refers to a DOE 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 Enforcement Process Overview (EPO). It provides detailed information on such topics as Noncompliance Tracking System (NTS) and Safeguards and Security Information Management System (SSIMS) notification 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 serve to benefit contractors by providing the Office of Enforcement and Oversight (HS-40) with a level of confidence in the contractors' compliance assurance processes such that the office may elect to exercise regulatory discretion and/or mitigate the possible sanctions associated with an enforcement proceeding.

As described in the EPO, HS-40 implements the safety and security enforcement program in accordance with 10 C.F.R. Parts 820, 824, and 851. The requirements that are enforceable under these procedural regulations include 10 C.F.R. Parts 830, 835, 850, 851, 708, 1016, and 1045; Section 820.11 of Part 820; and DOE security directives that include language as to their enforceability under Part 824. For a current list of those security directives, see [http://www.hss.doe.gov/enforce/secenforce/secenforce\\_regs\\_dirs\\_guidance.html](http://www.hss.doe.gov/enforce/secenforce/secenforce_regs_dirs_guidance.html).

This handbook is updated periodically based on feedback from DOE and contractor enforcement coordinators and others having regulatory compliance responsibilities. The most current version is available from the HS-40 website.

## II. Enforcement Coordinator Roles and Responsibilities

### DOE Enforcement Coordinator

A key step toward facilitating improved performance, enhancing compliance with safety and security requirements, and interfacing with HS-40 is the designation of a point of contact from each DOE organization. Each DOE organization with responsibility for management or oversight of activities that comes under the DOE safety and security rules should identify an enforcement coordinator. 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/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 HS-40 prior to implementing a contract fee reduction or similar contract action related to a safety-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 collaborate with HS-40 in evaluating noncompliances reported into NTS and SSIMS.
- Coordinating the identification of DOE and contractor personnel for technical support to bring an issue to closure.
- Coordinating a periodic review of noncompliances tracked locally by the contractor.
- Conducting routine oversight of the contractor's program for identifying, screening, trending, reporting, correcting, and closing noncompliances.
- Communicating to HS-40 any noncompliances that appear to be above the NTS reporting thresholds but that the contractor declined to report into NTS.
- 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 items reported into SSIMS.

- Reviewing contractor effectiveness reviews performed for NTS-reported noncompliances and ensuring appropriate follow-up actions.
- Entering verification/validation results into NTS with clear recommendations for closure.
- Providing input, with their DOE management, 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 Site Office Coordinator).
- Assisting with the resolution of Requests for Investigation submitted directly to HS-40.

### **Contractor Enforcement Coordinator**

The contractor enforcement coordinator is pivotal in driving improved safety and security performance. As the primary interface with HS-40 and the DOE Field Element and Headquarters Program Office enforcement coordinators, and with support from senior management, the coordinator can positively influence the 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 (i.e., events, performance assessment reports, nonconformance reports, radiological assessment 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 screening and NTS, SSIMS, and internal reporting.
- Ensuring proper and timely reporting of noncompliances into NTS, SSIMS<sup>1</sup>, 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 and scheduling of responses to HS-40 requests for information, investigations, inspections, and enforcement conferences.
- Serving as the liaison between DOE and the contractor during an investigation to ensure that the facts and technical issues are fully understood.
- 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 regulatory screening and reporting program.

---

<sup>1</sup> Includes mandatory SSIMS reporting in accordance with DOE Order 470.4B, Attachment 5, *Incidents of Security Concern*.

### III. Noncompliance Reporting Criteria

All noncompliant conditions are expected to be documented, and a subset are expected to be reported to DOE through NTS or SSIMS, consistent with the guidance provided in this section. As discussed in Chapter IV of the EPO, noncompliance reporting into NTS for worker safety and health and nuclear safety noncompliances is voluntary, although such reporting facilitates HS-40's consideration for discretion as well as mitigation based on prompt reporting. Reporting of noncompliant classified information security conditions into SSIMS is mandatory. 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. These thresholds are also available on the HS-40 Safety and Security Enforcement Program website. Use of these thresholds is discussed generally in Chapter IV of the EPO and specifically in the NTS and Occurrence Reporting and Processing System (ORPS) reporting discussions that follow Table III-4.

#### Worker Safety and Health Noncompliance Reporting Criteria

**Table III-1**

**Worker Safety and Health Noncompliances Associated With Occurrences (DOE Order 232.2)**

*Consult the DOE Order for the full text of each occurrence criterion<sup>1</sup>.*

Reporting Criteria Group	Subgroup	Occurrence Category and Summary Description <sup>2</sup>
1. Operational Emergencies <sup>3</sup>	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 $> IDLH$ (4) Personnel exposure $> limits$ but $< IDLH$ requiring medical treatment (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 Control	(1) Unexpected/unintended personal contact (2) Unexpected discovery of uncontrolled energy source
	F. Hazardous Energy Control (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 NTS Worker Safety and Health Reportable Conditions**

Reporting Threshold	Notes <sup>4</sup>
Severity Level I noncompliance(s) with Parts 851 or 850 (Refer to Part 851, Appendix B, Section VI(b)(1)) <sup>5</sup>	Conditions of noncompliance 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.
Programmatic deficiencies involving noncompliances	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 and requires broad corrective actions.
Repetitive noncompliances	Two or more different 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 associated with 851.20(a)(6) or (9)	Customarily referred to as worker retaliation.

Notes to 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 on 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 event-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.
- 5 Conditions of noncompliance identified by any method or means (e.g., assessments, inspections, observations, employee concerns, event evaluation) that would not otherwise be reported into NTS as either a Management Issue or Occurrence, but 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.

## **Nuclear Safety Noncompliance Reporting Criteria**

**Table III-3**

### **Nuclear Safety Noncompliances Associated With Occurrences (DOE Order 232.2)**

*Consult the DOE Order for the full text of each occurrence criterion<sup>1</sup>.*

<b>Reporting Criteria Group</b>	<b>Subgroup</b>	<b>Occurrence Category and Summary Description<sup>2</sup></b>
1. Operational Emergencies <sup>3</sup>	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 <sup>4</sup>
	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 835 App. E)
	B. Spread of Radioactive Contamination	(1) Offsite radioactive contamination <sup>5</sup>
	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 (3) Onsite personnel/clothing contamination <sup>6</sup>

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 <sup>7</sup>
Programmatic deficiencies involving noncompliances	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 and requires broad corrective actions.
Repetitive noncompliances	Two or more different 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 830/835 noncompliances	Customarily referred to as worker retaliation <sup>8</sup> .

#### Notes to 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 on the table should evaluate the event 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 event-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 Structure, System, or Component preventing satisfactory performance of its design function when required to be operable or in operation.
5. Report noncompliances associated with an offsite spread of contamination event where a contamination level exceeds 100 times the applicable value identified in 10 C.F.R. Part 835, Appendix D.
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 of 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. Potentially 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 the ability of organizations 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.

Classified information security noncompliances are categorized according to the disclosure or potential disclosure of DOE classified information placed at risk. There are two categories of noncompliances that are based on the relative severity of a classified information security incident. The categories are identified by an event category and type (see Table III-5 below). Each of the two categories is further subdivided into three types based on the type of interest (security interest, management interest, and procedural interest).

(NOTE: Security incidents involving the protection and control of classified information categorized as “B” require documented evidence to support the determination that a compromise has not occurred or the likelihood of potential compromise is remote.)



**Table III-5**

**Classified Information Security Reportable Noncompliances (DOE Order 470.4B)**

*This table contains those reportable noncompliances involving classified information security. Consult the DOE Order for the full text of each IOSC criterion.*

<b>Significance Level Category</b>	
<b>A</b>	<b>B</b>
<p>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 DOE/National Nuclear Security Administration (NNSA) Cognizant Security Officer (CSO), contractor CSO, and reporting in SSIMS.</p>	<p>Category B incidents, which do not meet the Category A criteria, are managed and resolved by the contractor CSO; however, this does not preclude the DOE/NNSA CSO from exercising its oversight responsibilities. The monitoring of Category B incidents by the contractor CSO is essential as it allows management to proactively address reoccurring 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.</p>
<b>Incident Type</b>	
<b>Security Interest (SI)</b>	<b>Security Interest (SI)</b>
<p>This type of incident results in the loss, theft, compromise, or suspected compromise of classified matter.</p>	<p>Not Applicable to Part 824</p>
<b>Management Interest (MI)</b>	<b>Management Interest (MI)</b>
<p>Not Applicable to Part 824</p>	<p>Not Applicable to Part 824</p>
<b>Procedural Interest (PI)</b>	<b>Procedural Interest (PI)</b>
<p>Not Applicable to Part 824</p>	<p>This type of incident is associated with the 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.</p>

### **Contractor Tracking of Non-NTS/SSIMS Reportable Noncompliances**

For enforcement purposes, reporting a noncompliance that is below an NTS and SSIMS reporting threshold into a contractor's tracking system also constitutes formal reporting to DOE. HS-40 expects these noncompliances to be tracked and managed to resolution by the contractor's internal issues management or corrective action process. HS-40 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.

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 and Program Office coordinators, as well as HS-40 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. HS-40 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**

The processes used by the contractor to self-identify problems may identify issues ranging from serious events, 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 the problems. 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 issues 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
- Occupational Safety and Health Administration 300 logs
- 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 or 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, management has concluded 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 are indicative of 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, but are not reported in NTS or SSIMS, 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 DOE determination that a contractor 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 any willful noncompliance involving worker safety and health, nuclear safety, or classified information security rules to be reported. 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, it may be discovered during an event investigation that a worker intentionally deviated from or overrode a safety control or security requirement, thereby constituting a willful noncompliance.

HS-40 expects that a matter should be treated as a willful noncompliance and reported into NTS or SSIMS whenever there is evidence indicating that the noncompliance was intentional or willful. The determination of intention requires careful consideration. Failure of a worker to perform a required action, for example, is not necessarily evidence of negligence or an intentional disregard of requirements. Such a failure could result for many reasons (e.g., a lapse in recalling the training or inadequate training) and does 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 a Worker Retaliation**

HS-40 has established an explicit NTS reporting noncompliance category that addresses reporting of retaliations against workers who raise worker safety and health or nuclear safety concerns.

HS-40 has 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 as a condition for asserting that a retaliation occurred. HS-40's general guidance for reporting worker retaliation is as follows:

- The standard NTS reporting requirement – 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 an initial determination, these decisions are authoritative in nature. Forgoing NTS reporting until the appellate process is complete is not considered timely and would preclude potential mitigation if a Notice of Violation is issued.
- HS-40 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 details on the contractor's planned path forward.

- A worker need not file a claim under 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 NTS reportable if a nuclear safety or worker safety and health regulatory noncompliance exists. 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 HS-40 personnel have sufficient information to understand the circumstances of the noncompliance or the events that led to the 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, a security notification report for an event and subsequent inquiry report must be completed and entered into SSIMS. These reports should contain appropriate information so that HS-40 personnel have sufficient information to 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 information specifically related to the noncompliance(s) or circumstances surrounding the event than is covered in the ORPS or initial security incident report. It 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 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 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 HS-40 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, the level of effort of 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. Not every NTS report will require a full root cause analysis or a complete extent-of-condition determination. HS-40 expects the corrective action section of an NTS or SSIMS report to include those principal corrective actions related to the noncompliance(s). The listing of a single corrective action indicating the intent to conduct a causal analysis or develop a corrective action plan is insufficient. When the corrective actions have been completed and all completion dates entered into the NTS/SSIMS systems, 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 effectively completed. 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 report closure is recommended, the DOE enforcement coordinator marks the report as "Ready for Closure" in NTS; HS-40 staff then reviews the NTS report closure status and the Field Element recommendation/response. Barring any concerns, HS-40 closes the report, and the report's status is subsequently changed in the database.

For classified information security noncompliances, inquiry officials must verify that corrective actions have been completed and forward a final report to line management for action and to the Office of Health, Safety and Security's Office of Security. This closure would be recorded in SSIMS. The Inquiry Report in SSIMS is officially closed after the cognizant Program Office concurs with the site management recommendation to do so, and the report's status is changed in SSIMS.



## **ORPS Occurrence Associated with a Noncompliance**

A number of ORPS event categories have significant safety implications, but not all ORPS occurrences involve regulatory noncompliances. A contractor is expected to report into NTS the 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, which can make managing worker safety and health more challenging. Subparts B and C of Part 851 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 must be given special consideration.

When investigating a matter involving risk to workers from multiple contractors, HS-40 determines the full extent of responsibility among those contractors for exposing employees to hazards. In such cases, HS-40's investigation will focus on determining which contractor(s): A) created the hazard; B) had responsibility for correcting and controlling the hazard; and C) exposed the employees to the hazard.

To establish the extent of contractor responsibility, HS-40 reviews available records and procedures that describe roles and responsibilities, determines whether responsible employees have received appropriate training, and ascertains the actual practices and conditions in the workplace. HS-40 may cite any contractor found responsible, whether or not the contractor's own employees were exposed to the hazard in question.

If an enforcement sanction will be issued, HS-40 also considers both mitigating and aggravating circumstances for each contractor involved, in accordance with the enforcement process described in 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 will pursue an enforcement case against a contractor who 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 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 where:

- 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 in noncompliance with Section 851.10(a) and may be subject to the issuance of a Notice of Violation with 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 the occurrence of 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 in the situation, 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 the use of a work practice that is contrary to an accepted industry practice or standard, 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 the hazard should have been recognized by a reasonable person.

3. *Is the hazard causing, or does it have the potential to cause, death or serious physical harm?* 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. This can include any potential 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. Alternatively, it could be an illness that significantly reduces 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 is a feasible and known 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 states that contractors indemnified under the Atomic Energy Act are subject to either civil or contract penalties, but not both. Most of DOE's contractors are indemnified under Section 170d of the Atomic Energy Act. Those that are not indemnified under Section 170d are handled under the contract remedy provisions of the Rule. The DEAR clause (48 C.F.R. 923.7002) also states that for a worker safety violation, the contracting officer must coordinate with HS-40 before pursuing a contract fee reduction in the event of a violation by the contractor.

The current enforcement process includes a determination by the Director of HS-40, in consultation with the appropriate Program Office and Field Element, that an enforcement action will be taken against a contractor and that a monetary penalty will be assessed. To ensure adequate consultation, HS-40 has built certain coordination steps into its enforcement process (see EPO Chapter VI, *Investigation Process*) to ensure that both DOE Program and Field Element representatives' perspectives and views are considered throughout the entire enforcement process.

## **Applicability of Part 851 and “Work for Others”**

Part 851 states that it applies to the conduct of contractor activities at DOE sites where a contractor is an entity under contract to DOE “that has responsibilities for performing work at a DOE site in furtherance of a DOE mission.” Often, DOE facilities, particularly in the science arena, are made available to representatives of various institutions, companies, and foreign organizations to conduct research studies and activities. Questions have been raised as to whether enforcement would apply to worker safety issues that involve such workers performing research for others using DOE facilities. DOE’s Office of General Counsel (OGC) has developed guidance on the application of 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 the DOE mission. This guidance has been incorporated into DOE Guide 440.1-8, *Implementation Guide for Use with 10 C.F.R. Part 851, Worker Safety and Health Program*, which is available through the following website:

[www.hss.energy.gov/healthsafety/WSHP/rule851/851final.html](http://www.hss.energy.gov/healthsafety/WSHP/rule851/851final.html)

The Part 851 enforcement process that is outlined in this guidance applies to those contractors and that work where the OGC has determined that Part 851 is applicable, as detailed in the above guide.

## **Offsite Support for Emergencies**

Part 851 applies to services provided under contract to DOE on a DOE site. In some cases, HS-40 may determine that Part 851 may apply 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 consequently falls within the scope of the Rule.
- Where the activities took place.

Contractors are expected to conduct appropriate baseline needs assessments to ensure that 10 C.F.R. Part 851 program requirements are addressed. Except for unusual or egregious deficiencies, HS-40 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 focus is normally directed toward the operating or management/integrating contractor in evaluating how well the program requirements are met. As in any potential enforcement situation, HS-40 will evaluate the situation based on its own specific merits.

## **Additional Guidance Unique to Nuclear Safety Enforcement**

To better support and describe the implementation of the Department’s nuclear safety enforcement program, over the years HS-40 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 for review on the HS-40 website at:

[http://www.hss.doe.gov/enforce/archives/guidance\\_supplement/egs.pdf](http://www.hss.doe.gov/enforce/archives/guidance_supplement/egs.pdf)

### **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 process is in addition to the mandatory security incident reporting requirements contained in 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 classified information security noncompliances, including events and self-assessment results, and the resulting corrective actions. Event reporting timeframes are based upon security significance and adhere to requirements identified in DOE Order 470.4B, Attachment 5, *Incidents of Security Concern*. 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, but are reported within the Inquiry Report.

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

To ensure a consistent approach in security noncompliances reported by contractors, 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 these controls. Additionally, when management determines the existence of conditions that require broad corrective actions to improve management or process controls, management has concluded 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 subsequent deficiencies should have been appropriately averted by the contractor’s corrective actions associated with the previous noncompliance.
- **Intentional/Willful Noncompliance or Misrepresentation**: An intentional/willful noncompliance or misrepresentation may involve inventory records or inventory results that are falsified intentionally, such as classified removable electronic media inventory activities. 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 specific noncompliance threshold should be reflected in the finding comments section of the SSIMS report along with a description of the self-identified security concern.

### **Common Deficiencies in Contractor Screening Processes**

Historically, HS-40 has observed a number of common weaknesses or errors in processes for screening deficiencies 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 (assessment reports, employee concerns, etc.).
- 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 these 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.

Further examples are contained within the reports of regulatory assistance reviews and program reviews available on the HS-40 website.

## 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 the Enforcement Coordinator Handbook by providing additional details on these processes, particularly those areas in which the Office of Enforcement and Oversight (HS-40) 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.

### Contractor Investigation, Causal Analysis, and Corrective Action

As part of the investigation of potential nuclear safety, worker safety and health, or classified information security noncompliances, HS-40 routinely reviews contractors' investigations of noncompliances, preliminary inquiry reports, the associated causal analyses, and the corrective actions developed to resolve the noncompliance and prevent recurrence. During those reviews, HS-40 has noted several common deficiencies. Additionally, an enforcement case is typically pursued because of recurrent events or deficiencies, indicating weaknesses in contractor processes for developing, implementing, or sustaining effective corrective actions. HS-40 provides this information as potential lessons learned for the DOE contractor community.

#### Investigation, Causal Analysis, and Corrective Action Process

##### Relevant Requirements and Other Regulatory Drivers

Specifically for nuclear safety, 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 both correct the deficiencies and prevent recurrence. Additionally, Part 820, Appendix A, *Nuclear Safety 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 rule does not mandate a quality improvement process, the enforcement provisions of Part 851, and its Enforcement Policy in Appendix B, establish incentives for crediting contractors' timely and comprehensive corrective actions as one of the factors in applying enforcement discretion and possible mitigation.

When HS-40 notes deficiencies during its investigation activities or observes recurring problems and repetitive events, HS-40 cannot make a favorable judgment regarding



compliance with the QA Rule requirements or granting discretion or mitigation as delineated in the above enforcement policies. It is hoped that contractors will evaluate and improve their processes in these areas and avoid these types of deficiencies.

## **General Principles**

HS-40 generally expects that a contractor conducting an investigation/causal analysis will ensure that the personnel who conduct the investigation are independent and adequately trained and qualified, the investigation includes appropriate scope and depth, and the corrective actions are timely and clearly relate to identified causes. This expectation applies to contractor investigations of events and investigations of safety/security issues identified as a result of more proactive means (e.g., assessments).

The level of effort of 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 root cause analysis criteria delineated in the DOE Order for occurrence reporting. For example, identification of apparent causes may be an appropriate endpoint when investigating less-significant problems, while a full root cause analysis would be appropriate for more significant or complex issues.

## **Scope of Investigation**

After a deficiency or quality problem has been identified, it must be fully evaluated and characterized 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, HS-40 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, an EOC review should be performed 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). Areas to be covered as part of an effective EOC review vary with the specifics of the identified problem, but generally include the following:

- 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 anticipated based on the identified problem.
- Reviewing prior applications of the deficient process or procedure to see whether earlier deficiencies had gone unnoticed.

The approach used in 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 specificity needed to adequately assess the scope of the problem.

The most common performance deficiency in this area is the simple failure to conduct an EOC review for deficiencies that are indicative of a programmatic deficiency or otherwise have a clear potential for generic 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 HS-40 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 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 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 determined 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 developed 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 on events, assessment results, etc.

## 3. Evaluation of Assessment Performance

Over the past several years, HS-40 has increasingly focused on the implementation and effectiveness of contractors' assessment programs in improving safety and security performance. HS-40 has concluded that self-identification through implementation of an effective internal assessment program (rather than by reacting to events) is a cost-effective way to improve worker safety and health, nuclear safety, and classified information security performance.

Consequently, when conducting an event investigation, HS-40 typically asks whether the subject safety or security noncompliance should have reasonably been identified through the contractor's assessment program. Based on the initial answers, follow-up questions can help identify deficiencies in assessment scheduling, quality, or corrective action development and implementation. The effectiveness of tools for self-identifying and tracking/trending deficiencies may be evaluated during an event investigation. Also, the development of corrective actions and independent validation of the effectiveness of the corrective actions will be evaluated. HS-40 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, and classified information security problems.

## **Causal Analysis**

An effective causal analysis is essential in developing appropriate corrective actions for an identified worker safety and health, nuclear safety, or classified information 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, HS-40 considers the most frequent deficiency in this area to be the tendency for analyses to be truncated before getting to underlying issues; that is, they do not go "deep" enough. In particular, HS-40 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 this 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 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 can include the following:

- 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

HS-40 has also noted that some causal analyses do not identify all significant issues associated with an event. For example, HS-40 is typically just as interested in the reasons why a longstanding nuclear safety noncompliance persisted without being identified as in the specific causes of the original noncompliance. Often, such questions are not asked as part of the causal analysis, which tends to focus on the specific failure condition.

## Corrective Actions

HS-40 evaluates contractor corrective action plans as part of the routine review of submitted Noncompliance Tracking System (NTS) and Safeguards and Security Information Management System reports during regulatory assistance reviews and as part of an investigation into a worker safety and health, nuclear safety, or security problem. HS-40 uses the general criteria outlined below to evaluate corrective actions, and also relies on the judgment of cognizant DOE/ National Nuclear Security Administration representatives when evaluating the adequacy of contractor corrective actions:

- Clear linkage to 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 culture 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. HS-40 expects that any delays in corrective action completion will be justifiable 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.

HS-40 views the practice of conducting an effectiveness review as a positive one that should reduce the incidence of recurrent events. For NTS-reportable noncompliances, 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 HS-40’s expectation that the contractor and local DOE personnel verify completion of corrective actions before closing 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. Section 830.122(i) identifies criteria specific to the conduct of management assessments, and Section 830.122(j) 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. DOE Order 470.4B, Attachment 2, Section 2, 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, 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 414.1-1B, *Management and Independent Assessments Guide*. DOE Guide 414.1-1B provides significant detail and guidance 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 part of a significant performance feedback loop, allowing the proactive identification and correction of safety and classified information security deficiencies that might otherwise result in significant events. However, over the past several years, DOE enforcement activity has indicated a need for improvement in the conduct of contractor assessment programs, including:

- 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, HS-40 typically reviews contractor assessment performance and results as they specifically relate to the subject area of the investigation.

### **Commonly Observed Assessment Weaknesses**

- A. Procedural expectations for assessment scoping and scheduling are unclear (or did not exist).
- B. Management and independent assessment processes have not been evaluated for effectiveness.
- C. Poor rationale (or no rationale exists) for not completing scheduled assessments.
- D. Assessments are not planned, conducted, and reported in accordance with procedural requirements.

- E. Management is not involved in completing the assessment (involvement may include participation in data collection or evaluation of results).
- F. Personnel performing the assessment are not trained in the assessment process or knowledgeable of the program, system, or process being assessed.
- G. Quality problems and noncompliances identified during the assessment are not evaluated and entered into a formal corrective action system consistent with site procedures.
- H. Causal analyses do not adequately evaluate the EOC, and corrective actions do not address causes or appear appropriate to prevent recurrence.
- I. Corrective actions are not assigned to specific “owners,” did not have associated milestone dates, and are not being completed/closed in a timely fashion.
- J. Review closure documentation is not consistent with planned corrective actions, and adequate evidence does not exist to support closure.
- K. No evaluation has been conducted of whether findings identified during assessments represent longstanding or recurring problems or whether assessment results are consistent with other indicators of performance.