

EVENT REPORTING PROGRAM

The Event Reporting Program is designed to integrate the requirements applicable to the Ames Laboratory for Occurrence reporting with the noncompliance reporting requirements for Worker Safety and Health, Nuclear Safety, and Incidents of Security Concern into a unified process. It also provides assurance to management and the Department of Energy (DOE) that issues connected with events that do not meet the DOE threshold reporting requirements are addressed through appropriate corrective actions.

1.0 APPROVAL RECORD

- Reviewed by: Document Control Coordinator (Amy Tehan)
- Approved by: Quality Assurance Manager & ESH&A Manager (Tom Wessels)
- Approved by: Chief Operations Officer (Mark Murphy)
- Approved by: Associate Laboratory Director for Sponsored Research Administration (Debra Covey)
- Approved by: Assistant Director for Scientific Planning (Cynthia Jenks)
- Approved by: Chief Research Officer (Duane Johnson)
- Approved by: Interim Deputy Director (David Baldwin)
- Approved by: Interim Director (Tom Lograsso)

The official approval record for this document is maintained in the Training, Documents & Records Office, 151 TASF.

2.0 REVISION/REVIEW INFORMATION

The revision description for this document is available from and maintained by the author.

3.0 PURPOSE AND SCOPE

Ames Laboratory is a government owned, contractor-operated national research laboratory that conducts basic and applied research for the DOE. Ames Laboratory is located on the Iowa State University (ISU) campus. Government owned buildings are located on land leased from the State of Iowa under a long-term lease and some space for Laboratory activities is rented from the University.

There are no major user facilities at this site, such as a nuclear reactor or accelerator. Ames Laboratory purchases utility services from the City of Ames and the University; therefore no power plants, water-treatment, sewage, or solid-waste facilities are operated by the Laboratory. The City of Ames provides fire protection, under contract. Local Law Enforcement Agency assistance is provided by ISU Department of Public Safety (DPS) and the City of Ames Police. Ames Laboratory conducts no classified research, has no classified documents and does not sponsor security clearances.

The Office of Health, Safety and Security's (HSS) [Office of Enforcement and Oversight](#) is responsible for enforcing Federal regulatory requirements pertaining to worker safety and health, nuclear safety, and classified information security programs at Department of Energy (DOE) sites. The [Safety and Security Enforcement Program](#) is the foundation of DOE's enforcement actions.

The Worker Safety and Health enforcement action include requirements in [regulations, directives, and enforceable consensus standards](#).

Regulations include:

- [10 C.F.R. Part 850](#) Chronic Beryllium Disease Prevention Program
- [10 C.F.R. Part 851](#) Worker Safety and Health Program
- OSHA regulations (29 C.F.R. [Part 1904](#), [Part 1910](#), [Part 1926](#))

The enforceable consensus standards include:

- National Fire Protection Association (NFPA)
- American National Standards Institute (ANSI)
- American Society of Mechanical Engineers (ASME)
- American Conference of Government Industrial Hygienists (ACGIH)

The Nuclear Safety enforcement actions include requirements in [regulations and directives](#).

Regulations include:

- [10 C.F.R. Part 820](#) Procedural Rules for DOE Nuclear Activities
- [10 C.F.R. Part 830](#) Nuclear Safety Management
- [10 C.F.R. Part 835](#) Occupational Radiation Protection
- [10 C.F.R. Part 708](#) Criteria and Procedures for DOE Contractor Employees Protection Program

Part 820 provides the procedural rules for the Nuclear Safety Enforcement Program, Appendix A to the rule provides the General Statement of its Enforcement Policy, and this Event Reporting Plan, [Plan 10200.002](#) details the Laboratory's enforcement reporting processes. The applicable section of Part 830 is Subpart A: Quality Assurance Requirements, which is addressed by the Ames Laboratory Quality Assurance Program Plan, [Plan 10200.026](#). Part 835 Occupational Radiation Protection is applicable to Ames Laboratory radiological activities as described in the Ames Laboratory Radiation Protection Program (RPP), [Plan 10202.004](#). Part 708 is a program that provides procedures to protect employees of DOE contractors who believe they have suffered retaliation for disclosing information concerning danger to health or safety, substantial violations of law, or gross mismanagement; for participating in Congressional proceedings; or for refusing to participate in dangerous activities.

The Security Enforcement program is primarily responsible for enforcing the requirements related to classified information.

Classified Information Security Regulations include:

- [10 C.F.R Part 824](#) - Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations
- [10 C.F.R Part 1016](#) - Safeguarding of Restricted Data
- [10 C.F.R Part 1045](#) - Nuclear Classification and Declassification

The Ames Laboratory does not have classified information or materials, but the Laboratory's contract includes [DOE Order 470.4B](#) Admin. Chg. 1 Safeguards and Security Program, which details reporting requirements for Incidents of Security Concern that are included in this plan.

The Office of Enforcement and Oversight's Enforcement Process Overview provides additional detail on how the DOE Safety and Security Enforcement Program is administered and implemented. For worker safety and health and nuclear safety noncompliances, DOE expects laboratories to voluntarily report noncompliances that meet certain criteria into the Noncompliance Tracking System. For an introduction to the enforcement program, consult the [Enforcement Process Overview](#) and the [Enforcement Coordinator Handbook](#).

3.1 Definitions

- Radiological Activities: The requirements in 10 CFR Part 835 are applicable to all DOE activities involving occupational exposure to ionizing radiation of DOE employees and DOE contractor and subcontractor employees, except for an activity specifically excluded under Part 835.1(b).
- Nuclear Facility: As per 10 CFR 830.3, nuclear facility means reactor and nonreactor nuclear facilities.
- Nuclear Safety Noncompliance: A Nuclear Safety Noncompliance is a failure to comply with an applicable nuclear safety requirement. Isolated minor noncompliances involving minimal or low safety significance will normally not be subject to enforcement action unless they are repetitive or multiple examples appear indicative of a larger programmatic breakdown.
- WSH Noncompliance: As per 10 CFR Part 851, a noncompliance of the Worker Safety and Health Program which meets or exceeds the thresholds established by the DOE Office of Enforcement criteria as described in its *Enforcement Process Overview*.
- Violation: A violation is a noncompliance that DOE has evaluated and found to be a significant failure to comply with an applicable nuclear safety requirement. DOE identifies a violation through a Notice of Violation.
- Enforcement Action: The issuance of an enforcement letter, Consent Order, or a Notice of Violation with or without a civil penalty.
- Safety Significant SSC: Ames Laboratory has one system recognized as a Safety Significant SSC (Structures, Systems and Components): the hydrogen fluoride operation in 147 Metals Development Building (Activity 30411.003, Hydrofluorination of Rare Earth Oxides). The hood exhaust, detectors and valves are interlocked to prevent employee exposure to HF gas. Performance degradation of this SSC should be considered for reportability as a Group 4 - Facility Status, Subgroup A, Safety Structure / System / Component Degradation.

4.0 Event Reporting Policy

It is the policy of Ames Laboratory to encourage a positive attitude toward reporting events to ensure that Ames Laboratory management and DOE officials are kept fully and currently informed of all events and conditions which could affect the health and safety of the public,

seriously impact the intended purpose of Laboratory facilities, have a noticeable adverse effect on the environment, impact safeguards and security, or endanger the health and safety of workers. It is also the policy of Ames Laboratory that the Event Reporting Program is established and shall include assignment of responsibilities and the establishment of processes in accordance with DOE requirements. The Event Reporting Program Plan and related documents shall address identification and categorization of events, notification of DOE, and preparation of reports, investigation and analysis, corrective action development, tracking, and verification, and distribution of lessons learned.

5.0 Roles and Responsibilities

The roles and responsibilities for activities related to Event Reporting are defined below.

5.1 Identification of Events

Events are discovered through a variety of methods including: observation by line management, internal and external reviews, and self-proclamations. Ames utilizes all of these methods and has designated an Event Screening Team to review information from a variety of sources for identification of potentially reportable events. Also, the Environment, Safety, Health and Assurance office (ESH&A) and the Event Categorization Team are involved with identification of potentially reportable events.

5.2 Categorization of Events

After the Event Categorization Team is notified that a potentially reportable event has occurred, an initial categorization shall be performed within two hours by at least two members of the Event Categorization Team. The [Event Categorization Team](#) consists of the Facility Manager, the Event Reporting Officer, the Emergency Coordinator, and the Event Investigators and Reporters.

5.3 Prompt Notification

Upon categorization of an event, the Event Categorization Team is responsible for notification of the Ames Laboratory Facility Manager (the Chief Operations Officer). Likewise, the Facility Manager is responsible for prompt notification of DOE officials, Laboratory Director, Deputy Director and in some cases other regulatory entities. The Chief Operations Officer is the Ames Laboratory Facility Manager, the ESH&A Manager is the first alternate Facility Manager, and Facilities and Engineering Services (F&ES) Manager is the second alternate Facility Manager.

5.4 Written Reports

ESH&A, Assistant Manager and Plant Protection & Industrial Safety Specialist, Event Investigators and Reporters, have responsibility for preparing written reports.

5.5 Investigation and Analysis

ESH&A, Assistant Manager and Fire and Plant Protection Specialist, Event Investigators and Reporters, have responsibility for investigation of events and the analysis of information for determination of the causes of events.

5.6 Approval of Initial, Updates, and Final Written Reports

The ESH&A Manager (the ESH&A Assistant Manager or the acting ESH&A Manager)

has responsibility for the approval of the initial, updates, and final written reports.

5.7 Analyses and Identification of Recurring Events

The Event Screening Team and the Event Categorization Team have responsibilities for the periodic performance analysis of Ames Laboratory information and events for identification of recurring events. Also, an annual trend analysis is the responsibility of the Laboratory's ESH&A Assistant Manager, according to [Procedure 10200.041](#) *Trend Analysis of ES&H Concerns*.

5.8 Corrective Action Development, Tracking and Verification

The responsibilities for development, tracking and verification of closure for corrective actions related to reportable events are outlined in [Procedure 10200.039](#) *Corrective Action Development, Tracking, and Verification*. Line management has responsibility for the development of corrective actions, with consensus of the issue identifier and ESH&A. ESH&A's Assistant Manager, has responsibility for tracking corrective actions. Line management and ESH&A have responsibility for verification of completion and effectiveness of corrective actions, when appropriate.

5.9 Lessons Learned

ESH&A's Assistant Manager is the Ames Laboratory operating experiences program coordinator and thereby has responsibility for issuance of lessons learned related to reportable events and Ames LOCAL events, according to [Plan 10200.020](#) *Operating Experiences and Lessons Learned Program*. ESH&A's Fire and Plant Protection Specialist has backup responsibility as operating experiences program coordinator.

6.0 Event Reporting Process

6.1 Event Screening

Events are identified by direct observation of equipment or process malfunctions, log or record reviews, operator recognition of their own or others' errors, or other means. Employees must take appropriate immediate action to stabilize and/or place the facility/operation in a safe condition and ensure that any potential environmental effects are stabilized and workers are treated for injuries sustained. Also, the appropriate line management should record and/or archive all pertinent information, including details concerning the discovery of the event and actions taken to stabilize or place the facility/operation in a safe condition.

Events and conditions related to the Ames Laboratory, which may have an adverse effect on the safety, health, security, quality assurance, or have an operational or environmental implication are required to be reported to:

- Facility Manager (Chief Operations Officer)
- Event Reporting Officer
- Members of the Event Categorization Team
- ESH&A Office (515-294-2153),
- Facilities and Engineering Services Office or
- Plant Protection Section (PPS) Office during off normal work hours (515-294-3483).

A team of selected Ames Laboratory personnel, the [Event Screening Team](#), is responsible for determining if issues, concerns, findings, and other operational data are potential reportable events as Occurrences, Worker Safety and Health noncompliances, Nuclear Safety noncompliances, and/or Incidents of Security Concern.

Analysis of issues identified during internal and external assessments should be screened according to the following guidance:

- All issues identified as or equivalent to Level 1 Findings (e.g., deficiencies of major significance that warrant a high level of attention on the part of line management) shall be submitted for categorization.
- All issues identified as or equivalent to Level 2 or Level 3 Findings shall be screened.

The screening process consists of the following:

1. The primary and/or secondary responsible individual(s) review(s) the source of information when the information is developed. The review includes:
 - Analysis of the information relative to the review criteria for considerations of event categorization.
 - Initiation of [Form 10200.149](#) *Event Categorization Form* for each specific item presented to the Event Categorization Team.
 - Documentation that the review was performed (Memo or e-mail to file by Screening Team member).
2. The Event Screening Team should meet with an Event Categorization Team member, or communicate by email or phone, to discuss reviews of information sources performed by Screening Team members since the last meeting.

Issues are designated as potential reportable items according to the event screening criteria, which is based on the specific criteria and guidance presented in DOE requirements for Occurrence Reports, Nuclear Safety Noncompliances, Worker Safety and Health Noncompliances, Security Concerns and CAIRS (Computerized Accident and Injury Report System).

The Event Screening Team should refer to Attachments 1, 2, and 3 of this plan to better understand the issues and events, which should be brought to the attention of the Event Categorization Team.

6.2 Event Categorization

Upon notification of the Event Categorization Team by a member of the Event Screening Team or another individual that an occurrence or a potentially reportable event has occurred, the cognizant Event Categorization Team member shall notify the Event Reporting Officer or the Facility Manager. At least two members of the Event Categorization Team should perform an initial categorization within two hours, except Operational Emergencies, which are categorized according to requirements of DOE Order 151.1C, *Comprehensive Emergency Management System*.

Ames LOCAL Events

Ames Laboratory maintains an internal tracking system onsite as a management tool for issues identified and schedules developed to correct those issues. Events that do not reach the thresholds defined below for Occurrence Reports (Occurrence), Nuclear Safety noncompliances (Nuclear Safety), Worker Safety and Health noncompliances (WSH), Incidents of Security Concern (Security), or injuries and illnesses [first aid cases] (CAIRS) can be classified as AMES LOCAL events and tracked with ALCATS (Ames Laboratory Corrective Action Tracking System). The AMES LOCAL events information must be readily accessible by DOE when they are onsite. The AMES LOCAL events are distinguished as:

- AMES LOCAL – Occurrence
- AMES LOCAL – Nuclear Safety
- AMES LOCAL – WSH
- AMES LOCAL – Security
- AMES LOCAL – CAIRS

For Nuclear Safety and Worker Safety and Health noncompliances, should a non-NTS reportable noncompliance be reviewed by DOE and considered for enforcement action, the Laboratory's recording and tracking of the noncompliance would be considered contractor-identified and reported for purposes of mitigation under DOE's enforcement policy if the noncompliance is clearly below NTS reporting thresholds. However, a significant mischaracterization of the facts or safety significance of the circumstances of a noncompliance could negate any consideration of mitigation.

6.2.1 Occurrence Reports

Ames Laboratory must categorize events, except Operational Emergencies, within 2 hours of discovery. Events can be categorized as Occurrences, within the following significance categories, according to the criteria included in Attachment 1, Occurrence Reporting Criteria, or can be categorized as an AMES LOCAL - Occurrence event at the discretion of the Event Categorization Team.

Operational Emergencies (OE): Major unplanned or abnormal events or conditions that: involve or affect DOE/NNSA facilities and activities by causing, or having the potential to cause, serious health and safety or environmental impacts; require resources from outside the immediate/affected area or local event scene to supplement the initial response; and, require time-urgent notifications to initiate response activities at locations beyond the event scene. Operational Emergencies are the most serious occurrences and require an increased alert status for onsite personnel and, in specified cases, for offsite authorities.

Significance Category (SC) 1: Non-OE events that caused actual harm; posed the potential for immediate harm or mission interruption due to safety system failure and required prompt mitigative action; or constituted an egregious noncompliance with

- regulatory requirements that created the potential for actual harm or mission interruption.
- Significance Category (SC) 2: Circumstances that reflected degraded safety margins necessitating prompt management attention along with modified normal operations to prevent an adverse effect on safe facility operations; worker or public safety and health, including significant personnel injuries; regulatory compliance; or public/business interests.
- Significance Category (SC) 3: Events or circumstances with localized implications including personnel injury, environmental releases, equipment damage or hazardous circumstances that were locally contained and did not immediately suggest broader systemic concerns.
- Significance Category (SC) 4: Events or circumstances that were mitigated or contained by normal operating practices, but where reporting provides potential learning opportunities for others.
- Significance Category (SC) R: Recurring occurrences are those identified as recurring, either directly or through periodic analysis of occurrences and other non-reportable events.

If the consequences are not fully determined or the event exceeds the threshold of more than one criterion, then the event must be categorized at the higher criteria level being considered. The occurrence criterion must be elevated, maintained, or lowered, as information is made available.

Occurrence Report Categorizing Instructions

1. An event can meet multiple reporting criteria that establish it as an occurrence. All of the specific reporting criteria applicable for an occurrence must be identified. Some criteria are “secondary” in that they complement other reporting criteria that require occurrence reporting. In these cases, all of the applicable criteria must be recorded. Each criterion is denoted by its Group, Subgroup (if applicable), and sequence number (#). Thus, for example, the violation of a safety limit is denoted as Group 3, Subgroup A, Sequence (1) or “3A(1).”
2. The attached Occurrence Reporting criteria lists a specific Significance Category (SC) for each criterion, between the sequence number (#) and the criterion text. Significance Categories are designated as “OE” for Operational Emergencies, “R” for recurring occurrences, or 1, 2, 3, or 4. Thus, for example, the Significance Category for a Stop Work Order issued by a DOE office, criterion 4B(1), is SC 2.
3. Operational Emergencies, Significance Category 1, and some other occurrences in lesser significance categories require prompt notification to the DOE HQ OC. **Asterisks (*) next to the significance categories denote occurrences requiring prompt notification to the DOE HQ OC.** Attachment 4 in the Order 232.2 contains the prompt notification requirements.
4. DOE Order 151.1C describes initiating events that are considered Operational Emergencies. DOE Order 225.1B defines when Federal Accident Investigation

Boards must be convened. While some Operational Emergencies and some other ORPS occurrences involve conditions that would be sufficient to initiate accident investigations, criterion 10(1) herein will report the actual initiation of a Federal Accident Investigation Board. All of the specific reporting criteria applicable for an occurrence must be identified. Some criteria are - secondary in that they complement other reporting criteria that require occurrence reporting. In these cases, all of the applicable criteria must be recorded and the event categorized as the higher SC reporting criterion being considered.

See Attachment 1 of this document for Occurrence Reporting Criteria.

6.2.2 Nuclear Safety Noncompliances

The first criterion to be considered is whether the occurrence or condition involves a noncompliance with a nuclear safety requirement set forth in Nuclear Safety Rules or the Ames Laboratory [Plan 10202.004 Radiation Protection Program \(RPP\)](#), a Rule implementation plan. Once it is established that the occurrence or condition in question indeed involves a noncompliance with a nuclear safety requirement, the noncompliance should then be appropriately documented and corrected. Criteria for determining whether a noncompliance is reportable have been developed by DOE and are detailed in Table 3-1 and 3-2 (Attachment 3). These threshold criteria aid in the identification of noncompliances that, because of their potential or actual adverse impact to the environment or the health and safety of workers or the public, merit additional management evaluation by both the Laboratory and DOE. Nuclear Safety noncompliances meeting or exceeding Table 3-1 or 3-2 reporting thresholds should be reported to the NTS. Noncompliances below the reporting thresholds (i.e., non-NTS reportable noncompliances) should be recorded in ALCATS as AMES LOCAL – Nuclear Safety. Reporting a noncompliance that is below an NTS reporting threshold as an AMES LOCAL – Nuclear Safety into ALCATS also constitutes formal reporting to DOE for enforcement purposes.

It is recognized that some judgment is required for Table 3-1 issues, such as to conclude that a series of noncompliances constitutes a programmatic problem. DOE recommends that where a condition indicates a sufficient concern to warrant some remedial action to correct a common underlying cause or weakness in controls, the condition be considered a programmatic noncompliance and reported to the NTS. Such reporting does not mean the issue is a serious safety noncompliance. However, DOE will expect some level of dialogue through the NTS to assure that proper steps are being taken to address the noncompliance and root causes.

Where there is legitimate disagreement between the Laboratory and DOE over whether a noncompliance should be reported to the NTS, it is recommended that the disagreement be addressed at the appropriate level between DOE and Laboratory management. If agreement cannot be reached, the Laboratory is encouraged to report the noncompliance. The Laboratory may note its disagreement with DOE in the NTS report.

DOE expects the Laboratory to submit noncompliance reports to the NTS without making a detailed evaluation of safety significance, or a prediction of whether DOE would pursue an investigation after receiving the report, as a precondition for reporting.

6.2.3 Worker Safety and Health (WSH) Noncompliance

On February 9, 2006, DOE issued the Worker Safety and Health Program rule, 10 CFR Part 851, which includes in subpart E the enforcement process to be applied to worker safety violations, and, in Appendix B, the enforcement policy for such violations.

The Office of Enforcement issued an [Enforcement Process Overview](#), which describes factors that the Office of Enforcement considers in judging positive steps taken by the Laboratory, as well as the factors affecting the application of enforcement sanctions. If enforcement actions are considered necessary, they are applied in accordance with the provisions of the enforcement policies noted in the Overview. The goal of the Department of Energy's enforcement policies is to improve occupational safety and health for workers at DOE facilities. This goal is the prime consideration in exercising enforcement discretion and in application of mitigation.

The simple occurrence of an event in any of the listed categories is not enough to warrant NTS reporting. Reportable noncompliances require the identification of a 10 CFR Part 851 noncompliance (e.g., 29 CFR Parts 1910 and 1926) in conjunction with the event. The Office of Enforcement is interested only in those portions of the criteria with direct worker safety and health implication. Laboratories identifying a significant worker safety and health noncompliance in association with an event type of category not listed on the table should evaluate the event for NTS reportability.

There are three (3) primary conditions that warrant reporting in the Noncompliance Tracking System (NTS) for violations of worker safety requirements of 10 CFR Part 851 in accordance to the *General Statement of Enforcement Policy* in 10 CFR Part 851, Appendix B. These are:

1. Noncompliances Associated with Occurrences [ORPS] (as defined by DOE [Order 232.2](#) *Occurrence Reporting and Processing of Operations Information*)
2. Management Issues Noncompliances (as defined by the procedures of NTS)
3. Other Significant Conditions

The NTS reporting criterion for worker safety and health noncompliances associated with Occurrences is presented in Table 4-1 of Attachment 4. NTS reporting is not necessary if the event lacks an associated noncompliance.

Programmatic, repetitive, and intentional violations and misrepresentations of worker safety and health noncompliances are to be reported as noted in Table 4-2 of Attachment 4. 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. Repetitive problems are generally two or more events that involve substantially similar conditions, locations, equipment, or individuals. Repetitive issues tend to be narrower in scope than programmatic problems and it is reasonable to assume that they should have been prevented by a laboratory's corrective actions from a previous noncompliance condition. They typically involve similar circumstances or root causes, separated by a period of time that suggests the possibility of a common solution. Intentional violations and misrepresentations may involve the intentional falsification of records. An NTS report is warranted, irrespective of the significance of the activity involving a false record because the act of falsifying the

information is serious and warrants significant DOE and Laboratory management attention. Other significant conditions related to the worker safety and health program are reportable as noted in Table 4-2 of Attachment 4, when the conditions meet the criteria of Severity Level I (serious) violations and high relative risk.

Noncompliances that do not meet the NTS reporting criteria are to be reported in the Ames Laboratory Corrective Action Tracking System (ALCATS).

6.2.4 Incidents of Security Concern

Security incidents include a range of possible actions, inactions, or events that:

- Pose threats to national security interests and/or Departmental assets;
- Create potentially serious or dangerous security situations;
- Have a significant effect on the S&S Program's capability to protect DOE S&S interests;
- Indicate the failure to adhere to security procedures; or
- Illustrate the System is not functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

DOE uses a graded approach for the identification and categorization of security incidents. This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into, and root cause analysis of, specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this policy.

All security incidents must be categorized by significance level and type. When an event is suspected to be a security incident, the Laboratory has 5 calendar days to conduct the preliminary inquiry, to make the initial categorization, and to perform the initial notification(s). Although a maximum of 5 calendar days are provided the Laboratory is required to report the incident as soon as the incident is categorized. If there is still uncertainty at the 5 calendar day mark the incident must be reported as a Category A pending completion of the inquiry process. If the final inquiry reveals additional details and facts, the incident can be re-categorized. As the following table illustrates, there are two levels of significance and three types of incidents.

Significance Levels and Incident Types	
SIGNIFICANCE LEVEL CATEGORY	
A	B
INCIDENT TYPE	
Security Interest (SI)	Security Interest (SI)
Management Interest (MI)	Management Interest (MI)
Procedural Interest (PI)	Procedural Interest (PI)

Category A incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require the notification of the DOE cognizant security office (CSO). The involvement of the DOE CSO for Category A incidents is important for assessing impacts, coordinating with external agencies, and/or notifying DOE senior management.

Category B incidents, which do not meet the Category A criteria, are managed and resolved by the Laboratory; however, this does not preclude the DOE CSO from exercising its oversight responsibilities. The monitoring of Category B incidents by the Laboratory's Safeguards and Security program is essential as it allows the Laboratory to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant incidents.

Incident Criteria

Attachment 3 provides additional criteria and a general framework for distinguishing between Category A and B incidents for these three types of incidents.

Security Interest (SI) This type of incident involves the loss, theft, compromise, or suspected compromise of Departmental assets.

Management Interest (MI) This type of incident does not necessarily involve Departmental assets but is a unique type of incident that may have potential undesirable impacts. MI incidents therefore warrant management notification. MI incidents differ from SI and Procedural Interest (PI) incidents in that the emphasis is on notification; therefore, MI incidents do not require formal inquiry, closure, etc.

Procedural Interest (PI) This type of incident is associated with the failure to adhere to security procedures, and all evidence surrounding the incident suggests the asset was not compromised or the likelihood of compromise is remote.

Safeguards and security events are not reported in ORPS unless they involve other consequences that meet the ORPS reporting criteria presented herein.

AMES LOCAL – Security

Security incidents not meeting the categorization criteria defined above can be categorized as AMES LOCAL – Security at the discretion of the Event Categorization Team. If it is determined that a security incident did not occur and the event is not categorized as an Ames Local event, no further action is required.

6.3 Prompt Notification

Prompt notification by the Facility Manager of DOE officials and in some cases other regulatory entities are detailed in the DOE requirements. The Chief Operations Officer, is the Ames Laboratory Facility Manager, the ESH&A Manager is the Facility Manager Designee, and the F&ES Manager is the Alternate Facility Manager Designee. After categorization, the Facility Manager will proceed with oral and written notification reports according to the notification requirements for the specific Occurrence Category as described in DOE [Order 232.2](#) *Occurrence Reporting and Processing of Operations Information* and [Plan 46300.001](#) *Ames Laboratory Emergency Plan*.

Notification Phone Numbers

Ames Site Office Manager, Cynthia Baebler: cynthia.baebler@ch.doe.gov

Office: 630-252-1563
Home: 630-553-1328
Cell: 630-417-2825
FAX: 630-252-2835

Ames Facility Representative, Eric Dallmann: Eric.Dallmann@ch.doe.gov

Office: 630-252-3340
Home: 630-553-0444
Cell: 630-890-2990
FAX: 630-252-2835

DOE Headquarters (HQ) Operations Center (OC): doehqec@oem.doe.gov

Non-emergency: 202-586-8100
Emergency: 202-586-8100
FAX: 202-586-8485

6.3.1 Occurrence Reports

ORPS Prompt Notification Report (e-mail) Submittal Schedule

Significance Category	Timelines*	Prompt Notification	Final Report Approval	Causal Analysis
Operational Emergencies	30 min (15 if further classified)	Fac. Rep. and DOE HQ	Fac. Rep and Program Manager	Root Cause or Local Procedure
Significance Cat. 1	2 Hours	Fac. Rep. and DOE HQ	Fac. Rep and Program Manager	Root Cause or Local Procedure
Significance Cat. R	NA	NA	Fac. Rep	Root Cause or Local Procedure
Significance Cat. 2	2 Hours	Fac. Rep (DOE HQ when required) †	Fac. Rep.	Apparent Cause or Local Procedure
Significance Cat. 3	2 Hours	Fac. Rep (DOE HQ when required) †	Fac. Manager	Apparent Cause or Local Procedure
Significance Cat. 4	2 Hours (as required)	When required, to Fac. Rep. and DOE HQ †	Per local procedure	Local Procedure

* Categorization Time is from Discovery Date and Time. Prompt Notification is from Categorization Date and Time. Written Notification is from Categorization Date and Time.

† Specific Significance Category 2, 3, and 4 occurrences (identified with an asterisk in Order 232.2 Attachment 2, Reporting Criteria) also require Prompt Notification to the DOE HQ EOC.

6.3.2 Nuclear Safety and Worker Safety and Health (WSH) Noncompliances

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.

6.3.3 Incidents of Security Concern

Each security incident with the exception of incidents of Management Interest (MI) requires categorization, an initial report, an inquiry, and a closure report. The level of detail associated with the latter three steps is graded based on the incident category and the factors (severity, asset, etc.) surrounding the incident. Initial and final reporting is imperative as the DOE has specific responsibilities for notifying and/or coordinating with other agencies, governments, Departmental leadership, and Congress for select incidents. All information generated as part of this process must be protected according to its sensitivity and/or classification determination. The main emphasis for MI incidents is on notification; therefore, investigations and closure reports are not required unless requested by the DOE or the Laboratory's Safeguards and Security Program.

Category A Preliminary Reporting Requirements

- (1) The DOE/NNSA CSO must be notified of all Category A incidents.
- (2) Section 6.3 of this plan contains the notification content and process to include the personnel and organizations identified for notification and any additional and/or specific notification requirements.
- (3) If the incident involves classified matter, the Departmental element with programmatic responsibility for the information must be identified. Notification must include whether origination was by another agency or foreign government and a description of the compromised or suspected compromised information. The following sections of this plan contain additional content considerations for reporting.
- (4) If the site determines that an incident involves the loss, theft, compromise, or suspected compromise of Top Secret, Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Restricted Data (RD) Nuclear Weapon Data, the designee(s) or element with programmatic responsibility of the information must review the incident and render two additional determinations.
 - (a) If it is determined that the incident meets the significant nuclear defense intelligence loss criteria, the appropriate Federal entity(s) after consultation with the Director, Central Intelligence, and the Director, FBI must provide notification to Congress. The notification to Congress must occur within 30 days of categorizing the event as a 50 U.S.C. Section 2656 reportable incident.
 - (b) The element with programmatic responsibility for the information must also determine if the incident warrants a damage assessment. Damage assessments are normally conducted for Top Secret, SCI, SAP, and RD Nuclear Weapon Data classified information; however, they can also be performed for other incidents involving other levels and categories of classified information. In addition to the specific information compromised or suspected of compromise, other considerations for conducting a damage assessment are, but not limited to, if the

incident is associated with a violation of law, if the information was compromised to a wide audience, etc.

Category B Preliminary Reporting Requirements

The notification and reporting of Category B incidents does not extend beyond the Laboratory Safeguards and Security Program and the internal notification process documented in this plan.

Reporting to Cognizant Personnel Security Offices

Security incidents, regardless of category, may impact an individual's eligibility for access to classified information. Therefore, upon closure, the outcome of the inquiry for all security incidents regarding individuals applying for or holding a DOE security clearance must be reported to the personnel security office with cognizance over the individual's access eligibility (as coordinated with Ames Site Office).

Reporting Incidents Associated with Sensitive Programs

Security incidents involving activities associated with sensitive programs must follow the same initial reporting process but may omit details because of programmatic controls. These programs include the SCI Program, SAP Program, the Technical Surveillance Countermeasures (TSCM) Program, the Counterintelligence (CI) Program, or other programs identified by the appropriate Federal designee(s). All subsequent reporting must be handled within the programmatic channels until the inquiry report has been closed within the sensitive program.

Other Multi-Program Reporting

An event that meets the criteria for reporting as an incident of security concern (IOSC) does not negate the responsibility to report through other related reporting chains such as (but not limited to):

- DOE Order 232.2, *Occurrence Reporting and Processing of Operations Information*.
- DOE Order 151.1C, *Comprehensive Emergency Management System*.
- Incidents involving personally identifiable information (PII) must be reported to the Office of Chief Information Officer in accordance with DOE Order 206.1, *Department of Energy Privacy Program*.
- DOE Order 475.1, *Counterintelligence Program*.
- DOE Order 221.1A, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*.
- DOE Manual 205.1-8 Admin Chg 2, *Cyber Security Incident Management Manual*.
- If a compromise of SCI has occurred, the Director, Office of Intelligence and Counterintelligence, must consult with the designated representative of the Director, Central Intelligence and other officials responsible for the information involved.

Special Reporting Situations

Under certain circumstances, related IOSCs that are anticipated to recur over a long period of time may be consolidated from a reporting and documentation perspective. This situation will be handled on a case-by-case basis between the Laboratory's CSO

and the Federal designee(s) with specific reporting plans documented in the approved site IOSC program plan.

6.4 Written Reports

The Event Investigators and Reporters have responsibility for preparation of written reports based on the results of initial information and the investigation.

6.4.1 Occurrence Reports

Written Occurrence Reports shall be prepared as described in DOE [Order 232.2 Occurrence Reporting and Processing of Operations Information](#) and directly entered into the computerized Occurrence Reporting and Processing System (ORPS). Occurrence Reports should document the significance, nature, cause, and the extent of the event or condition, as well as the immediate action taken, the corrective actions, and the lessons learned.

An Update Report must be submitted for all occurrences, with the exception of Significance Category 4 occurrences, if there is any significant and new information about the occurrence. The status of occurrence inquiries, recurring consequences, and the identification of additional component defects must be included in the update.

Occurrence reports containing classified information, Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO), or other controlled information, such as information of counterintelligence concern, must **not** be entered into the ORPS database, but a sanitized information version must be submitted to ORPS. Any information of a potentially controlled nature should be reported to either the Ames Laboratory Safeguards and Security (S&S) Program Director or the Ames Laboratory S&S Manager.

ORPS Written Notification Report Submittal Schedule

(NLT = Not Later Than) (OE = Operational Emergencies) (SC = Safety Significance)

OE	COB next business day (NLT 90 hours)
SC 1	COB next business day (Not to exceed 90 hours)
SC R	COB 2 business days
SC 2	COB next business day
SC 3	COB 2 business days
SC 4	COB 2 business days

Note: Categorization Time is from Discovery Date and Time. Prompt Notification is from Categorization Date and Time. Written Notification is from Categorization Date and Time.

ORPS Update Report and Submittal Schedule

If the required analysis cannot be completed within 45 calendar days, an Update Report, with a detailed explanation of the delay and an estimated date for the Final Report, must be submitted within the 45 days.

OE, SC 1, SC R, SC 2, SC 3 As needed

- Unless necessary to record and explain the event (e.g., suspect/counterfeit items or material), use general descriptions of equipment, procedures, etc., rather than presenting lengthy detailed titles and the numbers and letters assigned to those items.
- Quantify the level of contamination, dose, release, and damage (e.g., estimate the acres of wild land burned) when possible, instead of merely stating a reportable limit was exceeded.
- Use active rather than passive voice whenever possible. For example, write, “*the electrician* severed the conduit” rather than “the conduit was severed.”
- When appropriate for clarification, photos, sketches, and drawings must be maintained with the occurrence report record. In addition, sites are encouraged but not required to make photos, sketches, and drawings available via a Web page, with the Web page address included as a hyperlink in the ORPS report.

6.4.2 Nuclear Safety and Worker Safety and Health (WSH) Noncompliance Reports

Nuclear Safety noncompliance will be reported through the Noncompliance Tracking System (NTS), a centralized database maintained by DOE. The NTS allows laboratories to promptly report noncompliances and take advantage of the Enforcement Policy's mitigation provision.

Laboratories are expected to provide appropriate information in an NTS report such that DOE understands the circumstances of the noncompliance. The “Description of Noncompliance” field in NTS should contain a clear, concise, factual, and objective description of the noncompliance including any impact to the environment, safety, or health of workers or the public. If the information in this field is not clear or if more information is needed, a DOE representative may request additional information. DOE will not take enforcement action based solely on information in the NTS. Laboratories may include their preliminary assessment of a noncompliance's safety significance in the noncompliance condition description portion of an NTS report.

The DOE Office of Enforcement, in coordination with appropriate DOE field elements, reviews noncompliances reported to the NTS. When appropriate, DOE will make an entry to an NTS report to indicate the report has been reviewed and is being closed without any further enforcement action. If enforcement action is to be taken, steps outlined in DOE's operational procedures will be pursued.

6.4.3 Incidents of Security Concern

The final closure report serves as the basis for closing security incidents. The level of detail provided in the report will vary on the category of the incident. The report content and closing procedures will, at a minimum, include:

- a. The final closure report for Category A incidents must be submitted within 90 calendar days of preliminary incident notification.
- b. Category A incidents must be closed via (SSIMS) [a DOE tracking system for security issues].
- c. Category B incidents can be closed using SSIMS or ALCATS. The incident notification and the inquiry report must contain supporting documentation of

factors used to determine that the likelihood of compromise and/or the potential for damage to national security is remote (e.g., failure to secure a document in a security container; however, multiple physical protection layers exist preventing unauthorized disclosure). This documentation provides the basis for making a statement that the circumstances surrounding the security incident are such that the possibility of damage to the national security can be discounted.

- d. All supporting documentation must be retained with the final report. For Category A incidents, at a minimum, the documentation must include:
- (1) Material and relevant information (i.e., the “who, what, when, and where”) that was not included in the initial report;
 - (2) The name of the individual(s) who was primarily responsible for the incident, including a record of prior incidents for which the individual had been determined responsible;
 - (3) If applicable, documentation noting if the unauthorized disclosure was willful (i.e., intentional vs. inadvertent disclosure);
 - (4) A statement of the corrective actions taken to preclude recurrence and the disciplinary action taken against the responsible individual(s), if any;
 - (5) If applicable, specific reasons for reaching the conclusion that the theft, loss, compromise, or suspected compromise, did not occur or that the likelihood of compromise was remote;
 - (6) Identification of any collateral (i.e., extent of condition) effect to other programs or security interests;
 - (7) If the incident involves the compromise or suspected compromise of information, the extent of the dissemination (e.g., number of individuals and their citizenship; global disclosure via cyber mediums, open source publication; etc.) must be identified; and
 - (8) Identification of specific impacts (i.e., degree of damage, reference 32 CFR Part 2001.48) of the incident to the Department and/or national security. Whenever an incident involves classified matter or interests of more than one Government agency, each agency is responsible for conducting the damage assessment resulting from its compromised matter.

6.5 Investigation and Analysis

The Event Investigators and Reporters have responsibility for investigation of events and the analysis of information for the purpose of improving operations through determination of the causes of events and the appropriateness of corrective actions. Analyzing occurrence reports promotes the values and concepts of a learning organization envisioned in the Integrated Safety Management (ISM) Feedback and Improvement function, including performance monitoring; identifying deviations or questionable conditions; self-assessing; and using quality analysis to improve.

A graded approach, based on the significance, severity, or risk associated with the event or condition is utilized when determining the level of detail required for the investigation and causal analysis of an event. Investigation and analysis of events reported as Occurrences, NTS Nuclear Safety Noncompliances, Worker Safety and health (WSH)

Noncompliances, and Security Concerns may be performed according to the guidance using System Improvements' TapRoot® Causal Process. It is believed that most investigations and analyses should be completed within 45 days of determining that a noncompliance exists.

All information generated as part of the investigation and analysis process must be protected according to its sensitivity and/or classification determination.

Inquiry officials may be either Federal or laboratory employees and must have previous investigative experience or Departmental inquiry official training. Ames Laboratory does not maintain capability for an inquiry official; therefore if the need arises for an inquiry official, the Ames laboratory will request assistance through the Ames Site Office.

Reportable Event Investigation and Analysis Process

The following actions are performed as part of the Investigation and Analysis of Reportable Events:

1. Collect data as soon as possible following the event to ensure all relevant information associated with the event is identified. Investigators are not authorized to detain individuals for interviews or to obtain sworn statements; however, they may conduct consensual interviews and request employees to prepare summaries of their observations.
 - Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc. The needed information includes conditions before, during, and after the event; personnel involvement; environmental factors and other information having relevance to the event. Conduct interviews to obtain additional information regarding the event. Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, read outs from monitoring equipment, etc.). Ensure physical evidence is protected and controlled and a chain-of-custody is maintained.
 - Reconstruct the event to the greatest extent possible using collected information and other evidence and develop a SnapCharT™, including a chronological sequence of events that describes the action preceding and following the event and the identification of persons associated with the event.
2. Analyze and evaluate the event information and reconstruction to determine which systems and functions performed correctly or failed to perform as intended. Make sure the information and chronology describe the incident completely and accurately. Collect additional data and reconstruct the incident if more information is required. Identify any collateral impact with other programs. Identify the factors that caused the event, define these as causal factors, and document potential causal factors.
3. Analyze each causal factor's root cause by application of TapRoot® Root Cause Tree®.
4. Analyze each root cause's generic cause by application of TapRoot® Root Cause Tree®.

5. Utilize the output of TapRoot® Root Cause Tree® and guidance (from Fluor Fernald *Guidance for Completing Cause Fields of Occurrence Reports*) to cross code TapRoot® root causes to the apparent causes of the Causal Analysis Tree (DOE [Order 232.2](#) (Attachment 5)). The Causal Analysis Tree will delineate specific designations of cause such as:
 1. Design/Engineering problem,
 2. Equipment/Materials problem,
 3. Human Performance LTA (less than adequate),
 4. Management Problem,
 5. Communications LTA (less than adequate),
 6. Training Deficiency,
 7. Other Problems
6. Develop a summary of output of the TapRoot® Causal Process and Apparent Causes from the DOE Causal Analysis Tree. A description should be included for each identified cause, including a brief discussion to clearly link the cause to the event. In addition to determining the causes of the occurrence, any weaknesses in implementation of the facility's ISMS must be identified.
7. Evaluate proposed Corrective Actions and ensure appropriateness of proposed and additional corrective actions. Utilize [Procedure 10200.039](#) *Corrective Action Development, Tracking, and Verification* for additional guidance related to corrective actions.
8. Ensure Lessons Learned are appropriate. Utilize [Plan 10201.020](#) *Operating Experiences and Lessons Learned Program* for additional guidance related to corrective actions.
9. Prepare Event Investigation and Analysis Report. At a minimum the report must describe the conduct and results of the investigation and include the following information for the event to be closed.
 - **Executive Summary.**
 - **Narrative**, which must include the following.
 - **When:** The date and time of event discovery, any notifications, the investigation and analysis, and other time-related actions pertaining to the event.
 - **Where:** All data pertinent to the location of an event, including the facility name and the Safeguards and Security Information Management System facility code (0033), building/room numbers, and other identifying information as appropriate.
 - **What:** A complete discussion of the facts and circumstances surrounding the event, including a description of all supporting information, such as the following:
 - a) detailed description of the event;
 - b) identification of all personnel involved in the event and when they were notified, including those associated with the investigation and analysis process;

- c) identification of the causes for the event (direct and contributing factors), descriptions of mitigating or aggravating factors that may reduce or increase the impact of the event;
- d) descriptions of the actions that precipitated the event;
- e) descriptions of all physical evidence, including all records/documents reviewed (e.g., training records, policy/procedures, personnel security files);
- f) results of any interviews performed;
- g) descriptions of actions taken to minimize vulnerabilities created by the event; and
- o **Conclusions:** An investigation's conclusion and the basis/facts that support the conclusion.
 - a) Given the facts determined through the investigation, the conclusion of the final report must address the potential risk to the event based upon a subjective analysis of the facts and circumstances surrounding the event.
 - b) The final report must also identify the management officials responsible for corrective actions.
- **Attachments**
 - o Pictures and copies of evidence,
 - o Training records of individuals associated with the event,
 - o Interview statements, etc.

The following must be included as attachments to the report of inquiry:

- A copy of the documentation appointing the inquiry official;
- A copy of any signed statements of involved individuals;
- A description of the compromised information (as appropriate);

AMES LOCAL Event Investigation and Analysis Process

AMES LOCAL events are investigated and analyzed according to a simplified process patterned after the Reportable Event Investigation and Analysis Process.

- Steps 1 and 2 will be performed.
- Basic cause categories will be determined by [Form 10200.153](#) *Basic Cause Category Determination*.
- Steps 7, 8, and 9 will be performed.

6.6 Approval of Written Initial, Updates, and Final Reports

The ESH&A Manager, the ESH&A Assistant Manager or the acting ESH&A Manager has responsibility for the approval of the written initial, updates, and final reports based on the report content requirements and guidance of the specific reporting program.

6.7 Identifying Trends and Recurring Events

The Event Screening Team has responsibility for quarterly performance analysis of Ames Laboratory information and events for identification of potential recurring events

and must consider at least the previous 12-months. The performance analysis includes review of events reported as Occurrences, Nuclear Safety Noncompliances, Security Concerns, and Ames Local events, as well as information from a variety of sources such as the sources utilized for event screening. Information from screening activities is used to produce a Quarterly Performance Analysis Review Report with a list of potential recurring events. The report is shared with the Event Categorization Team and the Facility Manager. Events identified as potentially recurring are submitted to the Event Categorization Team for review and, if warranted, categorized as a recurring occurrence and submitted as a new Occurrence Report.

Also, an annual trend analysis is performed according to [Procedure 10200.041](#), *Trend Analysis of ES&H Concerns*.

6.8 Corrective Action Development, Tracking and Verification

The responsibilities for development, tracking and verification of closure for corrective actions related to reportable events are outlined in [Procedure 10200.039](#) *Corrective Action Development, Tracking, and Verification*. Line management has responsibility for the development of corrective actions, with consensus of the issue identifier and ESH&A. ESH&A has responsibility for tracking corrective actions. Line management and ESH&A have responsibility for verification of completion and effectiveness of corrective actions.

6.8.1 Occurrences Reports

A complete description of the corrective actions and the target date when completion of the corrective action is anticipated should be entered into ORPS. A complete list of corrective actions should be included in the report to ensure it can stand on its own (readers do not have to search for other reports, etc.).

6.8.2 Nuclear Safety and Worker Safety and Health (WSH) Noncompliances

Laboratories 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. The level of detail of the 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. DOE expects the 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 system, the Laboratory should mark the report “Completed” or “Closed,” as applicable.

At this point, the cognizant DOE Field Element validates 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 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 (DOE-HSS) 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.

A noncompliance condition should be corrected for the facility or radiological activity where the noncompliance occurred, as well as for any other facility or activity under Laboratory management where Price-Anderson is applicable. Corrective actions are not required to be approved by DOE. DOE may, however, be involved in the selection of a corrective action and the timing of work activities if there will be a significant commitment of funds or a request for additional funds to correct the noncompliance. Under normal circumstances, DOE field elements will have this responsibility.

6.8.3 Incidents of Security Concern

Corrective actions identified in response to a security incident must be documented. Whenever possible, the responsibility for a security incident should be assigned to an individual rather than to a position or office. When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to a security incident, responsibility must be assigned to that official.

6.9 Other Administrative Actions

Persons deemed responsible for events, especially security incidents, may, at management's discretion, be issued a security infraction or have disciplinary actions taken in accordance with DOE and Ames Laboratory policies and practices. Any administrative actions imposed as a result of a security incident on an uncleared individual must be communicated to the respective personal identity verification office for Homeland Security Presidential Directive-12 (HSPD-12).

6.10 Lessons Learned

Lessons Learned related to reportable events are developed and disseminated within the Laboratory and DOE as appropriate by the operating experiences program coordinator; [Plan 10200.020](#) *Operating Experiences and Lessons Learned Program*.

7.0 Additional Information

- DOE [Order 232.2](#) *Occurrence Reporting and Processing of Operations Information*
- [10 CFR Part 851](#) *Worker Safety and Health Program*
- [10 CFR Part 850](#) *Chronic Beryllium Disease Prevention Program*
- [10 CFR Part 835](#) *Occupational Radiation Protection*
- [10 CFR Part 830](#) *Nuclear Safety Management*
- [10 CFR Part 820](#) *Procedural Rules for DOE Nuclear Activities*
- DOE [Order 470.4B](#) *Admin. Chg. 1 Safeguards and Security Program*
- DOE Office of Enforcement, [Enforcement Process Overview](#)
- DOE Office of Enforcement, [Enforcement Coordinator Handbook](#)
- DOE [Order 151.1C](#) *Comprehensive Emergency Management System*

Attachment 1
Occurrence Reporting Criteria

The following pages are taken from the DOE [Order 232.2](#) Attachment 2, Occurrence Reporting Criteria.

Attachment 2
Worker Safety and Health Noncompliance Reporting Criteria
Nuclear Safety Noncompliance Reporting Criteria

The following pages are taken from section III of the DOE Office of Enforcement, [Enforcement Coordinator Handbook](#), August 2012.

Attachment 3
Incidents of Security Concern Reporting Criteria

The following pages are taken from DOE [Order 470.4B](#) Admin. Chg. 1 *Safeguards and Security Program (Attachment 5, Incidents of Security Concern)*.