Office of Enterprise Assessments
Lessons Learned from Targeted Reviews of the Management of Safety Systems at U.S. Department of Energy Nuclear Facilities

April 2016

Office of Nuclear Safety and Environmental Assessments
Office of Environment, Safety and Health Assessments
Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

Acronyms

ATR	Advanced Test Reactor
CFR	Code of Federal Regulations
CRAD	Criteria and Review Approach Document
CSE	Cognizant System Engineer
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
EA	DOE Office of Enterprise Assessments
EM	DOE Office of Environmental Management
FY	Fiscal Year
INPO	Institute of Nuclear Power Operations
ISM	Integrated Safety Management
NTS	Noncompliance Tracking System
ORPS	Occurrence Reporting and Processing System
SMP	Safety Management Program
SSO	Safety System Oversight
TSR	Technical Safety Requirement
WIPP	Waste Isolation Pilot Plant

Office of Enterprise Assessments
Lessons Learned from Targeted Reviews of the Management of Safety Systems at U.S. Department of Energy Nuclear Facilities

EXECUTIVE SUMMARY

The U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments, within the Office of Enterprise Assessments (EA), conducted independent safety system reviews at 11 selected DOE nuclear facilities between 2013 and 2015. The purpose of the reviews was to assess the effectiveness of line management of safety systems at DOE nuclear facilities. The nuclear facilities were selected based on risk and included facilities under the direction of every DOE program office managing nuclear facilities. The reviews were conducted by selecting a safety system and reviewing the system against DOE requirements in the areas of maintenance, surveillance testing, operations, cognizant system engineer program, safety system oversight, and feedback and improvement. The objective of each review was to determine whether the safety systems were operated and maintained in such a manner as to ensure the safety system can reliably perform its intended function of protecting workers, the public, and environment from hazards during upset conditions. Reports documenting an overall assessment, including specific strengths and deficiencies, were provided to site managers for each review. This report is not intended to provide each strength and deficiency but rather highlight best practices, as well as, weaknesses that were evident at multiple facilities in support of organizational learning.

The results from the 2013 – 2015 reviews are based on direct observation of system condition and a sample of maintenance, testing, and operations activities from each facility, as well as documentation and records of related programs and processes. EA found at every facility reviewed that the safety systems were operated and maintained such that the selected safety systems could perform intended safety functions. Additionally, surveillance and testing activities at most facilities were performed in accordance with technical safety requirement surveillance requirements and specific administrative controls. Overall, EA found that contractor and DOE organizations are properly managing safety systems consistent with DOE directives and approved safety basis documents.

EA identified several best practices at one or more facilities. Some facilities are making full use of Institute for Nuclear Power Operations resources to improve contractor management and nuclear safety programs, and at one facility, management requires use of human performance error reduction techniques for all maintenance activities to make maintenance activities safer and to reduce the likelihood of human error.

However, a few common areas of weakness exist, including procedure use and adherence, implementation of the cognizant system engineer program, and the effectiveness of performance measures to affect continuous improvement in nuclear safety performance. These areas of weakness are similar to those identified in past independent oversight reviews. While some improvements are evident, the results of the recent reviews indicate that corrective actions have not been fully effective in resolving previously identified weaknesses in some areas. Examples of more recent weaknesses identified by EA at multiple sites are:

- Procedures were not always performed as written or not up-to-date and/or the procedure use category was not properly identified as required to be in-hand for performance.

- At the facilities where configuration management processes were evaluated in detail, engineering processes in some cases did not ensure system configuration was maintained during plant modifications, and unverified assumptions in safety calculations were not always tracked and resolved.

- At some sites cognizant system engineer (CSE) system assessments and walkdowns were performed infrequently, lacked detail, were not comprehensive, and were not well documented. DOE and contractor management rely on these activities to identify safety system conditions affecting performance to ensure reliability of safety functions.

- Performance measures were not consistently effective in improving performance, including missing or ineffective goals, missing analysis for adverse trends, and misuse of certain measures to justify personnel resources rather than driving continuous improvement.

- Most facilities did not have measures in place to ensure that nuclear facility operators were adequately informed on changes in site systems (e.g., compressed air, steam, electrical distribution) also known as interrelated processes that could impact nuclear safety systems. The remaining facilities reviewed did not meet the expectations for control of interrelated processes.

EA reviewed 2015 data from the DOE Occurrence Reporting and Processing System, which contains reportable events, and the Noncompliance Tracking System, which reports violations of DOE nuclear safety rules, as part of developing this report to determine if themes identified in reviews performed between 2013 and 2015 were consistent with nuclear safety occurrences and violations reported from around the complex. The 2014 Waste Isolation Pilot Plant fire and radiological events accident investigation reports were also reviewed against the themes of this report. The data and accident investigations showed that procedure use and adherence, configuration management, and feedback and improvement were important contributors to nuclear safety issues in 2015 and the Waste Isolation Pilot Plant events of 2014, which was consistent with this lessons learned report.

EA also identified a few aspects of DOE directives and guidance documents that could be revised to improve clarity. For example, limited guidance for implementation of the CSE program likely contributed to the CSE performance issue discussed above. In addition, a minor revision to DOE Order 422.1, *Conduct of Operations*, Section 2.m, *Control of Interrelated Processes*, or other guidance document to state that the section applies to both facility and site infrastructure operators would likely mitigate the control of interrelated processes deficiency stated above.

Office of Enterprise Assessments
Lessons Learned from Targeted Reviews of the Management of Safety Systems at U.S. Department of Energy Nuclear Facilities

1.0 INTRODUCTION

The U.S. Department of Energy (DOE) Office of Enterprise Assessments (EA) manages the Department's independent oversight program. EA's oversight program is designed to enhance DOE safety and security programs by providing the Secretary and Deputy Secretary of Energy, Under Secretaries of Energy, other DOE managers, senior contractor managers, Congress, and other stakeholders with an independent evaluation of the adequacy of DOE policy and requirements, and the effectiveness of DOE and contractor line management performance and risk management in safety and security and other critical functions as directed by the Secretary. The DOE independent oversight program is described in and governed by DOE Order 227.1, *Independent Oversight Program*, and EA implements the program through a comprehensive set of internal protocols, operating practices, assessment guides, and process guides.

EA's predecessor organization identified management of safety systems as a targeted assessment area beginning in 2013 in a memorandum to DOE senior line management, *Independent Oversight of Nuclear Safety – Targeted Review Areas starting in FY 2013*, dated November 6, 2012. Between 2013 and 2015, independent review teams conducted targeted reviews of the management of safety systems (at 11 DOE nuclear facilities under the line management responsibility of 11 different DOE field elements) and corresponding DOE Headquarters program offices.

1.1 Report Scope and Methodology

The EA targeted reviews focused on the effectiveness of safety system management across the DOE complex and included evaluation of elements key to ensuring that safety systems will reliably perform intended safety functions when required. These key elements were maintenance, surveillance testing, operations, cognizant system engineers (CSEs), safety system oversight (SSO), and feedback and improvement implementation. EA conducted the reviews at the facility level by selecting a safety system(s) and performing a vertical slice review. Contractor and DOE feedback and improvement processes were evaluated to determine whether these process were effective in improving system performance and reliability. The reviews, based on a sampling of data, were not intended to represent a full programmatic review of site programs and processes. The scope of the targeted reviews did not include the adequacy of the documented safety analysis (DSA) and other safety basis documents but rather evaluated the implementation of the safety basis.

EA also reviewed 2015 data from the DOE Occurrence Reporting and Processing System (ORPS), which contains reportable events, 2013 through 2015 data from the Non-compliance Tracking System (NTS), which reports violations of DOE nuclear safety rules, and 2010 through 2015 data from the DOE Pilot Nuclear Safety Information Dashboard, which trends information contained in the ORPS data base related to nuclear safety, as part of developing this report to determine if themes identified in reviews performed between 2013 and 2015 were consistent with nuclear safety occurrences and violations reported from around the complex. The 2014 Waste Isolation Pilot Plant fire and radiological events accident investigation reports were also reviewed against the themes of this report.

EA selected the nuclear facilities identified for review based on the level of risk. The sites and facilities selected included those from all DOE program offices who have nuclear facilities to ensure an acceptable cross-section of DOE nuclear facilities were sampled. The sites and facilities reviewed, along with

associated contractors, local DOE offices and DOE Headquarters program offices, are listed in Table 1 below.

Table 1. Nuclear Facilities, Operator, DOE Program Offices, and Local DOE Offices in the Review

Review Site	Facilities Reviewed	Operator	DOE Headquarters Program Office	DOE Field Element
Hanford Site	Hanford Tank Farms	Washington River Protection Solutions, LLC	Office of Environmental Management	Office of River Protection
Oak Ridge National Laboratory	Transuranic Waste Processing Center	Wastren Advantage, Inc.	Office of Environmental Management	Oak Ridge Environmental Management Site Office
Pantex Plant	Bays and Cells	Babcock and Wilcox Technical Services Pantex, LLC	National Nuclear Security Administration	National Nuclear Security Administration Production Office
Nevada Nuclear Security Site	Device Assembly Facility	National Security Technologies, LLC	National Nuclear Security Administration	Nevada Field Office
Hanford Site	Plutonium Finishing Plant	CH2M Hill Plateau Remediation Company	Office of Environmental Management	Richland Operations Office
Lawrence Livermore National Laboratory	Plutonium Facility	Lawrence Livermore National Security, LLC	National Nuclear Security Administration	Livermore Field Office
Los Alamos National Laboratory	Technical Area 55 Plutonium Facility	Los Alamos National Security, LLC	National Nuclear Security Administration	Los Alamos Field Office
Oak Ridge National Laboratory	Irradiated Fuels Examination Laboratory	UT-Battelle, LLC	Office of Science	Oak Ridge National Laboratory Site Office
Pacific Northwest National Laboratory	Radiochemical Processing Laboratory	Battelle Memorial Institute	Office of Science	Pacific Northwest Site Office
Idaho National Laboratory	Advanced Test Reactor	Battelle Energy Alliance, LLC	Office of Nuclear Energy	Idaho Operations Office
Y-12 National Security Complex	High Enriched Uranium Material Facility	Consolidated Nuclear Security, LLC	National Nuclear Security Administration	National Nuclear Security Administration Production Office

The scope of the targeted reviews included criteria from criteria and review approach document (CRAD) 45-11, Rev. 3, *Safety Systems Inspection Criteria, Approach, and Lines of Inquiry*, which is based on the requirements of DOE Order 226.1B, *Implementation of DOE Oversight Policy*, DOE Order 420.1B or 1C, *Facility Safety*, DOE Order 422.1, *Conduct of Operations*, and DOE Order 433.1B, *Maintenance Management Program for DOE Nuclear Facilities.* EA used these criteria to determine whether the policies, procedures, and operational performance met DOE's objectives for operating and maintaining safety systems in a condition and configuration that ensures reliability of safety functions. The review took into consideration that a few DOE sites were contractually bound to DOE Order 420.1B, while other sites have implemented the new DOE Order 420.1C.

EA's predecessor issued an independent oversight report in June 2008 entitled, *Annual Report for Calendar Year 2007 on Status of Implementation of Integrated Safety Management at the Department of Energy*, which addressed some of the same areas as this lessons learned report. Specifically, the 2008 integrated safety management (ISM) report stated that essential systems at DOE nuclear facilities were in good material condition and operators were typically well trained, experienced, and knowledgeable. The 2008 report also identified some weaknesses that align with each area evaluated within the scope of the 2013 – 2015 management of safety systems reviews. EA compared the results of the current reviews with those presented in the 2008 ISM report. The results are presented in the results discussion of applicable subsections of this report.

1.2 Requirements and Guidance

DOE requires that safety systems at its nuclear facilities be operated and maintained to ensure that the systems can reliably perform intended functions when called upon. These requirements, which flow down from Title 10, Subpart 830 of the United States Code of Federal Regulations (10 CFR 830), *Nuclear Safety Management*, are contained in various DOE orders, including DOE Order 420.1B (or 1C), *Facility Safety*, DOE Order 422.1, *Conduct of Operations*, and DOE Order 433.1B, *Maintenance Management for DOE Nuclear Facilities*. In addition, DOE line management oversight (in accordance with DOE Order 226.1B, *Implementation of DOE Oversight Policy)* is required of DOE contractors operating DOE nuclear facilities to ensure, in part, that safety systems will be available if needed.

1.3 Report Organization

Section 2 of this report provides a consolidated assessment based on the results from all the individual safety system reviews. In addition, Section 2 includes data analysis from the DOE occurrence reporting and nuclear enforcement databases. Section 3 of this report identifies best practices that EA observed during the targeted reviews; Appendix A lists the members of the EA review team, the Quality Review Board, and EA management responsible for this report; and Appendix B provides recommended actions for consideration as potential improvements at all sites.

2.0 OVERALL ASSESSMENT

2.1 Maintenance

Results: For the facilities and systems reviewed, acceptable maintenance processes are in place for corrective, preventive, and predictive maintenance, and the processes are consistent with the systems' safety designation. EA observed that the selected safety systems were fully operable, with little or no out-of-service equipment and no active temporary modifications. Also, nearly all system instrumentation requiring calibration was current. The Nuclear Maintenance Management Program and implementing procedures generally meet the requirements of DOE Orders 433.1B and are adequate to maintain

acceptable levels of safety system operability, availability, and reliability. Overall, observed performance and reviewed procedures, work documents, and records demonstrated acceptable maintenance programs with few significant performance problems. Additionally, EA found that the procurement of safety system parts and programs to ensure quality and guard against the installation of suspect/counterfeit items at almost every site was acceptable with few issues.

Although EA identified few significant performance problems, EA identified several weaknesses at multiple sites in areas of work package records and execution, maintenance performance measures, and failure to identify maintenance as a safety management program (SMP), as discussed below.

Examples of procedure non-compliance were identified where preventive maintenance was not performed as specified in the work steps of the package. In these cases, the work steps were incorrect and instead of stopping and revising the work package, workers performed the maintenance in the manner they thought to be correct.

Although most facilities reviewed had maintenance performance measures, the measures were not effective in identifying maintenance issues requiring corrective actions and lessons learned, counter to DOE Order 433.1B requirements. Performance measures are intended to result in improved performance. Some of the measures were not appropriately measuring areas of the maintenance program. For example, a maintenance backlog performance measure was used to justify craft headcount rather than to reduce the backlog of maintenance on important facility equipment. Other measures did not have goals that were challenging. Furthermore, others had no analysis performed nor action taken for adverse trends reflected in the indicator data. (See Section 2.6.)

DOE Order 433.1B defines the SMP required by 10 CFR 830.204(b)(5) for maintenance and the reliable performance of structures, systems and components that are part of the safety basis for hazard category 1, 2, and 3 DOE nuclear facilities. Five of 11 facilities reviewed did not recognize maintenance as an SMP and did not perform management and independent assessments of the maintenance program.

Certain aspects of maintenance programs were also identified in the June 2008 report as areas of weakness. The 2008 report identified that maintenance implementation plans were not adequate to ensure that replacement parts met specifications. The report also identified that tracking and trending of maintenance information could be improved. EA found that the facilities reviewed between 2013 and 2015 had Nuclear Maintenance Management Programs that, overall, complied with DOE Order 433.1B, *Maintenance Management Program for DOE Nuclear Facilities*, including requirements for the procurement of safety system replacement parts. However, tracking and trending (i.e., performance measures) of maintenance information remains an area of weakness.

2.2 Surveillance and Testing

Results: Overall, surveillance and testing activities for the selected safety systems are properly performed in accordance with facility technical safety requirements (TSR) surveillance requirements. Except for a few isolated instances, surveillance and testing of the systems reviewed demonstrates that the system can accomplish its safety functions and continues to meet applicable system requirements and performance criteria.

Overall, the 2008 report found acceptable performance in the area of surveillance testing. However, the report found weaknesses at some sites related to the adequacy of surveillance test procedures. Although isolated inadequacies were identified with the surveillance test procedures at some facilities reviewed between 2013 and 2015, the quality of surveillance test procedures at most facilities has improved since 2008.

2.3 Operations

Results: Operation of safety systems for the facilities reviewed is generally conducted in a manner that ensures the availability of the selected safety systems to perform their intended safety functions when required. Most procedures are technically adequate to achieve required system performance. Operator training programs are acceptable and operators are knowledgeable of safety system function and operation. Shift routines, operating practices, and detailed procedures generally provide operations personnel with a current operational awareness and verification of normal configuration of the selected safety systems.

However, EA observed weaknesses in conduct of operations at several facilities, including a few instances where procedures were not followed as written or not up to date, and/or the procedure use category was not properly identified for procedures that must be in-hand in order to be followed consistently and accurately. Other weaknesses included inadequate shift turnover processes and performance, lack of formal communication with repeat-backs when communicating important plant information between operations personnel and, in a few cases, conduct of operations requirements treated as guidance rather than requirements for conducting operations. (See Section 2.7.)

EA observed weaknesses at all but one of the reviewed facilities regarding control of interrelated processes. Interrelated processes (e.g., water for fire protection, steam, electrical distribution) are used by the facility but are under the control of either an entity within the contractor organization or a group from another company. When DOE Order 422.1, *Conduct of Operations*, was issued in 2010 replacing DOE Order 5480.19, three requirements were introduced in Section 2.m, *Control of Interrelated Processes*: definition of responsibilities, training/qualification, and communication. The intent of Section 2.m is to establish responsibilities for both facility operators and the personnel who operate/control interrelated processes to ensure that impacts to facilities are minimized. Some facilities addressed responsibilities and training for interrelated processes for facility operators, but only one facility also addressed the organizations operating the interrelated processes. Most facilities did not establish communication processes for timely notification between groups for anomalies with interrelated processes. During an EA observation of a safety system functional test at one facility, facility operators noticed that, although stack flow was within acceptable limits, the flows did not return to expected levels following completion of return to normal steps in the surveillance test. Stack flow was provided by a different contractor through exhaust fans and a stack that is shared by multiple nuclear facilities. The facility personnel subsequently contacted the EM contractor and learned that an exhaust fan had failed and an alternate fan, which provided a different flow rate, was brought on line. This fan change occurred during the conduct of the functional test, which changed the functional test parameters without the knowledge of the facility personnel, and emphasizes the importance of DOE Order 422.1, Section 2.m, requirements for controlling interrelated processes.

Some of the observed DOE Order 422.1, Section 2.m, implementation weaknesses resulted from vague wording in Section 2.m. For example, the section refers to "The operator" and does not specify that this term was meant to apply to operators of interrelated processes as well as facility operators. Additionally, the DOE standard referenced in Section 2.m (DOE-STD-1037-93, *Guide to Good Practices for Operations Aspects of Unique Processes*, June 1993) does not adequately address interrelated processes. [Policy Inadequacy] Other than mentioning interrelated processes one time, the standard does not address any of the requirements in Section 2.m. In a related observation, most of the standards referenced in DOE Order 422.1 have not been revised to reflect updated Order requirements, even though the Order was revised in 2010.

Overall, the 2008 report found acceptable performance in the area of operations. However, the report found weaknesses at some sites related to the integration of operations with other nuclear safety

programs, such as the safety basis and CSE programs. No weaknesses were noted in the 2013 – 2015 reviews related to integration of operations with other nuclear safety programs.

Although most incumbent operators observed possess the knowledge to perform their assigned duties, EA observed inadequate continuing training for operators as an area of weakness at several sites. In addition, some operator training programs did not meet the systematic approach to training described in DOE Order 426.2, *Personnel Selection, Training, Qualification, and Certification Requirements for DOE Nuclear Facilities*. The weaknesses were mainly in the area of training documentation, including how the program was developed using the elements of the systematic approach to training (such as training needs analysis, task lists, and task-to-training matrices).

2.4 Cognizant System Engineer and Configuration Management

Results: At the facilities assessed CSE programs have been established. Safety systems requiring CSE coverage have been identified and CSEs assigned. CSEs are responsible for providing support to operations and maintenance, and for configuration management of their assigned system(s). However, some specific weaknesses detract from the effectiveness of the program.

Some facilities reviewed did not have requirements for routine safety system monitoring, including system walkdowns and system assessments. For other facilities, walkdowns and assessment were not performed frequently enough to effectively and consistently monitor ongoing health of active safety systems. Additionally, CSEs did not adequately document their activities at many of the facilities reviewed, creating gaps in evaluating system performance trends and potential safety system reliability issues. At one facility, implementation of a recommended preventive maintenance activity identified during a system walkdown was overlooked because the CSE was not required to document and follow-up on the results of system walkdowns, and, at another facility, documentation of an annual system walkdown did not include all accessible portions of a system resulting in overlooking inoperable valves in the system. This lack of documentation also limits knowledge transfer to new CSEs following attrition. Several facilities did not have fully qualified CSEs for all safety systems because of attrition and the time required to qualify on a given safety system.

EA also identified instances of inadequate CSE training at several facilities, including CSE qualification processes that did not include safety system specific training and proof of completed training not available in the training records.

EA reviewed the CSE role in the configuration management process for assigned systems at each site. In addition, at three sites, EA conducted a more detailed review of the configuration management program as part of the reviews. CSE involvement in the area of configuration management is adequate, and overall, the implementation of the configuration management programs is acceptable at the reviewed sites. However, EA observed weaknesses in engineering processes for maintaining system configuration during plant modifications, tracking and resolution of unverified assumptions in safety calculations, and control of quality assurance records. Additionally, a weakness was identified regarding the scope and frequency of configuration management program assessments. (See Section 2.7.)

In the June 2008 report, most CSE programs were not fully implemented and processes governing CSE responsibilities and functions had not been adequately defined and fully implemented in such areas as performing system assessments, performing periodic system reviews and walkdowns, trending system performance, evaluating system reliability and maintainability, and preparing system health reports. Although most of the 11 sites reviewed between 2013 and 2015 had implemented the CSE requirements in DOE Order 420.1B or 1C, some CSE responsibilities at several sites reviewed were also not well defined, and the effectiveness of performing these duties varied significantly, as discussed above.

2.5 Safety System Oversight

Results: The DOE field elements at 10 of the 11 sites reviewed have established and implemented effective SSO programs. The remaining site (an Office of Science laboratory) is not required to follow the requirements for implementing an SSO program because DOE Order 426.1, *Federal Technical Capability*, only applies to defense nuclear facilities. Although also not required, the Idaho Operations Office has voluntarily implemented the DOE SSO function for both its EM and Office of Nuclear Energy nuclear facilities.

Overall, the DOE field elements with SSO programs have adequately trained and qualified SSO staff and have acceptable implementing procedures. The SSOs interviewed and observed were knowledgeable of the status and performance of assigned safety systems and generally provided adequate oversight of associated contractor CSEs. However, at several sites, EA observed two recurring weaknesses.

First, DOE line management within several field elements was not conducting periodic assessments of SSO program effectiveness as required by DOE Order 426.1B. Second, at multiple sites reviewed, significant amounts of time had elapsed (more than 1 year) without scheduling and performing formal SSO assessments of contractor performance.

The 2008 report indicated that DOE SSO programs were an appropriate measure for improving nuclear safety at DOE sites, but the expected benefits had yet to be fully realized. Of the sites reviewed as part of the scope of the 2008 report, only one DOE field element had an acceptable SSO program. Conversely, most field elements reviewed between 2013 and 2015 showed effective implementation of the SSO function.

2.6 Feedback and Improvement

Results: The reviewed contractor organizations have generally established and implemented feedback and improvement programs and processes necessary for evaluation of nuclear safety systems and performance. Feedback and improvement processes are described in program description documents and procedures. Many assessment and review activities are planned and scheduled to evaluate safety system programs and performance at respective DOE nuclear facilities using a structured process, and these activities are usually performed and documented as scheduled and in a generally comprehensive manner. Related safety issues are identified and appropriately placed into an issues management process. Incidents and events at most nuclear facilities, including those below DOE occurrence reporting thresholds, are documented and investigated, and corrective actions are identified and implemented. Internal lessons learned are identified and documented.

However, EA observed weaknesses in several areas of feedback and improvement, including the conduct of assessments, investigation of events, and performance measures. The scope of contractor management and independent assessments at several sites did not include all nuclear safety related areas (e.g., system engineering, configuration management, and technical procedures). At some facilities, the contractor processes for conducting assessments did not ensure that nuclear safety related topics were rigorously assessed and issues entered into the issues management system. EA identified the lack of prompt gathering of information following a facility event as a weakness at multiple sites. For example, at one site, initial fact finding was performed during critique meetings where causal factors and potential corrective actions were also discussed, which is contrary to DOE Order 422.1, Section 2.f, *Investigation of Abnormal Events, Conditions and Trends*, and limits the effectiveness of obtaining initial statements from individuals involved and other facts associated with the event. (See Section 2.7.)

Performance measures for safety systems at a number of sites were not challenging or helpful in improving organizational performance. Some goals were consistently met over long periods and had not been revised to challenge the organization toward continuous improvement. Most measures were lagging, only evaluating past performance, rather than leading indicators that help to identify/predict future trends.

The 2008 report found feedback and improvement programs were improving. However, the report further stated that process weaknesses and inadequate implementation persist in each of the assurance systems elements that were reviewed. Specifically, it found that DOE contractors "do not conduct sufficiently rigorous self-assessments based on a structured process." Furthermore, the report said, in part, "An area of particular concern is the lack of rigorously performed and documented investigations." The conduct of investigations, including fact finding and critiques, remains an area of weakness, as stated above.

2.7 Occurrence Reporting and Processing System and Noncompliance Tracking System Data Analysis

Occurrence Reporting and Processing System Data

EA reviewed DOE-wide Occurrence Reporting and Processing System (ORPS) data for 2015 to identify any trends relevant to the management of safety systems. Of the 1,037 ORPS reports filed across the DOE complex in 2015, 342 of them were related to the management of safety systems. EA was able to relate information and common themes identified in these 342 ORPS reports to some aspects of issues discussed in this report. The most common and readily evident theme gleaned from the ORPS reports was the large percentage of reportable events (31 percent of the 342 reports) that can be directly attributed to procedure violation and/or inadequacy, consistent with the issues identified in this report. Next in relative importance was the area of configuration management and control, where 20 percent of the ORPS reports involved problems with maintaining configuration of safety systems. Although only three of the reviews performed between 2013 and 2015 focused specifically on configuration management and control processes, the ORPS data is consistent with issues identified at those sites where configuration management was evaluated in more detail. This also suggests that configuration management and control processes should be included as a specific area of focus in future EA targeted assessments. Other common themes between ORPS data and issues found during the targeted reviews of the management of safety systems included maintenance (6 percent).

In addition, EA reviewed information from the DOE Pilot Nuclear Safety Information Dashboard, which trends ORPS data, for any trends related to themes from this lessons learned report. Since 2010, there has been a slight downward trend in the number of reportable occurrences resulting from procedure issues. However, the number for 2015 remains high as stated above. There is no discernable trend in the number of occurrences resulting from configuration management issues over the same 6-year period. Between 2010 and 2015, significant improvement (greater than 50 percent reduction) has been seen in the numbers of occurrences resulting from feedback and improvement issues.

EA also analyzed the ORPS data for the 11 sites encompassed in this lessons learned report to determine whether the ORPS data validates the 11-site sample as representative of DOE-wide performance. The ORPS data shows that 64 percent of the procedure violation issues identified in reported occurrences across the DOE complex in 2015 came from the 11 sites for this report. Examples of procedure inadequacies identified in 2015 ORPS reports include, an inadequate in-service inspection procedure that was required for verification of acceptable facility confinement system and a technical document used at another facility to safely move and store uranium material was reported to be out of date for the last 9 years.

Configuration management and control issues identified in 2015 reportable occurrences at the 11 sites reviewed accounted for 63 percent of configuration management issues across the complex documented in ORPS. One ORPS report discovered confinement penetrations not properly sealed caused by inadequate configuration management of the barriers at a facility. In another occurrence, following a change made to a facility DSA to add existing doors to credited fire barriers, a door was omitted because of inadequate configuration management and control processes. In addition, an ORPS report documented the failure to validate a nuclear criticality safety code as the latest version because configuration management processes were not followed.

Maintenance occurrences at the 11 sites reviewed accounted for 67 percent of the maintenance issues identified in 2015 DOE-wide ORPS reports. One of the 2015 occurrences resulting from improper maintenance involved the installation of an incorrect gasket in an instrument air compressor that failed because of inadequate maintenance procedures at one facility. At another facility, a detector used at a DOE reactor to calculate primary coolant leakage when the reactor is pressurized was installed backwards because maintenance work documents were inadequate.

This analysis of ORPS data suggests that the results of management of safety system reviews conducted at the 11 sites are consistent with DOE complex-wide performance.

Noncompliance Tracking System Data

EA compared the enforcement data from the Noncompliance Tracking System (NTS) for 2015 to the issues contained in this lessons learned report. Of the 89 nuclear safety NTS reports filed in 2015, 45 of the reports directly related to the topics and issues discussed in this report. There was good agreement between reasons for these noncompliances and the themes addressed in Sections 2.1 through 2.6 above. For example, 58 percent of the nuclear safety noncompliances reported into NTS were related to procedure violations or inadequacies, and configuration management problems accounted for 18 percent of the nuclear safety violations.

Enforcement outcomes covering nuclear safety investigations for the period of January 2013 through December 2015 were also reviewed against the themes addressed in this lessons learned report. Eleven nuclear safety enforcement outcomes (2 preliminary notices of violation, 4 consent orders, and 5 enforcement letters) were issued on non-compliances that occurred between January 2013 and December 2015 across the DOE complex. The nuclear safety issues addressed in these enforcement actions involved procedure violations and configuration management in 7 of 11 enforcement actions. Feedback and improvement process issues were also identified as contributors to the nuclear safety violations.

Based on the review of available nuclear safety enforcement information, consistent agreement exists between the areas of noncompliance associated with the nuclear safety issues for 2013 – 2015 and the issues identified in this lessons learned report in the areas of procedure use and adherence, configuration management and control, and feedback and improvement processes discussed in Sections 2.1 through 2.6 above.

2.8 Waste Isolation Pilot Plant 2014 Fire and Radiological Events Analyses

The accident investigations associated with the Waste Isolation Pilot Plant (WIPP) 2014 underground fire and radiological release events were reviewed for management of safety system issues identified in this lessons learned report. Throughout the three WIPP investigation reports, causal factors and judgements of need were associated with procedure inadequacies and violations, configuration management failures, inadequate maintenance, and ineffective feedback and improvement processes, which relate to issues discussed in Section 2.1-2.6 above.

The WIPP ventilation High Efficiency Particulate Air (HEPA) system, designed as a safety system to automatically filter air discharged from the underground in the event of a radioactive airborne release from the mine, was not properly maintained and its operations were not clearly defined in emergency procedures. During the February 5, 2014, fire event, the Central Monitoring Room operator, unsupported by emergency procedures, incorrectly reacted to the emergency by aligning the ventilation system to HEPA filtration mode making conditions worse in the mine for those evacuating from the fire. In addition, preventative maintenance procedures for the underground hauling truck that caught fire did not follow manufacturer's recommendations. There were also problems with the WIPP configuration management elements of design requirements, work control, change control, and assessments that significantly contributed to the fire event. The configuration of the underground was not maintained in accordance with prescribed combustible limits, and the DSA/TSR allowed the hauling truck in a degraded condition to be placed near the waste stored in the underground.

On February 14, 2014, another event occurred, a radiological release from the mine. The continuous air monitor in the mine detected the release and signaled the ventilation system to shift automatically to HEPA filtration mode as it was designed. However, the automatic operation of the system failed (due to poor maintenance and testing) and only after quick response by an operator was the ventilation fully shifted to filtration mode. As it turned out, the release of radioactivity occurred because there was significant leakage through the shut HEPA bank bypass dampers which was then released to the environment through an exhaust duct. The leakage was the result of poor system design, maintenance, and testing.

The root cause from the radiological release accident at WIPP was the inability to "fully understand, characterize, and control the radiological hazard", which directly relates to weaknesses of the WIPP configuration management program. The root causes specifically related to waste packaging activities associated with the radiological release accident identified that, in addition to configuration management weaknesses, procedure inadequacies and non-compliances contributed to the radiological release at WIPP.

While the magnitude of concerns identified in the 11 EA management of safety system reports do not approach the degree to which programs and processes broke down at WIPP, the problems which led to these two WIPP events are similar to issues discussed in this report. Based on review of the WIPP events, the issues from the WIPP fire and radiological release events are consistent with this lessons learned report.

3.0 BEST PRACTICES

EA identified the following best practices that could also be valuable to other DOE sites.

3.1 Use of Institute of Nuclear Power Operations Resources

Two of the sites reviewed used Institute of Nuclear Power Operations (INPO) good practice documents, onsite assistance, and INPO training sources to promote continuous improvement in facility operations and management. Advanced Test Reactor (ATR) and Y-12 management and operating (M&O) contractors have taken advantage of DOE membership in INPO through assist visits where INPO subject matter experts conduct reviews on specific topics from operations to maintenance to engineering using INPO good practice standards to measure performance in selected areas. For example, ATR has received assist visits in the areas of equipment reliability and engineering during 2014 and 2015, and Y-12 received assistance from INPO maintenance subject matter experts to help validate a pilot preventive maintenance optimization program to more effectively apply maintenance resources to key systems and equipment. Battelle Energy Alliance, LLC (BEA) and Consolidated Nuclear Security, LLC also routinely send members of their management team to INPO supervisor and manager training where they are exposed to commercial nuclear industry managing practices. BEA has also joined INPO as an individual member in order to obtain additional assistance resources. Based on the analysis of the EA assessments of safety systems conducted between 2013 and 2015, EA considers this a best practice.

3.2 Required Use of Human Performance Error Reduction Tools for all Maintenance Activities

Battelle Energy Alliance, LLC requires and reinforces the use of human performance error reduction tools, such as formal 3-way communication, work steps/procedure place-keeping, and peer checking, as work is conducted at ATR. Integration of the human performance error reduction tools into the work control process helps to ensure that work activities are safely performed right the first time. This best practice was identified in EA's ATR assessment report dated October 2015.

3.3 Voluntary Implementation of DOE Order 426.1 SSO Requirements

Although DOE Order 426.1 only applies to defense nuclear facilities, the Idaho Operations Office has recognized the oversight benefit from assigning staff engineers to perform SSO of safety systems, and has fully implemented the SSO requirements of DOE Order 426.1, Appendix D, at EM and Office of Nuclear Energy nuclear facilities. Based on the analysis of the EA assessments of safety systems conducted between 2013 and 2015, EA considers this a best practice.

Appendix A
Recommendations

The recommendations discussed below are based on lessons learned identified during the Office of Enterprise (EA) reviews between 2013 and 2015. While the underlying deficiencies and weaknesses did not necessarily apply to all the sites, and many sites may have developed and implemented actions for the issues identified at their sites, the recommended actions are intended to provide additional insights for potential improvements at all sites. Consequently, U.S. Department of Energy (DOE) organizations and site contractors should evaluate the applicability of the following recommended actions to their respective facilities and/or organizations, and consider their use as appropriate in accordance with Headquarters and/or site-specific program objectives.

Office of Environment, Health, Safety and Security

Revise DOE Order 422.1, *Conduct of Operations,* Section 2.m, *Control of Interrelated Processes,* and/or supporting guidance/standards to clarify the requirements for this section of the Order. Consider the following actions:

- Revise Section 2.m, *Control of Interrelated Processes*, to specify that the requirements of the section apply to both facility and interrelated process operator organizations.

- Revise DOE-STD-1037-93, *Guide to Good Practices for Operations Aspects of Unique Processes*, dated June 1993, or other similar guidance document to align with DOE Order 422.1, Section 2.m.

Revise DOE Order 420.1C, *Facility Safety,* or supporting guidance/standards to provide additional requirements for effective implementation of cognizant system engineer (CSE) programs. Consider the following actions:

- Add requirements to DOE Order 420.1C for system walkdowns, development and implementation of system notebooks, and documentation of CSE activities.

- Include guidance in DOE Guide 420.1-1A to define acceptable methods of CSE program implementation, expanding upon the Order requirements to improve the consistency in CSE implementation.

DOE Field Elements

Verify that supervisors of safety system oversight (SSO) personnel periodically evaluate SSO program effectiveness required by DOE Order 426.1B. Consider the following action:

- Review SSO program documents to verify program requirements include periodic assessment of SSO program effectiveness.

Site Contractors

Ensure that maintenance programs are identified in the documented safety analysis (DSA) as safety management programs (SMP). Consider the following actions:

- If the maintenance program is not listed as an SMP in the DSA, revise the DSA at the next annual update to identify Maintenance as an SMP.

- Conduct management and independent assessments for maintenance consistent with other SMPs.

During self-assessments, consider the adequacy of surveillance testing to demonstrate operability of safety systems as defined in the facility safety basis. Consider the following actions:

- During self-assessments, evaluate surveillance test performance of technical safety requirements to ensure all possible combinations of safety equipment are tested.

- Include review surveillance test procedures against the safety basis requirements to ensure that the safety basis is properly implemented as part of self-assessment activities.

Ensure requirements in DOE Order 422.1, *Conduct of Operations*, Section 2.m, *Control of Interrelated Processes*, are met for both facility operators and interrelated process operators. Consider the following actions:

- Review and revise (as necessary) operator responsibilities (both facility and interrelated process operators) to ensure that those related to interrelated processes are adequately addressed. For facility operators, responsibilities should include facility impacts to interrelated processes (e.g., water, steam, electrical distribution). Conversely, responsibilities for operators of interrelated processes should address impacts that the interrelated process may have to facility operations.

- Develop and implement training (if necessary) on interrelated process responsibilities for facility and interrelated process operators.

- Develop and implement (as necessary) communication protocols for normal, outage, and abnormal interrelated process conditions. For example, communication procedures should be established in both facility and interrelated process organizations so that if an upset condition occurs on either side, it is clear how notifications are made as soon as possible to the appropriate counterpart.

Assess and verify effectiveness of CSE program requirements related to conducting safety system walkdowns and assessments. Consider the following actions:

- Conduct self-assessments of CSE program effectiveness, including the frequency with which walkdowns and systems assessments are performed, and revise the program accordingly.

- Review the CSE program to ensure that requirements for documentation of CSE system monitoring activities are adequate to capture all information pertinent to system health and reliability (e.g., results of formal and informal system walkdowns, and other performance observations and data).

Verify that existing performance measures are effective in promoting continuous improvement in nuclear safety. Consider the following actions:

- Review site procedures and processes for management of performance measures to make sure that the requirements for establishing and revising performance measures goals result in continuous improvement in nuclear safety programs and processes.

- Review current maintenance performance measures against the guidance in DOE Guide 433.1-1A, *Nuclear Facility Maintenance Management Program Guide for Use with DOE O 433.1B*, Section O, Performance Measures.

- Establish leading indicators where possible for organizational and program performance measures to help predict future performance trends.

Appendix B
Supplemental Information

Office of Enterprise Assessments (EA) Management

Glenn S. Podonsky, Director, Office of Enterprise Assessments
William A. Eckroade, Deputy Director, Office of Enterprise Assessments
Thomas R. Staker, Director, Office of Environment, Safety and Health Assessments
William E. Miller, Deputy Director, Office of Environment, Safety and Health Assessments
Patricia Williams, Director, Office of Worker Safety and Health Assessments
Gerald M. McAteer, Director, Office of Emergency Management Assessments

Quality Review Board

William A. Eckroade
Karen L. Boardman
John S. Boulden III
Thomas R. Staker
William E. Miller
Patricia Williams
Gerald M. McAteer
Michael A. Kilpatrick

Office of Enterprise Assessments Team Members

William Miller (Lead)
Charles Allen
Aleem Boatright
Ronald Bostic
Jimmy Dyke
Robert Farrell
Robert Freeman
William Macon
Timothy Mengers
Jeff Snook
Robert Compton
Timothy Martin
Glenn Morris
Terry Olberding
Joseph Panchison
Edward Stafford
Eric Swanson
Greg Teese