

Bruce Hamilton, Acting Chairman  
Jessie H. Roberson  
Daniel J. Santos  
Joyce L. Connery

**DEFENSE NUCLEAR FACILITIES  
SAFETY BOARD**

Washington, DC 20004-2901



The Honorable James Richard Perry  
Secretary of Energy  
U.S. Department of Energy  
1000 Independence Avenue, SW  
Washington, DC 20585-1000

Dear Secretary Perry:

The Defense Nuclear Facilities Safety Board (Board) approved the conduct of a safety investigation (preliminary safety inquiry) regarding the implementation of Title 10, Code of Federal Regulations, Part 830 (10 CFR 830), *Nuclear Safety Management*, at the Pantex Plant. In addition, the Board staff has completed an evaluation of the adequacy of safety controls for nuclear explosive operations at the Pantex Plant. The staff has brought the following to the attention of the Board:

- The safety basis at Pantex is deficient in meeting Title 10, Code of Federal Regulations, Part 830, *Nuclear Safety Management*. There are high consequence hazards that (1) are not adequately controlled; (2) may have controls, but lack documentation linking the controls to the hazards; and (3) have controls that are not sufficiently robust or that lack sufficient pedigree to reliably prevent or mitigate the event.
- Multiple components of the process for maintaining and verifying implementation of the safety basis at Pantex are deficient, including (1) completion of annual updates as required by 10 CFR 830, (2) processes for handling Unreviewed Safety Questions (USQ) and Justifications for Continued Operations (JCO), and (3) processes for performing Implementation Verification Reviews of credited safety controls.
- To date, the NNSA Production Office and the Pantex contractor have been unable to resolve the known safety basis deficiencies.

The enclosed reports provide examples of the deficiencies noted. The Board is currently evaluating the impact to public health and safety of the deficiencies noted and other items identified during the safety investigation and the staff evaluation, and has not yet reached any conclusions.

Pursuant to 42 U.S.C. §2286b(d), the Board requests a written response and a briefing from DOE within 30 days to inform the Board regarding the actions taken and progress to date. The Board is providing you the enclosed reports for context in responding to this reporting requirement. The Board will consider the additional information provided by DOE in support of any further Board action on this matter as it continues its deliberations.

Yours truly,

Bruce Hamilton  
Acting Chairman

Enclosures

c: Mr. Joe Olencz

# DEFENSE NUCLEAR FACILITIES SAFETY BOARD

## Staff Issue Report

**SUBJECT:** Nuclear Explosive Operations with Uncontrolled Hazards at the Pantex Plant

Members of the Defense Nuclear Facilities Safety Board's (Board) staff reviewed the hazard analysis reports (HAR) for B61, W76, W78, W87, and W88 nuclear explosive operations at the Pantex Plant (Pantex). The staff team held multiple interactions between November 2017 and March 2018 with personnel from the National Nuclear Security Administration (NNSA) Production Office (NPO) and the Pantex contractor, Consolidated Nuclear Security, LLC (CNS), responsible for development and maintenance of the Pantex documented safety analysis (DSA)<sup>1</sup> to discuss specific scenarios identified in the safety basis documents.

The Board's staff team identified credible hazard scenarios that lack documented evidence that Pantex has identified and implemented credited safety controls to prevent high order consequences, i.e., inadvertent nuclear detonation (IND) and/or high explosive violent reaction (HEVR). High order consequences have the potential to significantly exceed the Evaluation Guideline to the public. Through evaluation of the Pantex safety basis, the staff team identified additional deficiencies related to (1) the design and classification of administrative controls relied upon for specific risk reduction, (2) the processing of new information through the approved unreviewed safety question (USQ) process, and (3) quality issues in the safety basis documentation.

Following the multiple interactions conducted during this review, the staff team concluded that CNS and NPO have not demonstrated how the current suite of credited controls—i.e., safety class and safety significant structures, systems, and components (SSC), specific administrative controls (SAC), and safety management programs—effectively prevent the identified hazard scenarios from resulting in high order consequences.

**Background.** In July 2010, the Board transmitted a letter to the NNSA Administrator communicating issues with the HARs for several nuclear explosive operations at Pantex [1]. The issues included concerns that the Pantex contractor<sup>2</sup> inappropriately used initiating event probabilities to exclude credible hazards from further consideration. In some instances, this resulted in hazard scenarios where the responsible design agency provided a credible weapon response but the Pantex contractor did not identify or implement controls to address these hazards. In its 2010 letter, the Board concluded that this practice was inconsistent with the safety basis safe harbor methodologies in use at the time, i.e., DOE-NA-STD-3016-2006, *Hazard*

---

<sup>1</sup> DSA refers to the full framework of safety analysis documents comprising the safety basis for conducting nuclear operations at Pantex. This includes HARs, safety analysis reports (SAR), the technical safety requirements (TSR) document, Justifications for Continued Operations (JCO), and Evaluations of the Safety of the Situation.

<sup>2</sup> At the time of the 2010 Board letter, Babcock & Wilcox Technical Services Pantex, LLC, was the management and operating (M&O) contractor for Pantex. Following a contract transition in July 2014, CNS became the M&O contractor.

*Analysis Reports for Nuclear Explosive Operations* [2], and DOE-STD-3009-1994, Change Notice 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses* [3].

NNSA<sup>3</sup> and the Pantex contractor developed a DSA Upgrade Initiative (DSAUGI), in part, to address the concerns communicated in the Board’s 2010 letter. DSAUGI included goals to (1) develop accident analyses for all hazardous events that do not have screened responses for IND and HEVR, and (2) update the safety management programs to ensure that the key provisions of the programs, as they relate to operational and facility safety, are adequately described and translated into TSRs [4]. As indicated in initial revisions of the upgrade initiative, the Pantex contractor and NNSA intended DSAUGI to be a multi-year effort<sup>4</sup>, with detailed schedules of deliverables maintained to ensure that its goals were accomplished in a timely and complete manner. Completion of DSAUGI, as it was initially described, would have entailed significant revisions to the W76, W78, W87, and W88 HARs to address deficient legacy conditions such as those identified in the 2010 Board letter [4].

In 2013, the Pantex contractor developed the DSA Improvement Plan (DSAIP) to “improve the Pantex DSA to achieve consistency and simplification, and to address legacy issues” [5]. DSAIP superseded DSAUGI. DSAIP had a stated goal to “achieve continuous improvement through incremental change,” as realized by incorporation of its core principles in DSA change package development and during the DSA annual update process [5]. The original revision of DSAIP specified 15 core principles, including the following principles relevant to the issues presented in this report:

- **Core Principle 4** – “Evaluate important to safety controls for either elimination or for elevation to a [credited safety-related] control” [5].
- **Core Principle 10** – “Evaluate key elements for either elimination or for re-categorization as a [credited safety-related] control” [5].
- **Core Principle 11** – “Ensure Specific Administrative Controls (SACs) are appropriately classified per DOE-STD-1186” [5].

Additionally, DSAIP stipulated specific initiatives necessary to address legacy issues in the safety basis and to accomplish the plan’s goals. These initiatives, developed in part to address the issues identified by the Board, included an effort to resolve “screening of high consequence/low probability events (in both Hazard and Accident Analyses)” [5]. The original issue of DSAIP included a notional schedule to complete this effort through proposed safety basis change packages, scheduled for submittal to NPO in February 2014 [5].

The Pantex contractor updated DSAIP annually from 2014 to 2017. The 2015 and 2016 DSAIP revisions listed the status of “Resolving High Consequence/Low Probability Events in the Accident Analysis” as “Ongoing,” and no longer provided an explicit path to closure [6, 7].

---

<sup>3</sup> At the time of the 2010 Board letter, the local NNSA office was referred to as the Pantex Site Office (PXSO). In 2012, PXSO merged functions with the Y-12 Site Office to form NPO.

<sup>4</sup>The original plan, issued in 2011, was to complete DSAUGI by the end of fiscal year 2015.

The 2017 revision of DSAIP represented a significant change to the plan—CNS retained the core principles and higher-level objectives, but no longer provided the status of the specific initiatives, including the initiative related to resolving high consequence, low probability events [8]. Based on feedback and concerns from NPO related to the quality of DSA change package submittals, CNS plans to revise DSAIP in 2018 “to identify ‘Core Principle’ efforts as discrete projects” [9].

In November 2017, the staff team performed a focused review of the W88 HAR to determine if actions taken by NNSA and CNS, including those accomplished through DSAUGI and DSAIP, effectively addressed the concerns presented in the 2010 Board letter. Based on the issues the staff team identified in the W88 HAR, the team expanded the review scope to include additional HARs. The issues and conclusions described in this report stem from that focused review and the staff team’s additional follow-on activities.

The remainder of this report will explore four types of deficiencies the staff team identified: (1) credible hazard scenarios that lack documented evidence that Pantex has identified and implemented credited safety controls to prevent high order consequences, (2) the design and classification of administrative controls relied upon for specific risk reduction, (3) the processing of new information through the Pantex contractor’s approved USQ process, and (4) quality issues in the safety basis documentation.

**Identification of Credited Safety Controls for Credible Hazards.** The Board’s staff team reviewed the hazard disposition tables and related hazard and accident analyses located in the approved HARs for B61, W76, W78, W87, and W88 operations to identify the controls relied upon to prevent hazard scenarios from resulting in high order consequences. While the safety bases identify adequate controls for the vast majority of credible hazard scenarios, the Board’s staff team identified credible hazard scenarios with unscreened weapon responses for IND and HEVR for which the safety bases either do not define credited safety controls or for which the credited safety controls are not sufficient. Of note, the staff team’s review of applicable safety basis documents was thorough but not exhaustive—and additional scenarios may exist.

*DOE Expectations for the Identification of Credited Safety Controls*—Title 10, Code of Federal Regulations, Part 830, *Nuclear Safety Management* (10 CFR 830), requires that the contractor responsible for DOE nonreactor nuclear facilities establish and maintain the safety basis for the facility. In doing so, the DSA for the facility must “[d]erive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use” [10]. The Pantex DSA is developed to implement the safety basis requirements specified in 10 CFR 830 through adherence to the following two safe-harbor methodologies: DOE-NA-STD-3016 for nuclear explosive operations and DOE-STD-3009 for the facilities in which nuclear explosive and nuclear material operations are performed. The guidance and requirements specified in these documents describe the DOE expectations for identification of hazard controls relied upon to protect workers and the public.

Per DOE-NA-STD-3016-2016, “[h]azard scenarios that are not screened for IND or HEVR consequences...are designated as Design Basis Accidents (DBAs), and are retained for consideration in the accident analysis section per DOE-STD-3009....With the exception of [natural phenomena hazards], initiating event probability information must not be used to dismiss the need to apply controls for plausible accident scenarios resulting in IND or HEVR” [11]. In this context, “screened” is defined as “[t]he weapon response likelihood provided for given hazards and associated nuclear weapon configuration combinations that the responsible DA(s) [design agencies] asserts will not result in a specific weapon response consequence. The assignment of an IND or HEVR numerical likelihood [weapon response] will be treated as screened if the likelihood were  $\leq 10^{-9}$ ” [11].

The 2016 revision of DOE-NA-STD-3016 was accepted into the Pantex M&O contract in 2016, but has not yet been fully implemented. The previous revision to this standard, DOE-NA-STD-3016-2006, does not include a numerical screening threshold, and simply describes screened weapon responses as “[h]azards and associated weapon configuration combinations that cannot result in a weapon response” [2]. The HAR development approach specified in DOE-NA-STD-3016 is built around an assumption and acknowledgement that offsite consequences from HEVR and IND accidents will challenge the Evaluation Guideline in the absence of any rigorous analysis. With this in mind, DOE-NA-STD-3016-2016 specifies that “[t]he approach to the identification and classification of controls in the hazard analysis is the same as the process described in DOE-STD-3009” [11].

The Pantex M&O contract applies the requirements of DOE-STD-3009-1994, Change Notice 3, to existing facilities. This standard specifies that “[i]n order to comply with 10 CFR 830, specific safety controls are to be developed in the DSA” [3]. It clarifies this expectation by stating that 10 CFR 830 “defines safety class designation for SSCs that are established on the basis of application of the Evaluation Guidelines. This designation carries with it the most stringent requirements (e.g., enhanced inspection, testing and maintenance, and special instrumentation and control systems)” [3]. When applied in the context of nuclear explosive operations, the standard stipulates that compliance with 10 CFR 830 requires application of safety class controls to prevent or mitigate unscreened hazards with HEVR or IND consequences.

*W88 Hazards with Insufficient Safety Controls*—In November 2017, the Board’s staff team provided NPO and CNS with an initial list of hazard scenarios from the DSA with unscreened weapon responses for IND and HEVR consequences, where safety class controls were not clearly applied. Each of these scenarios potentially is encountered during W88 operations in nuclear explosive cells. The scenarios included postulated hazards related to mechanical impacts caused by falling technicians; mechanical impacts due to dropped tooling and components; and scrapes, pinches, and gouges of critical weapon components. The Appendix to this report identifies the specific scenarios in greater detail.

Each identified hazard scenario applies a weapon response rule where the likelihood of high order consequences is listed as “sufficiently unlikely.” This frequency bin generally corresponds to conditional response likelihoods of  $10^{-7}$  or  $10^{-8}$  depending on the weapon program and consequence, given a particular stimulus or insult. In the framework of weapon response

and HAR development, sufficiently unlikely is not equivalent to “screened.” While the likelihood of high order consequences for any of these scenarios is extremely low, credited safety controls are still necessary to protect the public.

Mitigative controls such as the specialized nuclear explosive cell structure may be credited to reduce the consequences to the offsite public from HEVR accidents, but such controls are not effective for IND scenarios. Control sets for scenarios with a credible risk of IND must be preventive in nature. Additionally, while the nuclear explosive cell structure could be credited as a mitigative control to protect the public from HEVR consequences, this control would not protect the facility worker from high order consequences, requiring consideration of additional preventive controls. Nuclear explosive bay structures are not designed to provide mitigation to protect the public from HEVR consequences.

During an initial interaction with CNS safety analysis engineering (SAE) and NPO nuclear safety and engineering personnel in November 2017, CNS presented its initial analysis of the identified scenarios to the Board’s staff review team. This initial analysis noted that, while not currently and explicitly documented in the safety basis, the cell structure is an in-place, safety class control that CNS could apply to mitigate the offsite consequences from HEVR accidents in the identified scenarios.

In addition, CNS noted that currently it has addressed other scenarios by compensatory measures implemented via a JCO, approved by NPO in May 2017 [12]. However, CNS acknowledged that the remaining scenarios did not have readily apparent controls. During subsequent discussions with the Board’s staff team, CNS personnel indicated that they had identified the potential for similarly treated hazard scenarios on the W76 program. Based on these initial concerns, the staff team decided to expand the scope of its review to include other HARs that CNS had not updated recently. This included the B61, W76, W78, and W87 programs.

*Treatment of New Information for W88 Hazard Scenarios:* The approved CNS procedure for USQ determinations defines a process whereby CNS captures new information and evaluates whether it represents a potential inadequacy of the safety analysis (PISA)<sup>5</sup>. At Pantex, this is termed the problem identification and evaluation (PIE) process. Soon after the initial meeting where the Board’s staff team presented the W88 hazard scenarios of concern, CNS SAE personnel captured the identified scenarios as new information and initiated the PIE process. Although CNS personnel indicated to the staff review team that other programs might contain additional similar scenarios, it did not formally evaluate other weapon programs via the PIE process.

After approximately one month of evaluation, CNS determined that the identified new information did not represent a PISA. Specifically, in response to the question “Does the situation indicate an unanalyzed hazard exists or a potential new credited control is needed?”, the PIE process disposition form states that “[a]lthough there are hazards that identify no controls are

---

<sup>5</sup> CNS has submitted, and NPO has approved, separate USQ procedures at Pantex and Y-12; there may be inconsistencies with 10 CFR 830 that occur at both sites. CNS plans to consolidate the USQ processes across both sites.

selected, these hazards have been dispositioned” [13] with one or more specified disposition pathways. The specified pathways are as follows: (1) controls are identified, (2) scenario is covered in the May 2017 JCO, (3) scenario is not credible, (4) scenario identifies “Facility Structure” as a mitigating design feature, and (5) scenario identifies “Procedures and Training” as a safety management program key element.

The Board’s staff team independently evaluated CNS’s disposition of the identified hazard scenarios. The staff team agrees that the scenarios dispositioned through the first two pathways, i.e., controls are identified in the HAR or in the May 2017 JCO, are adequately controlled. Per the CNS evaluation, these pathways apply to only seven of the twenty-five identified hazard scenarios.<sup>6</sup> The staff team concluded that the three remaining disposition pathways (which CNS applied for 18 hazard scenarios) are either not technically justified or insufficient with regards to established expectations for control reliability and efficacy.

CNS concluded through its PIE evaluation that a specific gouge scenario, in a configuration with bare high explosives, is not credible. The conclusion that this specific scenario is not credible contradicts the Hazard Analysis Summary Table in the approved HAR, which concludes that the hazard is credible. The staff team further evaluated the scenario by reviewing the associated operating procedures and could not identify any controls that would preclude the event. With the current information provided by CNS, the staff team is unable to independently reach the same conclusion. The staff review team further notes that CNS would need to request approval from NPO to reverse a conclusion presented in the approved safety basis.

CNS concluded that the remaining 17 scenarios were controlled through the use of the facility structure or through key elements of safety management programs. However, as discussed above, the facility structure is incapable of mitigating the consequences of IND scenarios or protecting the facility worker from HEVR consequences.

For the remaining scenarios that have credible IND consequences, the only preventive features are key elements of safety management programs, such as “procedures and training” or the “falling man awareness protocol.” In some instances, these key elements are ill-defined and are not developed for the specific context for which they are currently relied upon. In the case of the W88, the “procedures and training” key element is not carried into the TSR document for application at the floor level; attributes of the key element are not defined to allow operators, supervisors, or oversight personnel to verify their implementation; and the key elements cited by CNS are not implemented via step-by-step operating procedures that would ensure they are performed properly. Key elements alone cannot reliably prevent these accident scenarios and do not meet DOE’s established expectations for controls relied upon to protect the public (this is discussed further in the *Administrative Controls Credited for Specific Risk Reduction* section).

Extent of Condition Review for Hazards without Identified Safety Controls—Based on the initial concerns noted on the W88 program, the Board’s staff team conducted an independent extent of condition review. Specifically, the Board’s staff team reviewed the B61, W76, W78,

---

<sup>6</sup> CNS performed its PIE response for 25 scenarios. The Board’s staff team identified additional scenarios during their independent evaluation.



and W87 HARs, associated nuclear explosive operating procedures, and sections of applicable SARs. Through this review, the staff team identified similar scenarios on each of the analyzed programs with the exception of B61. After a preliminary review of the B61 HAR, the staff team identified discrepancies in the identification of controls for scenarios with sufficiently unlikely weapon response but did not find any instances of a sufficiently unlikely weapon response without appropriately implemented safety controls. For the remaining programs, the staff team communicated hazard scenarios of concern to NPO and CNS as they were identified. The specific scenarios are identified in greater detail in the Appendix to this report. At the time of this report, CNS had not reviewed these scenarios via its PIE process as actionable new information, with the exception of those identified for the W88 program.

*W76 Hazards without Identified Safety Controls:* The staff team identified five weapon configurations during W76 cell operations where the HAR identifies a falling production technician hazard and applies a sufficiently unlikely weapon response for a high order consequence. For these hazard scenarios, there is no credited control. During discussions with NPO and CNS personnel, CNS noted that the “falling man awareness protocol” is an applicable control, albeit, currently uncredited in the HAR. The protocol includes specific training to ensure the area of approach to a unit is clear of any objects that could lead to a tripping hazard, to ensure approaches to the unit by production technicians are minimized and only performed as needed to support the process, and to ensure that production technicians approach slowly and cautiously. The falling man awareness protocol was developed as a best practice when it was implemented in 2014 [14], in part, to address Board concerns and nuclear explosive safety evaluation findings [1, 15, 16]. However, CNS has since credited the protocol with performing a safety class function as a compensatory measure in B83 and W88 JCOs<sup>7</sup>. CNS also credited the protocol as an operational restriction following a PISA on the W76. The development of the protocol was not intended to meet DOE requirements and guidance for designation as a safety class control. It is not appropriate to credit the falling man awareness protocol as an operational restriction or compensatory measure in lieu of developing engineered controls and/or SACs and process improvements to prevent the hazard.

*W78 Hazards without Identified Safety Controls:* The staff team identified that the W78 HAR treats sufficiently unlikely weapon responses as screened—an approach that could result in high order consequence scenarios existing in the safety basis without safety class preventive controls. The staff team did not find deficiencies in the W78 HAR similar to those found for the other weapon programs, but this could be due to the lack of clarity in assignment of controls to process steps. Specifically, in the accident analysis, the W78 HAR inappropriately credits controls that are not applicable in all of the process steps for which they are credited to perform a safety function. As a result, the applicable control suite for hazards in each process step is not explicitly defined. Additionally, W78 program cell operations recently implemented a transfer cart, mitigating some falling technician concerns. However, the staff team did identify the following deficiencies in the identification of safety controls for the W78 program in the Sitewide and Transportation SARs.

---

<sup>7</sup> The B83 JCO that includes the falling man awareness protocol as a compensatory measure expires on May 16, 2018. Upon expiration, CNS plans to no longer implement the protocol as a compensatory measure, and instead administratively pause B83 operations. The W88 SER remains in effect.

For a lightning insult scenario, a single control, i.e., a transportation cart, is applied that only decreases the potential for weapon response from the threat to sufficiently unlikely. Although CNS has additional controls available that could address this gap—e.g., use of a lightning detection and warning system and prohibiting transport (e.g., movement of transportation cart containing unit within the ramps that connect the bays and cells at Pantex) during lightning warnings—W78 transport is currently authorized during lightning warnings. NPO has formally accepted the risk presented by these operations.

During the movement of the unit in other facilities, the unit is at risk from a hydraulic fluid fire (see Appendix). The hazard analysis states that based on the weapon response to this threat, there is no credible response because the frequency is sufficiently unlikely. As a result, Pantex did not identify any safety class controls to prevent the high order consequences from this scenario.

*W87 Hazards without Identified Safety Controls:* During W87 disassembly operations, the mechanical safe and arm detonator (MSAD) becomes exposed to mechanical impacts prior to its removal. The HAR documents mechanical impact scenarios, including dropped tooling or weapon components, seismic hazards causing an impact, and falling technicians. The identified hazard scenarios of concern apply a sufficiently unlikely weapon response for a high order consequence. Special tooling is installed and the process is defined to minimize hazards; however, the HAR does not identify any credited engineered or administrative controls to prevent the accident.

Additionally, due to the older design of the process, the special tooling itself is the drop hazard in several cases. The W87 program does not have an integrated workstand and does not use process carts to introduce tooling and remove weapon components. These techniques are standard practice for *Seamless Safety for the 21st Century (SS-21)*<sup>8</sup> tooling and process design and have been used successfully to control similar hazards on other weapon programs. The staff team focused on W87 disassembly operations; similar issues likely exist in assembly operations.

During certain operations, the MSAD is intentionally operated in a controlled manner. The weapon response summary document supporting the HAR includes separate response values applicable to both configurations—where the MSAD is not operated and where it is operated. The likelihood of high order weapon response for scenarios involving mechanical insult to the sensitive area of an operated MSAD is higher than for the un-operated configuration. However, the HAR assumes that it is not credible to impact the sensitive area of the MSAD. The staff team reviewed both the HAR and applicable discussion in the design agencies' weapon response summary document and concluded that CNS has not adequately described the technical basis or

---

<sup>8</sup> An SS-21 compliant process is one that incorporates the principles outlined in the Design and Production Manual, Chapter 11.3, *Seamless Safety (SS-21) For Assembly and Disassembly of Nuclear Weapons at the Pantex Plant*. Such a process prevents the application of unauthorized or unanalyzed energy from sources external to the nuclear weapon, contains no single-point failures in the operation, and minimizes radiation exposure to personnel. NNSA and the Pantex M&O contractors implemented SS-21 from 2004–2012; however, the W87 was one of the earlier programs to be evaluated. Subsequent to its implementation on the W87, SS-21 matured substantially. In 2017, NNSA directed CNS to evaluate the potential for undertaking an “SS-21 refresh” to implement tooling and processes that would reflect current SS-21 concepts.

referenced supporting documentation to support the HAR's assertion that the scenario is not credible.

*Safety Implications*—For the weapon programs discussed in the above sections, the staff team identified credible scenarios with potential high order consequences, without applied controls. Safety class controls, meeting DOE expectations for such, are necessary to prevent scenarios with IND consequences and prevent or mitigate scenarios with potential HEVR consequences. Without adequate, reliable controls identified in the Pantex DSA, NNSA has not demonstrated that these hazards are prevented or mitigated.

NNSA, CNS, and the design agencies are currently pursuing safety basis updates on the B61 and W88 programs. The updates will improve the overall quality of the HARs by using current practices and methodologies that were not included when the original HARs were developed—e.g., meeting DOE-NA-STD-3016-2016 expectations, including additional implementation guidance. As part of the development process for upcoming modernization of the B61 and W88, both programs' operations are being overhauled, including making special tooling and process improvements and upgrading the hazard analysis with the use of *Collaborative Authorization for the Safety-Basis Total Lifecycle Environment-Pantex* (CASTLE-PX).

CASTLE-PX is a software tool used to organize, maintain, and track hazards, weapon responses, and controls as Pantex and the design agencies support hazard analysis development and maintenance. Given that the W88 HAR currently is being updated, there would be a limited period where compensatory measures would be needed to allow W88 operations to continue with a compliant and reliable control set. Given the limited duration until the new HAR is approved, a near-term JCO that identifies controls to address hazard scenarios with unscreened weapon responses without currently identified controls would be an appropriate vehicle to implement these necessary compensatory measures.

With respect to the W76, W78, and W87 HARs, these programs do not fully use CASTLE-PX, nor have the HARs received a full upgrade since their implementation. With the W76, a subset of bay operations was upgraded via CASTLE-PX in 2013; however, the hazard scenarios of concern identified by the staff team occur during cell operations, which do not have a related HAR upgrade. With no near-term, comprehensive safety basis upgrades planned for the W76, W78, and W87 programs, the staff team believes that timely action is needed to identify controls and make any necessary procedure changes.

**Administrative Controls Credited for Specific Risk Reduction.** CNS has identified key elements of safety management programs, or the falling man awareness protocol, as the controls relied upon for preventing high order consequences for some of the hazard scenarios that the staff review team identified as lacking credited controls. However, relying on key elements of safety management programs does not provide a level of protection for members of the offsite public or workers equivalent to an engineered SSC or a properly implemented SAC, and does not comply with codified expectations in DOE directives.

DOE Expectations for Administrative Controls Identified to Prevent or Mitigate Accident Scenarios—When a contractor responsible for operation of a nuclear facility develops the hazard analysis in accordance with DOE-STD-3009, the contractor is required to put in place controls to prevent or mitigate the consequence of hazards that challenge the Evaluation Guideline to an acceptable level. As discussed above, because the consequences from HEVR and IND are so grave, these accidents are assumed to exceed the Evaluation Guideline and therefore require safety class controls.

If a contractor cannot design engineered controls for an accident scenario, it has the option of developing an administrative control. DOE-STD-1186-2016, *Specific Administrative Controls*, states, “SACs shall be designated where an administrative control performs [a safety class (SC)] or [safety significant (SS)] safety function to prevent or mitigate a postulated hazard or accident scenario” [17]. As such, any administrative control selected to prevent postulated accident scenarios where the consequence is HEVR or IND should be designated in the TSRs as a SAC. Due to the safety importance of SACs (i.e., fulfilling the role of a safety class or safety significant engineered control), these controls require an enhanced pedigree and reliability compared to other administrative controls to ensure their dependability. For example, a human reliability assessment is recommended when developing SACs to ensure their dependability, and a SAC should be written so that it is verifiable through testing, examination, and assessment that it is performing its safety function [17].

Application of Safety Management Program Key Elements for Specific Risk Reduction—Key elements might be identified as part of an administrative control; however, when the administrative control is relied upon to prevent high order hazard scenarios, the critical elements of the control should be designated as SACs, not simply noted as key elements of the administrative control. The following discussion from DOE-STD-3009-2014, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*, is relevant:

*The criteria for designating an [administrative control (AC)] as a SAC include two conditions that need to be met: (1) ACs are identified in the safety analysis as a control needed to prevent or mitigate an accident scenario and (2) ACs have a safety function that would be SS or SC if the function were provided by an SSC. These ...may serve as the most important control or only control, and may be selected where existing engineered controls are not feasible to designate as SS SSCs. Therefore, when ACs are selected over engineering controls, and the AC meets the criteria for an SAC, the AC is designated as a SAC. Controls identified as part of a safety management program may or may not be SACs, based on the designations derived from the hazards and accident analyses in the DSA. Programmatic ACs are not intended to be used to provide specific or mitigative functions for accident scenarios identified in DSAs where the safety function has importance similar to, or the same as, the safety function of SC or SS SSCs – the classification of SAC was specifically created for this safety function – this generally applies to the key element of the safety management program that provides the specific preventive or mitigative safety function. [emphasis added] [18]*

DOE-STD-3009 identifies several safety management programs that an M&O contractor might want to consider for inclusion in a potential DSA. The examples include criticality safety,

fire protection, and other programs. The standard also discusses key elements of these programs that are critical for ensuring that the program can perform its credited safety function:

*Key elements are those that: (1) are specifically assumed to function for mitigated scenarios in the hazard evaluation, but not designated an SAC; or, (2) are not specifically assumed to function for mitigated scenarios, but are recognized by facility management as an important capability warranting special emphasis. It is not appropriate for a key element to be identified in lieu of a SAC. The basis for selection as a key element is specified, including detail on how the program element: (1) manages or controls a hazard or hazardous condition evaluated in the hazard evaluation; (2) affects or interrupts accident progression as analyzed in the accident analysis; and (3) provides a broad-based capability affecting multiple scenarios. [emphasis added] [18]*

Application of the Falling Man Awareness Protocol—Recently, CNS has credited the falling man awareness protocol to perform a safety class preventive function as a compensatory measure in B83 and W88 JCOs, as well as an operational restriction for the W76 program. This protocol includes the provisions that specific training will be provided to ensure that:

- Approaches to nuclear explosives are clear of any objects that could lead to a tripping hazard.
- Approaches to nuclear explosives by production technicians are minimized and only occur as needed to support the process.
- Production technicians approach the nuclear explosive slowly and cautiously.

DOE's nuclear safety directives establish a hierarchy of controls that specifies a preference for engineered controls over administrative controls. In instances where engineered controls are not available to prevent the falling technician hazard, CNS should formalize this protocol as a SAC during the next safety basis annual update. This is necessary to meet the intent of DOE directives, as discussed above. Moreover, CNS should consider application of this SAC across the remaining weapon programs and evaluate the application of additional measures (e.g., tooling handoffs, transfer carts, work tables closer to the unit) to increase the reliability of the control. Of note, on the W78 program, a SAC is currently implemented to remove any potential tripping hazards at the beginning of the production technicians' shift. This SAC does not provide the same level of control as the W88 JCO, which seeks to control the falling technician concern throughout the entire shift; however, CNS recently implemented transfer carts for W78 operations, mitigating some falling technician concerns. Adoption of the falling man awareness protocol SAC on the W78 program should also be considered to fully control these scenarios.

Safety Implications—Reliance on procedures and training and other safety management program key elements as controls for specific risk reduction in lieu of designation as a SAC is not appropriate in the Pantex safety basis. There is no reliability assessment or appropriate pedigree associated with the key elements, and reliance on procedures and training has inherent

weaknesses. Safety management programs do not have the requisite reliability to assure appropriate prevention or mitigation of hazards with potential consequences that exceed the Evaluation Guideline. A recent report from the Board's Pantex resident inspectors identified multiple breakdowns in the falling man awareness protocol, a compensatory measure that lacks the required pedigree of a SAC [19]. The falling man awareness protocol, if used for specific risk reduction, should be formally codified as a SAC across weapon programs, and application of additional measures, as noted above, should be considered to increase the reliability of the control. In instances where safety management programs are the only measures implemented in the Pantex DSA to control high order consequences, NNSA has not demonstrated that the hazards identified in this report are prevented or mitigated.

**Processing of New Information.** The USQ process as implemented at Pantex includes a PIE process to evaluate new information, operational events, and discrepant as-found conditions to determine whether they represent a PISA. As part of the PIE process, CNS safety analysts answer the following questions to determine if the problem will be addressed as a PISA:

1. Does the situation indicate that an unanalyzed hazard exists or a potential new credited control is needed?
2. Does the situation indicate that the parameters used or assumed in the DSA, or in calculations used or referenced in the DSA, may not be bounding or are otherwise inadequate with respect to consequences or frequency?
3. Does the situation indicate that a directive action SAC may not provide the safety function assigned to it within the DSA?

CNS determined that the unscreened hazard scenarios with high order consequences without credited safety class preventive controls for the W88 program did not warrant a PISA designation. As discussed in detail earlier in this report, the staff team disagrees with CNS's evaluation. Moreover, the staff team does not believe that CNS has met the relevant DOE expectations for processing new information.

DOE Expectations for Evaluating New Information—DOE Guide 424.1-1B, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements*, states the following for timeliness of evaluating new information:

*10 CFR 830. 203(g) requires certain actions for a PISA. A PISA may result from situations that indicate that the safety basis may not be bounding or may be otherwise inadequate; for example, discrepant as-found conditions, operational events, or the discovery of new information. It is appropriate to allow a short period of time (hours or days but not weeks) to investigate the conditions to confirm that a safety analysis is potentially inadequate before declaring a PISA. The main consideration is that the safety analysis does not match the current physical configuration, or the safety analysis is inappropriate or contains errors. If it is immediately clear that a PISA exists, then the PISA should be declared immediately. [20]*

CNS flows down this guidance into its local implementing procedure, CD-3014, *Pantex Plant Unreviewed Safety Questions Procedure*, as follows:

*If the determination can be readily made that a PISA does not exist within 3 business days from when [new information] is determined to be mature, or an operational event occurs, the decision will be documented. If the determination cannot be readily made in this timeframe, a PISA is declared and documented.*  
[21]

*Evaluation of New Information Identifying Credible Hazards without Credited Safety Controls*—CNS dispositioned the W88-focused PIE entry after approximately one month, concluding there was no PISA. This lack of timeliness in processing the new information is inconsistent with the expectations of relevant DOE directives and the NPO-approved site implementing procedure. Based on its evaluation of the W88 PIE entry, CNS has not entered the PIE process for the corresponding new information for the other weapon programs discussed above. Furthermore, NPO and CNS informed the staff review team that the DSA will be further improved under the current DSAIP, so more immediate actions are not needed. However, the staff team identified significant problems with relying on the DSAIP to address the handling of unscreened “sufficiently unlikely” scenarios:

- DSAIP included a core principle to discontinue the use of key elements of safety management programs as a control for specific risk reduction. However, CNS has not defined a timeline or included specific tasks (e.g., individual SARs and HARs) to eliminate this use of key elements. Additionally, although the core principle has been present since the original DSAIP was developed in 2013, the use of key elements as controls for specific risk reduction remains prevalent throughout the DSA.
- DSAIP included an initiative to meet DSA requirements to address high consequence, low probability events. DSAIP revisions 1 and 2 included this initiative with explicit tasks and schedules. However, revisions 3 and 4 included it as a general initiative with an “ongoing” schedule status. CNS removed any discussion of high consequence, low probability events from the current DSAIP (revision 5).

In a February 2018 interaction with the Board’s staff team and a Board Member, NPO and CNS discussed the development of a safety evaluation report to justify the current safety posture [22]. Additionally, NPO and CNS discussed the concept of separating the DSAIP into an improvement plan and a “compliance” directed plan, the latter of which might be included in support of the safety evaluation report. NPO and CNS are developing the documents to support the proposed safety evaluation report. CNS submitted a JCO to NPO for review and approval on June 29, 2018, to justify the current safety posture and continue operations.<sup>9</sup> However, the submitted JCO does not formalize safety controls for a number of the credible accident scenarios detailed in this report. As of July 27, 2018, NPO was still reviewing the JCO. CNS has not taken any immediate actions in the interim, e.g., identifying and implementing compensatory measures for the applicable scenarios.

---

<sup>9</sup> This Issue Report updated on July 27, 2018, to incorporate issuance of the JCO.

*Safety Implications*—The staff team finds CNS’s evaluation of this new information to be inadequate. CNS has continued nuclear explosive operations on all applicable programs without applying compensatory measures or operational restrictions to address the deficiencies identified by the staff team. Furthermore, CNS’s disposition of the PIE entry for W88 hazard scenarios failed to meet the timeliness expectations of relevant DOE directives and the NPO-approved site implementing procedure.

**Overall Challenges with DSA Quality.** Throughout the independent extent of condition review, the staff team encountered numerous DSA quality concerns, including the following:

- Poor documentation of how hazard scenarios are dispositioned.
- Unscreened hazard scenarios not carried forward for control selection.
- Multiple, duplicate scenarios existing in the safety basis document with different control suites selected.
- Unclear documentation of control selection.
- Inappropriate use of safety management program key elements.
- Assumptions in safety basis not protected in the TSRs to show that a hazard is not credible.
- Inconsistencies between HARs on what hazard scenarios require a control.

Inconsistencies and conflicting statements between different sections of the safety basis document.

- Errors in mapping weapon response rule probabilities from the design agency document to the HAR.
- Unreferenced supporting documentation.

Additionally, while not within Pantex’s control, the quantity of different design agency-provided weapon response summary documents for each program can be cumbersome. It is not clear how and when the design agencies update their weapon response summary documents or which weapon response rule version is being implemented.

Each of these quality concerns on its own might not represent a safety issue; however, it is clear that Pantex DSAs are not consistently maintained with appropriate rigor. One way DSAs are maintained and improved is through annual updates, as required by 10 CFR 830. Specifically, 10 CFR 830 requires the M&O contractor to “[a]nnually submit to DOE either the updated documented safety analysis for approval or a letter stating that there have been no changes in the documented safety analysis since the prior submission...” [10]. In recent years,



CNS has had issues with submitting annual updates on a timely basis. For example, in a December 22, 2016, memorandum NPO identified to CNS the concern with safety basis annual update timeliness, as well as quality concerns. The memorandum identified specific examples, including the annual updates for the W80 and W78 HARs being overdue for more than four and six months, respectively [23]. Additionally, the majority of improvement activities have been de-scoped from Pantex annual updates, leaving little value-added in the update efforts besides incorporating negative USQs into HARs and SARs.

CNS recently started taking actions to address issues with the quality of DSA change package submittals [9]. Throughout 2017, NPO rejected or CNS withdrew numerous DSA change package submittals due to technical and quality issues. While recent actions that CNS has instituted are intended to improve submittal quality, these actions will not necessarily address the types of DSA quality deficiencies encountered by the staff review team.

## Appendix

### Specific Hazard Scenarios with Uncontrolled Hazards

The Board’s staff team reviewed Hazard Analysis Reports (HAR) and select portions of the Safety Analysis Reports (SAR) for five weapon programs—B61, W76, W78, W87, and W88. The staff team reviewed the hazard disposition tables and related hazard and accident analyses located in the approved HARs and SARs, and found that they contained hazard scenarios with unscreened weapon responses for inadvertent nuclear detonation (IND) and high explosive violent reaction (HEVR) consequences where safety class controls were not clearly applied. The tables below identify the specific scenarios of concern. The tables include the hazard identification number referenced in each corresponding HAR or SAR, a description of the insult type, the credited controls (if any) for high order consequences, and additional staff comments. Of note, while thorough, the staff team’s review of applicable safety basis documents is not exhaustive. Additional scenarios with similar concerns may exist.

#### W88

The Board’s staff team reviewed the W88 HAR. The HAR categorizes certain unscreened scenarios as “sufficiently unlikely” to result in weapon response with a high order consequence. In several such scenarios, although the HAR identified a control, the staff team identified an issue with the documentation of the control. For the remaining such scenarios, the HAR did not identify an appropriately documented control. In the table below, superscript numerals within each row associate applied controls to the hazard scenarios (if no superscript exists, the control applies to all listed hazards).

Hazard ID	Insult Type	Currently Applied Controls	Board’s Staff Team Comments
C.DI.6.I.06	Drop	Personnel Evacuation (Specific Administrative Control [SAC])	No safety class controls applied to mitigate/prevent high order consequences. Control of Equipment (SAC) could be applied as preventive control.
C.ADI.I.20 <sup>1</sup> C.A.22.I.11 <sup>1</sup> C.A.23.I.02 <sup>1</sup> C.A.24a.I.06 <sup>1</sup> C.A.19.I.15 <sup>1</sup> C.DI.6.I.02 <sup>1</sup> C.ADI.I.21 <sup>2</sup>	Falling Technician	Safety Management Program (SMP) Key Element (Procedures and Training)*  Nuclear Explosive Cells Facility Structure <sup>1</sup>  Personnel Evacuation (SAC) <sup>2</sup>	Facility Structure credited to mitigate HEVR consequences, but no sufficient controls applied to prevent IND or to protect facility worker from HEVR. SMP Key Element inappropriately used for risk reduction.
C.DI.7.I.04 C.ADI.I.22	General Falling Technician	Use of Process Transfer Cart (SAC)	Two example scenarios listed are not all inclusive. Use of Process Transfer Cart (SAC) applies for production technician manipulating special tooling, but does not apply for second technician without special tooling approaching unit.

<b>Hazard ID</b>	<b>Insult Type</b>	<b>Currently Applied Controls</b>	<b>Board's Staff Team Comments</b>
C.ADI.I.29	Falling Technician	Personnel Evacuation (SAC)  Procedures and Training SMP*  Conduct of Operations SMP*	No safety class controls applied to prevent/mitigate high order consequences. SMPs inappropriately used for risk reduction.
C.DI.6.G.02	Scrape	No controls applied	In response to the 11/16/2017 problem identification and evaluation entry, CNS concluded this event is not credible. The basis for this determination is unclear given the probability of insult specified in the approved HAR. As a result, no safety class controls applied to prevent/mitigate high order consequences.
C.DI.7.G.01	Scrape	Procedures and Training SMP*	No safety class controls applied to prevent/mitigate high order consequences. SMP Key Element inappropriately used for risk reduction.
C.DI.9I.I.04 <sup>1,2</sup> C.DI.9.I.08 <sup>3,4</sup> C.DI.10.I.09 <sup>3,4</sup> C.DI.10.I.10 <sup>1</sup> C.DI.11.I.08 <sup>3</sup> C.DI.12.I.06 <sup>3,4</sup> C.DI.14.G.02 <sup>3</sup> C.A.1.I.01 <sup>3,4</sup> C.A.3.G.02 <sup>3</sup> C.A.12.I.01 <sup>3,4</sup> C.A.12.I.02 <sup>3,4</sup> C.A.14.I.04 <sup>3,4</sup> C.A.16.I.02 <sup>3</sup> C.A.17.I.16 <sup>3</sup> C.ADI.I.41 <sup>1</sup> C.ADI.I.70 <sup>3</sup>	Drop, falling technician, and gouge scenarios resulting in HEVR consequences only (no IND)	Personnel Evacuation (SAC) <sup>1</sup>  SMP Key Element (Procedures and Training) <sup>2,*</sup>  Procedures and Training SMP <sup>3,*</sup>  Conduct of Operations SMP <sup>4,*</sup>	The Nuclear Explosive Cells Facility Structure could be credited to mitigate HEVR consequences to the public but would not protect the facility worker.
C.DI.12.I.03 C.DI.15.I.02 C.A.2.I.03 C.A.3.I.04 C.A.4.I.06 C.A.10.I.02	Drop and falling technician scenarios resulting in HEVR consequences only (no IND)	No controls applied	The Nuclear Explosive Cells Facility Structure could be credited to mitigate HEVR consequences to the public but would not protect the facility worker.

\*SMP Key Element (Procedures and Training) or SMPs (Procedures and Training or Conduct of Operations) are discussed in the HAR as a reason to accept the risk without applied safety class controls. It is not clear where attributes of the Procedures and Training Key Element are developed for specific application to W88 operations (i.e., neither in W88 HAR nor Sitewide SAR).

Source: (U) W88 Disassembly & Inspection and Assembly Hazard Analysis Report, AB-HAR-941335, Issue 28, January 31, 2018.

Extent of Condition Review for Hazards without Identified Safety Controls

Based on the concerns identified in the W88 HAR, the Board’s staff team conducted an independent extent of condition review. Members of the Board’s staff reviewed the B61, W76, W78, and W87 HARs, associated nuclear explosive operating procedures, and sections of applicable SARs. Through this review, the staff team identified similar scenarios on each of the analyzed programs with the exception of the B61.

**B61**

After a preliminary review of the B61 HAR, the staff team identified discrepancies in the identification of controls for scenarios with sufficiently unlikely weapon response but did not identify concerns related to the application of a sufficiently unlikely weapon response without appropriately identified implemented safety controls. The hazard scenarios below include safety basis quality issues.

Hazard ID	Insult Type	Currently Applied Controls	Board’s Staff Team Comments
5324 5325 5329 5342 5526 5529 5557 5558 5571 5572 5799 12716	Drop / Pressure of Force	Special tooling	Special tooling has safety significant functional requirements to address low order consequences but is not designated safety class because the HAR asserts that high order consequences are sufficiently unlikely. Based on the specifications of the special tooling program, there are limited differences between analysis activities required to meet safety significant functional requirements and safety class functional requirements. Additionally, each of the tools relied upon to prevent the accident have other safety class functional requirements applied for other hazard scenarios.

5333	Impact or Crush by an Object (hose whip)	Safety Cable, Tyrap, Filament Tape, Material Access Area Operations Requirement (Sitewide SAR)	This scenario, as listed in the HAR, is controlled for several other weapon configurations. Authorization Basis Change Packages 18-06 and 17-62 implement a new control suite to require air hose restraints to be used, including step-by-step implementation with two technician verification. Per the new control description, as specified in B61 HAR section 4.3.1 and Sitewide SAR section 4.3.50, the controls do not explicitly apply to the ultimate user configuration; however, Hazard ID 5333 applies to the ultimate user configuration and lists HEVR and IND consequences as sufficiently unlikely. Rule 2.7.1 in GE1A4947, (U) General Engineering, Weapon Response Summary, B61, Issue C, indicates that this hazard screens in this configuration.
------	--	--	--

Source: (U) B61 SS-21 Hazard Analysis Report, AB-HAR-940572, Issue 44, January 18, 2018.

**W76**

The staff team identified the following hazard scenarios during W76 operations that have inadequate controls assigned.

Hazard ID	Insult Type	Currently Applied Controls	Board's Staff Team Comments
2.1.16.3 2.1.17.3 2.1.18.3	Mechanical Impact	Facility Structure	Section 3.4.2.2.6 of the HAR states: "Given the nature of these operations and the actions that would be required to produce a weapon response, no additional Task Exhaust or Pump Fixture controls are assigned to further reduce the potential for an impact from these items. The event contributors for Rules 2.1.16.3, 2.1.17.3, 2.1.18.3, 2.1.20.3, and 2.1.21.3, which are all uncased [high explosive] configurations, are dominated by an impact from a Production Technician that trips and falls into the uncased HE configuration. No controls were identified that could further reduce the potential for a trip." Facility Structure is credited to mitigate HEVR consequences, but no sufficient controls are applied to prevent IND or to protect facility worker from HEVR.

Hazard ID	Insult Type	Currently Applied Controls	Board's Staff Team Comments
2.1.13.8 2.1.14.11 2.1.14.16 2.1.14.2 2.1.14.4 2.1.23.16 2.1.23.18 2.2.2.21 2.2.2.24 2.2.5.8	Mechanical Impacts to the CSA	Personnel Evacuation (SAC)	The referenced scenarios list a Burning Dispersal response of sufficiently unlikely; however, the applicable weapon response summary document lists the burning dispersal response as screened. The prior revision of the weapon response summary document lists the burning dispersal response as sufficiently unlikely, so the HAR appears to present outdated information.
2.2.2.22	Mechanical Drop/Topple/Swing/Push	Personnel Evacuation (SAC)	The referenced rule is not listed in the referenced weapon response summary document. The prior revision of the weapon response document contained a rule that was formerly applicable. Based on the current weapon response summary document, the staff team concluded there is no control deficiency in this instance.

Source: (U) W76-0/1 SS-21 Assembly, Disassembly & Inspection, and Disassembly for Life Extension Program Operations Hazard Analysis Report, RPT-HAR-255023, Issue 71, November 30, 2017.

## W78

The staff team identified the following hazard scenarios during W78 operations that have inadequate controls assigned.

Hazard ID	Insult Type	Currently Applied Controls	Board's Staff Team Comments
B.2.H.1 B.3.H.1 B.4.H.1	Exothermic Reaction	Sufficient control set for HEVR	The HAR inappropriately uses combined frequency (i.e., initiating event frequency with weapon response) to remove IND from further consideration. However, sufficient controls applied for HEVR consequences.
Sitewide SAR (Rule 4.4.3)	Lightning	W78 Transportation Configuration	The HAR asserts that the mitigated weapon response, with the applied control, is sufficiently unlikely, so no additional controls were applied. Similar concerns apply to other weapon programs.
Transportation SAR (Rule 3.1.3)	Hydraulic Fluid Fire	No controls applied	No controls applied for high order consequences. According to the Transportation SAR, "Based on weapon response, no credible response as frequency is Sufficiently Unlikely." Similar concerns apply to other weapon programs.

Source: (U) W78 Step II Disassembly & Inspection and Repair Hazard Analysis Report, AB-HAR-319393, Issue 63, September 22, 2017; (U) Transportation SAR, AB-SAR-940317, Issue 81, September 19, 2017; (U) Sitewide SAR, AB-SAR-314353, Issue 288, January 31, 2018.

**W87**

The Board’s staff team reviewed the disassembly portion of the W87 HAR. Although not reviewed, similar concerns likely exist with the assembly portion of the W87 HAR. The identified hazard scenarios of concern apply a sufficiently unlikely weapon response for a high order consequence. In several instances, the control set is adequate; however, there is a safety basis quality issue with the documentation of the control. With the remaining instances, a sufficiently unlikely weapon response for a high order consequence exists without an appropriately documented control.

Hazard ID	Insult Type	Currently Applied Controls	Board’s Staff Team Comments
B.ISMO.14.D.02 B.ISMO.16.D.02	Drop of unit	Special Tooling  Verification of Proper Installation of the Nuclear Explosive/Tooling Interface (SAC)	While the staff team believes the control set to be adequate, the documentation of the hazard scenario does not appear to be fully developed. Tables 3.4.2.2.3-5 and -6 of the HAR state that the particular high order consequence related to the sufficiently unlikely weapon response is not carried forward for further evaluation, i.e., control selection.
D32WS-48 D32WS-52 D32WS-86  D32WS-100 D32WS-129	Drop of weapon component and/or tooling onto configuration  Falling technician	No controls applied	Table 3.4.2.1.3-3 of the HAR states that the particular high order consequence related to the sufficiently unlikely weapon response is not carried forward for further evaluation, i.e., control selection.

<b>Hazard ID</b>	<b>Insult Type</b>	<b>Currently Applied Controls</b>	<b>Board's Staff Team Comments</b>
<p>B.ISMO.24.I.03 (3rd instance, Rule 2.1.4.26a)</p> <p>B.ISMO.24.I.09 (1st instance, Rule 2.1.4.25a)</p> <p>B.ISMO.24.I.09 (2nd instance, Rule 2.1.4.25a)</p> <p>B.ISMO.24.I.09 (3rd instance, Rule 2.1.4.25a)</p>	<p>Drop of weapon component and/or tooling onto configuration</p> <p>Falling Technician</p>	No controls applied	<p>Table 3.4.2.1.3-4 of the HAR states that the particular high order consequence related to the sufficiently unlikely weapon response is not carried forward for further evaluation, i.e., control selection.</p> <p>An example of special tooling that could be dropped and result in an impact to the sensitive area of the component (per CODT-2004-0295 Rev. 6, the LLNL weapon response summary document) is any of the three guide bearings during their removal. The removal of the guide bearings occurs after a protective cover (Skull Cap) has been removed, but before the component is removed. Note that the Skull Cap is not a credited safety class control. The Skull Cap is analyzed for a particular force but has not been evaluated to ensure it could perform a safety requirement if needed.</p> <p>For a falling technician, the impact location is not controlled to prevent impact to the sensitive area.</p>
N/A	Drop of hand tool onto sensitive area of component	No controls applied	HAR does not include this scenario for the unique operation and configuration analogous to Hazard ID D32WS-86 above.
D32WS-70	Drop of flashlight with electrical coupling	Approved Equipment Program	Section 3.3.2.1 of the HAR states that the electrical hazard is sufficiently unlikely, and therefore, not carried forward for further evaluation. CODT-2004-0295 Rev. 6 states that the weapon response does not screen. However, CODT-2004-0295 Vol. 2 Rev. 3 clarifies that the weapon response screens. The staff team concluded that the scenario does screen, but the discussion in Section 3.3.2.1 is inappropriate, and lack of a singular weapon response summary document makes for unclear documentation.
D33WSa-18 D34WS-12 D34WS-14	Drop of weapon component and/or tooling onto configuration	No controls applied	Table 3.4.2.1.3-3 in the HAR states that the high order consequence is sufficiently unlikely and the hazard is not carried forward for further evaluation.



<b>Hazard ID</b>	<b>Insult Type</b>	<b>Currently Applied Controls</b>	<b>Board's Staff Team Comments</b>
D34WS-41	Falling technician while carrying special tooling (metal with hard corners/edge)	No controls applied	Table 3.4.2.1.3-3 in the HAR states that the high order consequence is sufficiently unlikely and the hazard is not carried forward for further evaluation.
N/A	Falling technician resulting in an impact to the sensitive area of component	No controls applied	<p>The HAR's Appendix does not include this scenario for the unique operation and more sensitive orientation (after rotating) of configuration analogous to Hazard ID D34WS-41 above.</p> <p>Similar hazard scenarios (D34WS-43, D34WS-50, D34WS-60) assume the technician will only impact the side of the unit. The staff team believes a direct impact from a falling technician to the sensitive area is a credible hazard.</p>
B.ISMO.26.I.01	Drop of Hand Tool onto configuration	No controls applied	<p>The HAR's Appendix states that the orange stick is the only tool used during this configuration and that weapon response "a" applies. The staff team notes that the selected weapon response (2.1.5.15) does not relate to the discussion in the HAR's Appendix.</p> <p>The more sensitive orientation (after rotating) is not considered. The staff team believes that given the postulated energies, weapon response 2.1.5.11b would be applicable. That response is applicable because any postulated impact could occur over the sensitive area. However, if the orange stick is the only tool that can be used in this task, then this hazard scenario would not be credible.</p>

<b>Hazard ID</b>	<b>Insult Type</b>	<b>Currently Applied Controls</b>	<b>Board's Staff Team Comments</b>
B.ISMO.26.I.03	Drop of special tooling onto configuration	No controls applied	The HAR's Appendix states that the design of the tool prevents a direct impact to the sensitive area of the component; therefore, weapon response "a" is applied. There is not an adequate basis for this assertion. While the weapon response summary document provides a probe size example, it also states the "b" weapon response applies if the insult is over the sensitive area. The staff team believes the special tooling could impact the sensitive area; therefore, weapon response "b" should be applied. Additionally, the tooling has sharp (i.e., 90 degree) corners.
N/A	Technician trips resulting in an impact to the sensitive area of component	No controls applied	The HAR's Appendix does not include this scenario for the same configuration and orientation analogous to Hazard ID B.ISMO.26.I.03 above.
N/A	Mechanical impact due to hand tool drop	No controls applied	Rule 2.1.5.24a is not referenced in the HAR's Appendix. However, the "a" weapon response is used to develop the impact scenario frequencies in Table 3.4.2.1.3-2. There is not an adequate basis for the selection of the "a" weapon response usage. The reviewers believe the special tooling could impact the sensitive area; therefore, weapon response "b" should be applied. Additionally, most articles of tooling have sharp (i.e., 90 degree) corners.

Source: (U) W87 Step II Assembly and Disassembly & Inspection Hazard Analysis Report, AB-HAR-940626, Issue 41

## References

- [1] Defense Nuclear Facilities Safety Board, *Review of Hazard Analysis Reports, Pantex Plant*, Washington, DC, July 6, 2010.
- [2] Department of Energy, *Hazard Analysis Reports for Nuclear Explosive Operations*, DOE-NA-STD-3016-2006, Washington, DC, 2006.
- [3] Department of Energy, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, DOE-STD-3009-1994 Chg Notice 3, Washington, DC, 2006.
- [4] Tiffany Wyatt, Babcock & Wilcox Technical Services Pantex, LLC, *Documented Safety Analysis Upgrade Initiative Project Plan*, Issue 3, Pantex Plant, May 17, 2011.
- [5] Authorization Basis Department, Babcock & Wilcox Technical Services Pantex, LLC, *The Documented Safety Analysis Improvement Plan (DSAIP)*, Revision 1, Pantex Plant, July 25, 2013.
- [6] Safety Analysis Engineering Department, Consolidated Nuclear Security, LLC, *The Documented Safety Analysis Improvement Plan (DSAIP)*, Revision 3, Pantex Plant, February 16, 2015.
- [7] Safety Analysis Engineering Department, Consolidated Nuclear Security, LLC, *The Documented Safety Analysis Improvement Plan (DSAIP)*, Revision 4, Pantex Plant, February 29, 2016.
- [8] Safety Analysis Engineering Department, Consolidated Nuclear Security, LLC, *The Documented Safety Analysis Improvement Plan (DSAIP)*, Revision 5, Pantex Plant, September 21, 2017.
- [9] Memorandum from M.S. Beck to K.D. Ivey, *Quality of Pantex Safety Basis Submittals*, Pantex Plant, February 20, 2018.
- [10] Title 10, Code of Federal Regulations, Part 830, *Nuclear Safety Management*, January 1, 2011.
- [11] Department of Energy, *Hazard Analysis Reports for Nuclear Explosive Operations*, DOE-NA-3016-2016, Washington, DC, 2016.
- [12] NNSA Production Office, *Justification for Continued Operations for W88 Uncased HE Operations*, PX-JCO-17-09, Pantex Plant, May 2017.

- [13] Consolidated Nuclear Security, LLC, *Problem Identification and Evaluation Processing Form*, Review ID 20392, Pantex Plant, January 16, 2018.
- [14] Consolidated Nuclear Security, LLC, *Falling Man Awareness Training*, PX-3864, Pantex Plant, 2014.
- [15] Defense Nuclear Facilities Safety Board, *Letter from Peter S. Winokur to Frank G. Klotz*, Washington, DC, June 2, 2014.
- [16] NNSA Nuclear Explosive Safety Study Group, *Nuclear Explosive Safety Master Study of the Approved Equipment Program at the Pantex Plant Volume II - Special Tooling*, Pantex Plant, May 31, 2013.
- [17] Department of Energy, *Specific Administrative Controls*, DOE-STD-1186-2016, Washington, DC, December 2016.
- [18] Department of Energy, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*, DOE-STD-3009-2014, Washington, DC, 2014.
- [19] Defense Nuclear Facilities Safety Board, *Pantex Plant Activity Report for Week Ending April 20, 2018*, Pantex Plant, April 2018.
- [20] Department of Energy, *Implementation Guide for Use In Addresssing Unreviewed Safety Question Requirements*, DOE-G-424.1-1B, Chg. Notice 2, Washington, DC, 2013.
- [21] Consolidated Nuclear Security, LLC, *Pantex Plant Unreviewed Safety Questions Procedure*, CD-3014, Pantex Plant, July 2017.
- [22] Consolidated Nuclear Security, LLC, *DNFSB Member Visit to Pantex - Joyce Connery*, Pantex Plant, February 2018.
- [23] Memorandum from K.A. Hoar to J. Papp, *NNSA Production Office Expectations for Pantex Documented Safety Analysis (DSA) Annual Updates*, Pantex Plant, December 22, 2016.

# DEFENSE NUCLEAR FACILITIES SAFETY BOARD

## Staff Issue Report

**SUBJECT:** Nuclear Safety Management at the Pantex Plant

The Defense Nuclear Facilities Safety Board (Board) approved the conduct of a safety investigation (preliminary safety inquiry) regarding the implementation of Title 10, Code of Federal Regulations, Part 830 (10 CFR 830), *Nuclear Safety Management*, for nuclear explosive operations at the Pantex Plant located near Amarillo, Texas [1]. Overall, the staff team found that (1) portions of Pantex safety bases are deficient; (2) multiple components of the safety basis process are deficient; and (3) the National Nuclear Security Administration (NNSA) Production Office (NPO) and the contractor, Consolidated Nuclear Security, LLC (CNS), have been unable to resolve known safety basis deficiencies.

**Pantex Safety Basis Requirements.** Table 2 of 10 CFR 830, Subpart B, *Safety Basis Requirements*, prescribes the methodologies and requirements for preparation of safety analysis reports (SAR) and hazard analysis reports (HAR) for nuclear explosive facilities and operations. SARs are required for the facilities associated with nuclear explosive operations. These SARs include the *Sitewide SAR*, *Bays and Cells SAR*, and various special purpose nuclear facility SARs. An approved method of meeting the requirements of 10 CFR 830 for SARs is described in Department of Energy (DOE) Standard 3009, *Preparation Guide for US Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports* [2]. HARs are required for specific nuclear explosive operations. Hazard analysis teams prepare HARs using weapon response inputs from the associated weapon design agencies. An approved method of meeting the requirements of 10 CFR 830 for HARs is described in DOE Standard 3016, *Hazard Analysis Reports for Nuclear Explosive Operations* [3].

**Review Scope.** The staff team reviewed the following areas in assessing compliance with 10 CFR 830:

- *Controls to Prevent/Mitigate Unscreened Weapon Hazard Scenarios.* The staff team selected two HARs (i.e., W76 and W78) for review [4, 5]. It evaluated the hazard analyses in the HARs for events that result in inadvertent nuclear detonation (IND) and/or high explosive violent reaction (HEVR). For each event that was not screened as physically incredible by the weapon design agency, the staff team evaluated the adequacy of the safety control set to prevent or mitigate the event. Identification of hazard controls to ensure adequate protection of workers and the public is required by 10 CFR § 830.204.
- *Implementation of USQ Process.* An unreviewed safety question (USQ) process is required by 10 CFR § 830.203 to ensure that operations are conducted within the DOE-approved safety basis. The staff team evaluated the USQ process implemented at Pantex. It reviewed USQ procedures, specific deficiencies identified in a potentially inadequate safety analysis (PISA), and justifications for continued operations (JCO).

- *Safety Basis Maintenance.* SARs and HARs are required to be updated and maintained in accordance with 10 CFR § 830.202. These requirements obligate the contractor annually to submit updates or a letter stating no changes have been made since the last submittal. The staff team reviewed safety basis maintenance to include annual updates and improvement plans.

The staff team reviewed the pertinent documents, prepared agendas, and held onsite discussions with representatives from NPO and CNS. It conducted the onsite visits during the weeks of May 28 and June 11, 2018. The onsite visits included observing nuclear explosive operations involving the W76 and W78 programs.

**Conclusions.** The staff team found that (1) portions of Pantex safety bases are deficient; (2) multiple components of the safety basis process are deficient; and (3) NPO and CNS have been unable to resolve known safety basis deficiencies. The conclusions are summarized below with the detailed evidence to follow:

- **Portions of the safety bases are deficient in meeting 10 CFR § 830.204(b).** There are high consequence hazards that (1) are not adequately controlled; (2) may have controls, but the controls are not clearly linked to the hazards; and (3) have controls that are not sufficiently robust or that lack sufficient pedigree to reliably prevent or mitigate the event. This conclusion is supported by observations 1 through 6 below.
- **Multiple components of the safety basis process are deficient.** (1) Contrary to 10 CFR § 830.202(c), CNS has failed to update annually the HARs and SARs. (2) Contrary to 10 CFR § 830.203(g), Pantex USQ procedures allow three days to correct discrepant-as-found conditions or implementation/execution errors without stopping operations, notifying DOE, or issuing a PISA. (3) Contrary to DOE G 424.1-1B, NPO and CNS revise existing JCOs instead of issuing new ones, thereby extending the expiration date and reliance on the compensatory measures beyond a year. (4) Contrary to DOE Guide 423.1-1B, CNS does not re-assess procedural controls via implementation verification reviews (IVR) every three years. This conclusion is supported by observations 7 through 10 below.
- **NPO and CNS have been unable to resolve known safety basis deficiencies.** (1) NPO and CNS have been unable to resolve several legacy conditions of approval (COA). (2) CNS has a *Documented Safety Analysis Improvement Plan* (DSAIP) that lacks sufficient information and resource loading required for the process to be successful, and is behind schedule. (3) Despite the fact that issues related to falling technician accident scenarios were identified in 2010, there is no timeline for improvements to be incorporated into the safety basis. This conclusion is supported by observation 11 below.

Eleven observations noted by the staff team over the course of the review support these conclusions:

1. *Missing Specific Administrative Control (SAC) for Operators Applying Brakes on Testers*—The W76 HAR identifies multiple events with credible IND and HEVR consequences that require safety-class controls but are prevented by an initial condition. The initial condition is a safety management program (SMP) (i.e., Electrical Equipment Program for Testers). The SMP ensures that the design of electrical testers (e.g., PT3746 Preset Tester) precludes mechanical and electrical insults to the weapon. The initial condition in the HAR references Section 18.2.3 of the *Sitewide SAR*. The *Sitewide SAR*, Page 18-16, states that testers are “[d]esigned to withstand the forces of a 95th percentile person falling into the tester without the tester tipping or moving the target” [6]. However, this analysis relies on the operator engaging a wheel locking device. Therefore, the design requirements contained in the SMP are insufficient as the lone control for this event. The operator action of engaging the wheel locking device is not protected by a SAC and is not marked as a critical step in the procedures. Additionally, the tester is not credited as a safety-class design feature in the hazard analysis tables. The review team concludes the safety control set for these events does not meet DOE requirements. CNS generated a problem identification and evaluation (PIE) form (PIE-18-537) and issued a PISA following the onsite discussions. The PISA was followed by a positive USQ determination.

2. *Analysis Supporting Adequacy of Safety-Class Carts not Bounding*—The W78 HAR includes events involving toppling of a preparation cart while carrying various items. The weight of the cart and items on top of it are assumed to impact a weapon configuration. This event results in the need for safety-class controls since IND and HEVR are not screened by the design agency. The preventive control for this event is the design of the preparation cart. The HAR, Section 4.3.1.1.2, credits the preparation cart with the functional requirement to “...withstand the forces imparted by a 95th percentile Production Technician as well as the forces due to a PC-3 [performance category-3] seismic event without toppling into the unit.” However, the assumed weight of the items on the cart in the HAR event exceeds the assumed weight in the supporting engineering analysis [7]. Therefore, the engineering analysis does not adequately demonstrate the preparation cart is capable of fulfilling its safety functional requirements. CNS generated a PIE form (PIE-18-539) and issued a PISA following the staff team’s onsite discussions. CNS followed the PISA with a positive USQ determination.

3. *Missing Safety-Class Controls for Impact and Electrostatic Discharge (ESD) Events*—The W76 HAR identifies rolling impact and ESD events involving a weapon configuration that represents a general bin of 16 separate configurations. The rolling impact is caused by production technicians pushing “freestanding equipment” into the 16 different weapon configurations. Freestanding equipment is defined as equipment or tooling not attached to the facility and not hand carried. The rolling impact events require safety-class controls since the design agency did not screen them for IND and HEVR. The ESD events are postulated from production technicians being in contact with freestanding equipment or the wrist strap checker. Since the design agency did not screen ESD events for tritium or mechanical releases and worker safety, ESD events require safety significant controls. The preventive control for the rolling impact and ESD events is a SAC (i.e., W76 Operations - Control of Equipment and Tooling). Among other requirements, this SAC prohibits freestanding equipment not required by the W76

process from being placed within 6.5 feet of any W76 configuration installed in the assembly stand, insertion cart, or assembly carts. Designating this SAC for these events as a preventive control results in several errors:

- The SAC does not include all freestanding equipment that could cause a rolling impact or ESD event (e.g., a tool box) to the weapon configurations. Therefore, this freestanding equipment excluded from the SAC represents an uncontrolled hazard.
- The ESD event involving a wrist strap checker credits the SAC as a preventive control, but the SAC does not include the wrist strap checker in the list of included equipment. Therefore, the wrist strap checker needs to be added to the SAC. The *Nuclear Explosive Operating Procedures* (NEOPs) and other technical procedures do include a safety requirement for production technicians to not bring the wrist strap checker near the weapon. However, this requirement does not flow down from this SAC.
- The SAC states that the 6.5-foot exclusion zone applies to W76 configurations installed in the assembly stand, insertion cart, or assembly carts. Although the majority of the 16 weapon configurations are processed in an assembly cart, the components that make up these configurations are processed on a bench or table. The SAC does not apply to operations on a bench or table.
- Some tools included in the list of freestanding equipment do not have wheels. Therefore, it is inappropriate to include these pieces of equipment in rolling impact events.

CNS generated a PIE form (PIE-18-536) and issued a PISA following the onsite discussions. The PIE form states: “A PISA was declared on 5/31/18, which resulted in pausing W76-0/1 Mechanical Assembly and Disassembly bay operations until operational restrictions were implemented.” CNS followed the PISA with a positive USQ determination.

*4. Non-Credited Administrative Controls/Training Used in Place of Safety-Class Controls for ESD Hazards*—The W76 HAR identifies multiple events with credible IND and HEVR consequences that are dispositioned by a “Category 2 Equipment Evaluation.” These events require safety-class controls since the design agency did not screen them for IND and HEVR. The hazard analysis tables contain a note that refers to equipment evaluations for the Overhoff monitor/hose and wrist strap checkers (i.e., EEE-06-0030 and EEE-06-0037, respectively) [8, 9]:

- EEE-06-0030 provides “General Requirements” that prescribe keeping the Overhoff more than 6.5 feet away from a nuclear explosive during “Radiation Safety Usage.” During “Manufacturing Usage” the Overhoff may make contact with a nuclear explosive using a short hose, which has a credited insulator. CNS personnel explained that during “Manufacturing Usage” the production technicians hold the Overhoff in one hand while guiding the hose to the nuclear explosive with the other hand (within 1/4 inch of the nuclear explosive). The NEOPs do not include safety



requirements, critical steps, warnings, cautions, or general notes that alert the production technicians to potential hazards associated with dropping the Overhoff onto the nuclear explosive. CNS personnel stated in onsite discussions that hazards involving the Overhoff are not credible due to its intended use and production technicians' "normal behavior" via training; thus no control is identified for this hazard.

- EEE-06-0037 prescribes a 6.5-foot standoff distance for the wrist strap checker from all explosives and nuclear explosives and references P7-2003, *Weapon Assembly/Disassembly Operations Requirements* (U) [10], as the implementing procedure. P7-2003 is a general use level procedure that implements the standoff distance requirement for the wrist strap checker via a boxed note. The staff team also reviewed the NEOPs that are critical use level procedures (higher level than general use). The staff team found that the NEOPs include a safety requirement to not carry the wrist strap checker to the unit. The production technicians are required to be familiar with the NEOP safety requirements, but they are not required to read them prior to performing NEOP steps. The NEOPs also do not specify a specific standoff distance (i.e., 6.5 feet). The wrist strap checker is secured to the wall in a bracket but may need to be removed for calibration. CNS personnel stated that production technicians and calibration technicians are trained to not bring the wrist strap checker within 6.5 feet of a nuclear explosive, referencing TABLE- 0068, *Safety Checklist*, which contains additional requirements for maintaining a 6.5-foot standoff distance to a nuclear explosive [11]. TABLE-0068, however, is not part of the technical safety requirements (TSR) for nuclear explosive operations.

The staff team finds that Pantex personnel ultimately rely on non-credited administrative controls and production technician training to implement safety-class functional requirements for HAR events involving the Overhoff monitor/hose and wrist strap checkers. There are no credited safety-class controls for these events. The review team concludes that this situation does not meet DOE requirements for identification of safety-class controls for high consequence events, and as such represents a PISA. CNS has not declared a PISA regarding its controls for these hazards.

5. *Missing Safety-Class Controls for Production Technician Tripping Hazards*—The W78 HAR identifies multiple events involving a production technician who trips and impacts the unit in various configurations. This event results in the need for safety-class controls since IND and HEVR are not screened by the design agency. The hazard analysis tables do not identify controls specific to these events. Instead, the hazard analysis tables refer to Section 3.4.2.4 of the HAR, dedicated to evaluating impact hazards. Section 3.4.2.4 lists the identified controls for this hazard. After reviewing the list of controls, the most applicable control is a SAC (i.e., W78 Process - Tripping Hazards), designated in the HAR to perform functions equivalent to a safety-significant control. This SAC requires production technicians to check for tripping hazards once per shift.

The staff team traced the SAC requirement to NEOPs. The NEOPs do contain critical steps in their setups that require signature for ensuring tripping hazards have been removed.

However, if this SAC is implemented to prevent the event (i.e., production technician trip), it would be an inadequate safety-class preventive measure because it does not prevent the tripping hazards from accumulating during operations. As a result, the review team concludes that the events involving a production technician trip are uncontrolled. During onsite discussions, Pantex personnel agreed that they do not have adequate controls in place for tripping events identified in the HAR. However, CNS personnel stated that this is a known deficiency and a JCO is being developed. Per 10 CFR § 830.203(g), the contractor is required to enter the PISA process and implement operational restrictions prior to issuing a JCO. The review team concludes that this situation does not meet DOE requirements and as such represents a PISA. CNS has not declared a PISA regarding its controls for these hazards.

6. *Drop Hazards*—The W78 HAR identifies several drop events involving a shielded apron or various pieces of equipment, tooling, or materials impacting weapon configurations from a height of two or four feet. These events result in the need for safety-class controls since the design agency did not screen them for high order consequences. A SAC (i.e., W78 Process - Hand Lifts) is one of the credited controls to prevent this event. The SAC flows down to safety requirements at the beginning of the NEOPs. The SAC justifies reliance on production technician training by stating:

*With the training to the technicians on not lifting hand tools, tooling, and materials over the unit unless required for the process and to only lift the object as high as required for the operation, both the frequency of a drop that would impact the units [is] reduced, and the possible impact energy is reduced if a drop were to occur....Based on the height of the unit being worked on, there would be no reason to lift the hand tooling 2 feet over the unit and it would be an unnatural act to do so. It is not considered credible that the tooling would be lifted more than 2 feet over the unit and dropped.*

Similarly, although not explicitly stated in the SAC, the NEOPs also cite a specific safety requirement for the shielded aprons to be relocated to staging cubicles or corridors out of direct line of sight of the cells when not in use. However, contrary to MNL-293084, *Pantex Writer's Manual for Technical Procedures*, the NEOPs do not provide critical steps or warnings when handling the specific equipment or materials, that when dropped, could initiate a high order consequence [12]. The staff team discussed the shielded apron and six different individual pieces of equipment considered in the HAR during the site visit. CNS stated that the production technicians are sufficiently trained to not lift items more than 2 feet over the weapon. Given the high consequences, the SAC would be strengthened by adding additional specificity (e.g., do not lift equipment higher than a set height above the weapon). In addition, consistent with MNL-293084, the NEOPs should include critical steps or warnings when handling specific equipment or materials that could initiate a high order consequence if dropped.

7. *Process for Discrepant As-Found Conditions*—The site USQ procedure, approved by NPO, does not comply with the requirements of 10 CFR 830 or recommendations of DOE Guide 424.1-1B, *Implementation Guide for Use in Addressing Unreviewed Safety Question*

*Requirements* [13].<sup>10</sup> In situations when a “discrepant as-found condition” is observed for a TSR-related control, the procedure allows returning the system to the original condition as described in the documented safety analysis (DSA) within three days without having to declare a PISA, formally notifying DOE, performing an extent of condition review, or implementing any compensatory measures.

10 CFR § 830.203, Unreviewed Safety Question Process, requires the contractors to “establish, implement, and take action consistent with a USQ process that meets the requirements of this section.” Paragraph (g) of this section states: “If a contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility discovers or is made aware of a potential inadequacy of the documented safety analysis, it must:

1. Take action, as appropriate, to place or maintain the facility in a safe condition until an evaluation of the safety of the situation is completed;
2. Notify DOE of the situation;
3. Perform a USQ determination and notify DOE promptly of the results; and
4. Submit the evaluation of the safety of the situation to DOE prior to removing any operational restrictions....”

CNS has prepared a USQ procedure, CD-3014, *Pantex Plant Unreviewed Safety Question Procedure* [14], approved by NPO, that does not comply with the requirements of 10 CFR 830. More specifically, Procedure CD-3014 allows the following:

*If the discrepant as-found condition can be restored to be within the DSA in a matter of hours, not to exceed three business days, a PISA does not exist [emphasis added]. This is limited to conditions where 1) an SSC [structure, system, or component] does not conform to the documented design description and specifications, or 2) implementation/execution errors, for which any immediate actions taken would be to return the facility to conditions described in the DSA. When the determination is made that the discrepant as-found condition can be fixed in three business days or less, the affected operations are restricted until actions are completed to restore compliance.*

This contractor procedure and its NPO approval do not comply with the four fundamental elements of the USQ process as established by 10 CFR 830:

- The Pantex procedure restricts operations whereas 10 CFR 830 requires the contractor to place or maintain the facility in a safe condition.
- The Pantex procedure does not require DOE to be notified of the discrepancy and actions taken. As a result, CNS may operate the facility up to three days outside the DOE approved safety basis without DOE’s formal knowledge of the situation.

---

<sup>10</sup> CNS has prepared, and NNSA has approved, a USQ procedure for the Y-12 National Security Complex that contains the same deficiency and inconsistency with the requirements of 10 CFR 830.

- The Pantex procedure states that a PISA does not exist when a discrepant as-found condition can be resolved within three business days, whereas following 10 CFR 830 would result in a PISA followed by a USQ determination.
- The Pantex procedure does not require evaluation of the safety of situation for submittal to DOE prior to removing the self-established operational restrictions, whereas 10 CFR 830 requires DOE's acknowledgement of the safety of the situation prior to the contractor removal of the operational restrictions.

During the discussions at the site, CNS and NPO personnel referred to an approval memorandum received from the NNSA Chief of Defense Nuclear Safety (CDNS) for application of the three-day grace period for not issuing a PISA. The CDNS memorandum [15], however, refers to conditions that involve defense in depth or other non-safety SSCs because those SSCs “wouldn't have LCOs [limiting condition for operations] associated with them but will normally wear out, or may be non-conforming for some other reason.” While the CDNS's concurrence with a situation that involves non-safety related controls may be justified, its extension by Pantex to safety-related and TSR controls is not permitted by DOE requirements of 10 CFR 830.

Additionally, Appendix C to CNS's USQ procedure, CD-3014, describes the PIE process that is a precursor to identification and declaration of a PISA. As part of the PIE process an inquiry is made [16]: “Does the situation indicate a directive action Specific Administrative Control (SAC) may not provide the safety function assigned to it within the DSA?” If the answer is “yes” a PISA is declared. The staff review team concludes that, consistent with DOE requirements, SACs perform a safety-class or safety-significant function and are part of the TSRs of the facility. SACs should not be subject to the USQ or PISA process; however, the analysis that led to the derivation of the SAC may be subject to the USQ/PISA process if the analysis is found to be incorrect. Any change to a SAC in order to perform its intended safety function should be considered a TSR change and must be approved by DOE. 10 CFR § 830.205, Technical Safety Requirements, mandates contractors to “(2) Prior to use, obtain DOE approval of technical safety requirements and any change to technical safety requirements; and (3) Notify DOE of any violation of a technical safety requirement.” This section of 10 CFR 830 is stand-alone and specific to the TSRs; it stands apart from the USQ process, (i.e., Section 203 of 10 CFR 830). As such, the staff team concludes that 10 CFR 830 requires a TSR violation to be directly reportable to DOE, and outside the USQ process.

An example of mistreating safety-related controls by using the USQ procedure CD-3014 occurred when a piece of safety-related electrical equipment failed testing in accordance with the in service inspection (ISI) requirement of the TSR for its commercial grade dedication. CNS issued a PISA on March 10, 2017, followed by a USQ determination [17], which CNS determined was negative and did not submit for DOE approval. The USQ determination stated that the piece of equipment credited was “redundant” and that CNS at a later date would provide DOE “a change to Chapter 4 of the Sitewide SAR to delete [this piece], add [another piece of equipment] as a reference, and delete the ISI to inspect from the TSRs....”

DOE Guide 424.1-1B identifies that a failure of a safety-related control, identified in Chapter 4 of the DSA and part of the TSRs, would be reportable to DOE upon verification under a positive USQ determination. Revision of the associated TSR for the failed equipment and replacement by the new piece are required to be completed and approved by DOE before lifting operational restrictions, and not at some later date when the DSA or the *Sitewide SAR* is revised. The staff review team notes that CNS has not successfully revised the Pantex *Sitewide SAR* via an annual update since 2014, and DOE has not approved the changes CNS has proposed in the last three years (including the change described above). Consequently, discrepancies exist between the approved *Sitewide SAR* and its associated set of controls (i.e., the failed equipment) and the contractor's set of controls relied on to support ongoing operations (i.e., the redundant equipment).

8. *Long Term JCOs*—Some JCOs last for several years without updating the relevant safety basis document, relying on compensatory measures without implementing rigorous controls (e.g., engineered design features). Section 7 of CD-3014 states that “[t]he purpose of a JCO is to make a temporary (i.e., less than one year) change to the facility safety basis that would allow the facility to continue operating...” This statement, however, is not codified to lead to closure of the JCOs within a certain period of time (i.e., less than one year) or incorporate the open JCOs into the next annual update of the safety basis documents as required by DOE.

Per 10 CFR § 830.202, Safety Basis, the contractors are required to “(1) [u]pdate the safety basis to keep it current, and to reflect changes to the facility, the work and the hazards as they are analyzed in the documented safety analysis. (2) Annually submit to DOE either the updated documented safety analysis for approval or a letter stating that there has been no change in the documented safety analysis since the prior submission.” These requirements of 10 CFR 830 serve two purposes: (1) consolidate all positive USQs and JCOs prepared during the year into one safety basis document for DOE approval and (2) ensure that compensatory measures, and thus less reliable controls, implemented for temporary changes resulting from the JCOs do not become the permanent control of hazards for protection of the public and the workers.

CNS applies the JCO process to temporary changes as reflected in CD-3014 but also to allow deviations from approved safety basis documents. The latter application has resulted in JCOs extending over several years without being integrated into the annual update of the safety bases for multiple operations at Pantex, and consequently, heavy reliance on compensatory measures for long periods of time while the JCOs are in effect [18–20].

9. *Maintenance of the DSA*—CNS has struggled to complete and obtain NPO approval of the yearly updates required by 10 CFR § 830.202. Starting in 2015, NPO has not approved the annual updates CNS has submitted for the *Sitewide SAR*. In 2016, CNS was unable to meet the annual DSA update requirements for the *Sitewide* and *Transportation SARs* and the W76 and W78 HARS. As NPO rejected CNS's submittals, a backlog developed. This process culminated in three rejected submittals and five approvals total in 2017. Overall, this resulted in 11 of 16 SARs and HARS not being approved for annual updates in 2017. In particular, the *Sitewide SAR* has not been successfully updated and approved via the annual update process since 2014.

In lieu of completing the 2017 annual updates, CNS submitted, and NPO approved, a schedule to “rework” three previously submitted annual updates and catch up on the remainder with calendar year 2018 annual updates. If CNS successfully executes its plan to submit and obtain NPO approval of a full slate of 2018 annual updates, it will be back on course to meeting the DSA maintenance requirements.

*10. Safety Basis Assessments*—CNS has processes and procedures for performing management assessments and IVRs. The review team found sufficient evidence that management assessments of safety controls are being performed on a five-year schedule (i.e., 20 percent per year). While a few assessments have been missed, the review team’s analysis indicates that CNS is generally holding to that schedule.

However, CNS performs IVRs when there is a new TSR or a change to an existing TSR. DOE Guide 423.1-1B, *Implementation Guide for Use in Developing Technical Safety Requirements*, specifies that IVRs should be conducted every three years for controls susceptible to the degradation of human knowledge (e.g., procedural controls) [21]. Therefore, CNS is not meeting the three-year guidance for re-verification of specific administrative controls. Furthermore, the review team’s evaluation of the management assessments for SACs for the W76 and W78 indicated that these assessments rarely identify any strengths, weaknesses, findings, or observations. The Pantex DSAIP includes an effectiveness review for the management assessments, but CNS does not have a path forward to improve management assessments.

*11. Action on Known Deficiencies*—CNS currently is implementing a DSAIP to address several longstanding issues with the Pantex safety bases [22]. The DSAIP has existed since 2013 and is currently in its fifth revision. CNS personnel informed the staff review team that there has been steady progress on a number of items contained in the fifth revision of the DSAIP. Of the three items scheduled for completion in calendar year 2017, CNS completed two. Seventeen items are scheduled for completion in 2018.

In addition, the DSAIP lacks detail. The plan is only a list of titles of activities with a targeted year for completion. It does not provide any detail of the scope and objectives for each task, the criteria that should be met for satisfactory execution, or the resources required for completion. While CNS representatives informed the staff review team that they understand the items listed and the tasks involved, the DSAIP does not include detail sufficient to allow verification of the accomplishments. Consequently, the staff team cannot independently verify that the plan is comprehensive, achievable, and on-track to meet the schedule for 2018 and beyond.

Over several iterations of the DSAIP, CNS has committed to working down a set of “legacy” COAs that existed prior to the creation of NPO. Originally, there were 40 COAs in this category, and 5 currently remain open. The current iteration of the DSAIP includes a task in fiscal year 2018 to develop metrics for tracking progress in resolving the remaining five COAs. Actual closure dates for the five remaining COAs currently are not identified in the schedule.

## REFERENCES

1. Code of Federal Regulations, Title 10, Part 830, *Nuclear Safety Management*, January 10, 2001.
2. Department of Energy, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, Change Notice 3, DOE Standard 3009-94, March 2006.
3. Department of Energy, *Hazard Analysis Reports for Nuclear Explosive Operations*, DOE Standard 3016, September 2016.
4. Consolidated Nuclear Security, LLC, (U) *W76-0/1 SS-21 Assembly, Disassembly & Inspection, and Disassembly for Life Extension Program Operations Hazard Analysis Report*, Revision 71, RPT-HAR-255023, November 2017.
5. Consolidated Nuclear Security, LLC, (U) *W78 Step II Disassembly & Inspection and Repair Hazard Analysis Report*, Revision 63, AB-HAR-319393, September 2017.
6. Consolidated Nuclear Security, LLC, (U) *Sitewide Safety Analysis Report (SAR)*, Revision 288, AB-SAR-314353, January 2018.
7. Pantex Plant, (U) *Preparation Cart*, Revision 3, Engineering Analysis 000-2-0836-ANL-03, June 2007.
8. Pantex Plant, (U) *System Engineering Category 2 Electrical Equipment Evaluations*, EEE-06-0030, Issue No. 010, March 2014.
9. Pantex Plant, (U) *Category 2 Electrical Equipment Evaluation*, EEE-06-0037, Issue No. 010, October 2013.
10. Pantex Plant, (U) *Weapon Assembly/Disassembly Operations Requirements*, Issue P7-2003, AT, March 2013.
11. Pantex Plant, *Safety Checklist*, TABLE-0068, Issue No. 033.
12. Consolidated Nuclear Security, LLC, *Pantex Writer's Manual for Technical Procedures*, MNL-293084, Issue No. 12.
13. Department of Energy, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements*, Change Notice 1, DOE Guide 424.1-1 B, April 12, 2013.
14. Consolidated Nuclear Security, LLC, *Pantex Plant Unreviewed Safety Question Procedure*, CD-3014, Issue No. 18.

15. Don Nichols (NNSA Chief of Defense Nuclear Safety) to James Goss (NNSA Y-12 Site Office), memorandum dated February 2, 2010.
16. Consolidated Nuclear Security, LLC, *Problem Identification and Evaluation Processing Form*, PX-4633, Issue No. 14.
17. Consolidated Nuclear Security, LLC, *Commercial Grade Dedication Testing of Delta Arresters*, PIE-18750, USQD-17-3434-A, February 24, 2017.
18. Consolidated Nuclear Security, LLC, *Justification for Continued Operation for W80 ESD*, PX-JCO-14-04, Revision 5, February 27, 2017.
19. Consolidated Nuclear Security, LLC, *Justification for Continued Operation for B61 ESD*, PX-JCO-14-05, Revision 5, October 4, 2016.
20. Consolidated Nuclear Security, LLC, *Justification for Continued Operation for W88 Uncased HE Operations*, PX-JCO-17-09, Revision 2, January 11, 2018.
21. Department of Energy, *Implementation Guide for Use in Developing Technical Safety Requirements*, DOE Guide 423.1-1B, March 18, 2015.
22. Consolidated Nuclear Security, LLC, *The Documented Safety Analysis Improvement Plan*, Revision 5, SB-MIS-941949, September 21, 2017.



**AFFIRMATION OF BOARD VOTING RECORD**

**SUBJECT: Uncontrolled Hazards Scenarios and Preliminary Inquiry Report**

**Doc Control#2018-100-061**


The Board, with Board Member(s) Daniel J. Santos, Joyce L. Connery *approving*, Board Member(s) Bruce Hamilton, Jessie H. Roberson *disapproving*, Board Member(s) none *abstaining*, and Board Member(s) none *not participating*, has voted to disapprove the above document on September 12, 2018.

The votes were recorded as:

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIPATING*	COMMENT	DATE
Bruce Hamilton	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	09/10/18
Jessie H. Roberson	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	09/12/18
Daniel J. Santos	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	09/10/18
Joyce L. Connery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	09/11/18

\*Reason for Not Participating:

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Board Members.

  
\_\_\_\_\_  
Executive Secretary to the Board

Attachments:

1. Voting Summary
2. Board Member Vote Sheets

cc: Board Members  
OGC  
OGM Records Officer  
OTD

**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**  
**NOTATIONAL VOTE RESPONSE SHEET**

**FROM: Bruce Hamilton**

**SUBJECT: Uncontrolled Hazards Scenarios and Preliminary Inquiry Report**

**Doc Control#2018-100-061**

Approved \_\_\_\_\_ Disapproved  X  Abstain \_\_\_\_\_

Recusal – Not Participating \_\_\_\_\_

COMMENTS: Below  X  Attached \_\_\_\_\_ None \_\_\_\_\_

This correspondence would require the Secretary to provide a written response and a briefing regarding actions taken and progress to date related to certain Board-identified deficiencies at the Pantex Plant.

42 U.S.C. § 2286b(d) authorizes the Board to, "... establish reporting requirements for the Secretary of Energy ...." The Board should generally practice a narrow interpretation of its statutory authority to require reports. This authority should be used with discretion, such as when information has been difficult to obtain through informal staff-to-staff interaction or when periodic recurring reports on program status are warranted. 42 U.S.C. § 2286b(d) should not be used as a mechanism to convey either an explicit or an implied mandate for the Secretary to carry out an activity. In this case, that appears to be the message.

Likewise, 42 U.S.C. § 2286b(d) should not be used as a surrogate for a recommendation. In the event that the issues identified in the Staff Issue Report, either individually or in totality, challenged the "... adequate protection of the public health and safety..." the statutorily appropriate path would be to recommend action to the Secretary of Energy. In this case, there is no indication that this threshold has been reached.

I therefore disapprove.

  
Bruce Hamilton

10 SEPT 2018  
Date

**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**  
**NOTATIONAL VOTE RESPONSE SHEET**

**FROM:       Jessie Roberson**

**SUBJECT:    Uncontrolled Hazards Scenarios and Preliminary Inquiry Report**

**Doc Control#2018-100-061**

**Approved** \_\_\_\_\_                   **Disapproved**   X                     **Abstain** \_\_\_\_\_

**Recusal – Not Participating** \_\_\_\_\_

**COMMENTS:**       **Below**   X     **Attached** \_\_\_\_\_       **None** \_\_\_\_\_

The technical information and conclusions included in this communication reflect consistency and alignment with the standard the Board has relied on for issuing a Recommendation in accordance with the Board’s statutory mission:

‘The Board **shall** make such recommendations to the Secretary of Energy with respect to Department of Energy defense nuclear facilities, including operations of such facilities, standards, and research needs, as the Board determines are necessary to ensure adequate protection of public health and safety.’

The conclusions in the proposed correspondence:

- The safety basis at Pantex is deficient in meeting Title 10, Code of Federal Regulations, Part 830, *Nuclear Safety Management*. There are high consequence hazards that (1) are not adequately controlled; (2) may have controls, but lack documentation linking the controls to the hazards; and (3) have controls that are not sufficiently robust or that lack sufficient pedigree to reliably prevent or mitigate the event.
- Multiple components of the process for maintaining and verifying implementation of the safety basis at Pantex are deficient, including (1) completion of annual updates as required by 10 CFR 830, (2) processes for handling Unreviewed Safety Questions (USQ) and Justifications for Continued Operations (JCO), and (3) processes for performing Implementation Verification Reviews of credited safety controls.

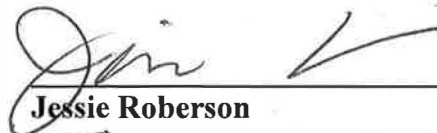
- To date, the NNSA Production Office and the Pantex contractor have been unable to resolve the known safety basis deficiencies.

DOE's own regulation defines the purpose of the Documented Safety Analysis as follows: 'A documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety.'

The relationship between the technical deficiencies described in the Board's communication and the assurance of public health and safety are clear and a DNFSB risk assessment would inform the Board regarding the impact of the deficiencies.

As a result of concerns raised earlier this year by the Board's Resident Inspectors assigned to the Pantex Plant, the Board approved the conduct of a safety investigation of the implementation of 10 CFR Part 830 at the Pantex Plant in early April of 2018. That investigation concluded in early July, 2018. The Board considered forwarding the unedited report of the safety investigation (Board Members did disagree over the desired document form for communicating with DOE on the topic) to the Department to supplement Board Members' timely evaluation process, but the vote failed.

The Board has now evaluated, modified, and edited the safety investigation results and combined those with other staff work products and the conclusions presented are those of the Board. I conclude the deficiencies outlined meet the statutory recommendation test.

  
\_\_\_\_\_  
**Jessie Roberson**  
Sept 12, 2018  
\_\_\_\_\_  
Date

**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**  
**NOTATIONAL VOTE RESPONSE SHEET**

**FROM: Daniel J. Santos**

**SUBJECT: Uncontrolled Hazards Scenarios and Preliminary Inquiry Report**

**Doc Control#2018-100-061**

**Approved   X   Disapproved        Abstain**

**Recusal – Not Participating**

**COMMENTS: Below   X   Attached        None**

**The Board approved the conduct of a safety investigation of the implementation of 10 CFR Part 830 (Nuclear Safety Management) at the Pantex plant. I approve this action since it is important to communicate to DOE in a timely manner the results presented to the Board by the safety investigation team.**

**In parallel, the staff should generate a draft Recommendation on this subject in order for the Board to complete its formal deliberations regarding any aspects necessary to ensure adequate protection of public health and safety.**



**Daniel J. Santos**

          9/10/18            
**Date**

**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**  
**NOTATIONAL VOTE RESPONSE SHEET**

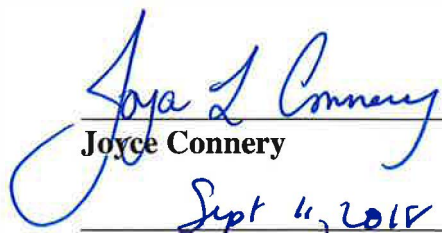
**FROM:** Joyce Connery

**SUBJECT:** Uncontrolled Hazards Scenarios and Preliminary Inquiry Report

**Doc Control#2018-100-061**

**Approved**  **Disapproved**  **Abstain**   
**Recusal - Not Participating**

**COMMENTS:** **Below**  **Attached**  **None**

  
\_\_\_\_\_  
**Joyce Connery**  
\_\_\_\_\_  
**Date** *Sept 11, 2018*