Department of Energy
Washington, DC 20585

December 20, 2019

The Honorable Bruce Hamilton
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, DC 20004

Dear Chairman Hamilton:

I am responding on behalf of Secretary Brouillette to your August 27, 2019, letter to the Secretary of Energy regarding the design of the safety-significant confinement ventilation system (SSCVS) at the Waste Isolation Pilot Plant (WIPP), which included a report from your staff detailing concerns with the SSCVS and its ability to prevent an unfiltered radiological release in certain scenarios. These scenarios included the continuous air monitor (CAM) system and its timely actuation to reconfigure the SSCVS in the event of an underground radiological release, as well as an interlock between the SSCVS exhaust fans and future supply fans. The staff report identified three safety items and two observations.

The first safety item of concern noted that a 60-second closure time for the Salt Reduction Building (SRB) isolation dampers may not be adequate time to isolate the SRB and prevent an unfiltered radiological release to the atmosphere. One of your staff's calculations found that contamination might reach the isolation dampers only 41 seconds after passing the bottom of the exhaust shaft.

The 60 seconds mentioned in the Preliminary Documented Safety Analysis (PDSA) for the SSCVS is considered to be a nominal closure time. The placement of the CAMs in the underground has not been finalized, and the credited closure time that will eventually be included in the WIPP Documented Safety Analysis (DSA) will ensure that the dampers close in time to prevent an unfiltered release of radioactive materials to the atmosphere. If necessary, the dampers are capable of closing in 30 seconds or less. Furthermore, several events that could push contamination from the waste shaft station toward the exhaust shaft, which are represented by the three cases discussed in your staff's report, do not credit the SSCVS to protect collocated workers or the public.

The second safety item concerns an interlock between the SSCVS exhaust fans and the future supply fans that will be installed as part of the new utility shaft project. The third safety item addresses the locations and set points for the underground CAMs. In the early stages of the SSCVS project, the Carlsbad Field Office (CBFO) made a conscious decision to limit the capital project scope to above-ground facilities and equipment. As a result, these topics were not addressed in the PDSA. However, CBFO now recognizes the need for an interlock between SSCVS exhaust fans and future supply fans. This issue was initially identified in February 2019, during a Department of Energy (DOE) project

peer review team. The SSCVS project has committed to installing such an interlock before the supply fans begin operation. The safety classification of the interlock awaits further analysis of the reconfigured mine airflow. Similar to the interlock, the CAMs were deliberately excluded from the PDSA. The responsibility for CAM design, procurement, and placement was assigned to existing facility operations. The CAM locations and set points, and the bases for them, will be included in the WIPP safety basis prior to SSCVS startup.

Your staff's report included two observations: (1) the CAM performance criteria are not specified; and (2) the redundancy objectives are unclear. The safety-significant underground CAM system will meet a Safety Integrity Level (SIL)-2 or equivalent reliability, with a minimum of three instruments in service. However, design of the full safety-significant architecture for this control system is not yet complete. The system should be installed and commissioned well before SSCVS becomes operational. As for the redundancy objectives, the SIL-2 calculations indicate the system will use one-out-of-three voter logic to maximize the probability of detection. The performance criteria and redundancy objectives will be fully described in the WIPP DSA before the CAM system enters service.

The enclosure provides more detail to each safety item and observation in your staff's report. DOE appreciates your staff's engagement with the SSCVS project and WIPP operations. Your independent, critical reviews will help this project succeed while protecting the public health and safety. DOE staff are working with your Technical Director to schedule the Board's requested briefing on this topic in the near future.

If you have any questions please, contact me or Mr. Dae Y. Chung, Deputy Assistant Secretary for Safety, Security, and Quality Assurance, at (202) 586-9636.

Sincerely,

Todd A. Shrader
Principal Deputy Assistant Secretary for
Environmental Management

Enclosure

cc: Joe Olencz, AU-1.1
Steve Petras, AU-1.1
Gregory Sosson, CBFO (Acting)
James Garza, CBFO
Roger Quintero, RL
William White, EM-1
Thomas Mooney, EM-2.1 COS
Jeff Griffin, EM-3
John Mocknick, EM-3
Dae Chung, EM-3.1
Brenda Hawks, EM-3.1

The staff review team identified the following safety items.

***Safety Instrumented Systems' Performance Criteria Are not Adequate*—The SSCVS project established performance criteria for the ventilation dampers to ensure that they reach their fail-safe positions (salt reduction building bypassed and HEPA filters enabled) within 60 seconds of receiving an actuation signal. WIPP selected this value to prevent any unfiltered release and to prevent radiological contamination and release through the salt reduction building, while avoiding potential negative impacts to SSCVS components that might result from rapid repositioning of dampers and sudden shifts in air flow rates and paths. The Board's independent analysis [Appendix A] has identified that even for a release that is immediately detected, a 60 second damper closure time may not be adequate to prevent radiological contamination releases for all potential event initiation locations.**

Response:
An analysis was performed in August 2017 (DN- 486300.030-09, *Panel 9B Transient Time Study*) that modeled air travel from Panel 9B to the exhaust shaft collar. The analysis assumed a new intake shaft would be west of the air intake shaft and assumed that entries south of S-1300 would be permanently sealed and waste storage was occurring in Room 1 Panel 9B. Two scenarios analyzed transit times with and without a new intake shaft. For both cases, transit times for air exiting Panel 9B Room 1 and traveling to the exhaust shaft collar were greater than 5 minutes. Therefore, the specification of the damper closure time of 60 seconds was judged to be adequate.

The preliminary documented safety analysis (PDSA) considered the 60 seconds to be a nominal closure time (PDSA Section 4.4.1.4) due to the uncertainty in the location of the intake shaft and final configuration of waste disposal areas in the underground once the Safety Significant Confinement Ventilation System (SSCVS) had become operational. The PDSA described a nominal closure time with the understanding that configuration of the underground and continuous air monitor (CAM) placement needed to be finalized. As stated in the PDSA, the credited closure time must be quick enough (relative to the time it takes for the release to reach the surface) to prevent significant radiological consequences to the collocated worker. Analysis must also show that the closure time is not too rapid so as to result in a transient condition that can damage the SSCVS or underground (UG) bulkheads, regulators, etc. The credited closure time will take into account the placement of the CAMs to determine the optimum damper response for the SSCVS.

The actuators that close the isolation dampers are capable of isolating the Salt Reduction Building (SRB) in 30 seconds or less, if necessary. Thus, during explosion/deflagration or high energy events at the waste shaft station (discussed in Appendix A of the Board's report), the SRB damper closure system is capable of isolating the SRB from a radiological release event.

The Board staff evaluated three cases in Appendix A of the June 26, 2019, staff report. The radiological releases of the three scenarios take place in the underground waste shaft station located between the waste shaft and exhaust shaft. This area was selected due to the proximity of the waste shaft station to the bottom of the exhaust shaft. The three cases evaluate fire, deflagration/over-pressurization, impact, and spontaneous combustion events. They encompass eight accidents analyzed in the PDSA: CH/RH-UG-02-001a, CH/RH-UG-02-002a2, CH/RH-UG-02-002a3, CH-UG-01-001a2, CH-UG-06-001a, CH/RH-UG-10-003a, CH/RH-UG-01-005a1, and CH/RH-UG-10-005a. The main differences between the three cases examined by the Board staff are the magnitude of the event and the location of the CAMs.

The events of greatest concern, requiring the quickest damper closure times, are explosion or high energy events of sufficient magnitude to push radiological contamination from the waste shaft station toward the exhaust shaft. The representative events are discussed below:

> Event CH/RH-UG-01-005a1 (PDSA Page 3-46) involves a vehicle containing liquid fuel (e.g., forklift, forklift with 300-gallon diesel tank) that enters an open Waste Shaft (i.e., conveyance not present) and drops onto loaded waste conveyance resulting in large pool fire in the Waste Shaft with a release of radiological material. The mitigated analysis credits above ground vehicle/equipment operation prohibition and waste conveyance controls which reduce the event frequency to beyond extremely unlikely (BEU). This event does not credit the SSCVS or placement of the CAMs for mitigating the risk.
>
> Event CH/RH-UG-10-005a (PDSA Page 3-131) occurs when a vehicle/equipment carrying waste drives into Waste Shaft Collar and drops onto loaded Waste Shaft Conveyance resulting in release of radiological material. The mitigated analysis credits waste conveyance controls which reduces the event frequency to BEU. This event does not credit the SSCVS or placement of the CAMs for mitigating the risk.
>
> Event CH/RH-UG-06-001a (PDSA Page 3-111) is the representative event for a contact-handled (CH) Waste Container deflagration in the UG prior to reaching the disposal room (event could occur at the Waste Shaft Station or in the Transport Path). No credited controls are required for the co-located worker or for the maximally exposed offsite individual (MOI) because the unmitigated consequences are Low for these receptors. Thus, this event does not credit the SSCVS or placement of the CAMs for mitigating the risk. Facility worker mitigated consequences are Low by crediting the Suspect Container control (LCO 3.7.1).
>
> Event CH-UG-06-001a (PDSA Page 3-113) is the representative event for a CH Waste Container deflagration in an open waste disposal room, which is located a significant distance away from the exhaust shaft and would not challenge the credited 60 second SRB damper closure time (*Ref Panel 9B Transient Time*

Study). Radiological dose consequences are mitigated by the Suspect Container Response administrative control (LCO 3.7.1) and by the SSCVS high-efficiency particulate air (HEPA) filtration and air flow in the underground.

Event CH/RH-UG-10-003a (PDSA Page 3-127) is the representative event for a loss of confinement due to a pressurized cylinder impacting a CH or remote-handled (RH) Waste container. The explosion occurs outside of a waste container, occurring anywhere in the UG. The Waste Isolation Pilot Plant (WIPP) Waste Acceptance Criteria (WAC) initial condition ensures waste confinement is within a metal container of sound integrity, which would limit the release. The unmitigated radiological consequences are Low for the facility worker and Low for the MOI. Thus, no credited controls are required for these receptors. The unmitigated consequences are Moderate for the collocated worker. The collocated worker consequences are mitigated by the SSCVS HEPA filtration. If this scenario occurred, damper actuators would have the capability to close the SRB dampers in time to prevent contamination of the SRB.

Events CH/RH-UG-02-002a2 (PDSA Page 3-85) and CH/RH-UG-02-002a3 (PDSA Page 3-87) are ordinary combustible fires in the Transport Path and Waste Shaft Station, respectively, with Waste containers present (solid combustible material fire) resulting in release of radiological material. Ordinary combustible fires are postulated to originate near an adjacent waste container. The events do credit SSCVS HEPA filtration and air flow in the underground for mitigation, as well as notification by attending workers. Ordinary combustible fires are slow to develop, and the waste would be protected in a WAC-compliant metal container (initial condition). These fires are not high energy release events of concern (as in an explosion) that would push radiological contamination from the waste shaft station toward the exhaust shaft. Therefore, these events would not challenge CAM placement, and damper actuators would have the capability to close the SRB dampers in time to prevent contamination of the SRB.

Event CH/RH-UG-01-002a2 (PDSA Page 3-40; Event CH-UG-01-001a2, WIPP-021 Rev. 8b, Page A-35) is the representative event for a pool fire in the Waste Transport Path resulting from the ignition of a liquid-fuel pool (e.g., vehicle fuel system leak) while transporting CH Waste on a vehicle (e.g., forklift). The WIPP WAC initial condition ensures confinement within a metal container of sound integrity. A leak resulting in pool formation and ignition produces a pool fire that would not instantaneously release radiological material. While the pool fire would engulf the container rapidly, the waste would be initially protected in a WAC-compliant metal container. Thus, an instantaneous explosive release of material would not occur to push radiological contamination from the Transport Path toward the exhaust shaft. The release would initially occur through seal failure, followed by lid ejection and unconfined burning of combustibles outside the container.

The mitigated event credits automatic fire suppression on UG vehicles/equipment; pre-op checks on vehicles; controls in the transport path such as spotters and attendants with liquid-fueled vehicles and/or equipment to reduce the likelihood of large combustible liquid spills, credited notification, and facility pallets. The SSCVS HEPA filtration is not credited in this event, it would not challenge CAM placement, and damper actuators would have the capability to close the SRB dampers in time to prevent contamination of the SRB.

Event CH/RH-UG-02-001a (PDSA Page 3-81) is an event involving an ordinary combustible material fire in a noncompliant Waste container due to spontaneous combustion (internal Waste container fire) resulting in release of radiological material. It takes place in a Waste Disposal Room not at the Waste Shaft Station or Transport Path. The event does credit SSCVS HEPA filtration and air flow in the underground for mitigation, as well as notification by attending workers. This event would not challenge CAM placement, and damper actuators would have the capability to close the SRB dampers in time to prevent contamination of the SRB.

In conclusion, the explosion or high energy events at the Waste Shaft Station generally do not credit CAM placement or HEPA filtration because these events are mitigated to BEU. For events that do credit HEPA filtration and SRB isolation, the damper closure design will be capable of isolating the SRB in 30 seconds or less, preventing the contamination from a radiological release to the atmosphere. Once the Utility Shaft is operational, only 65% of the 540,000 cfm or approximately 350,000 cfm will flow up the exhaust shaft. In this configuration the time to reach the surface would increase from 41 seconds to over a minute.

***Supply Fans Are not Interlocked with Exhaust Fans*—The final SSCVS design did not establish any requirements for an interlock with supply fans as recommended by Table A-1 of DOE Guide 420.1-1A, *Nonreactor Nuclear Safety Design Guide for use with DOE O 420.1C, Facility Safety.* The non-safety utility shaft project proposes fans to supply a total of 500,000 cubic feet per minute (cfm). SSCVS has the capacity to exhaust 540,000cfm. If utility shaft fans are not automatically shut down when the SSCVS fans stop, an imbalance in the underground air flow has the potential to up-cast unfiltered air from the contaminated circuit. The DOE-EM Project Peer Review Exit Briefing also identified this item as a recommendation (R-TTQA-10), stating that "WIPP needs to ensure that provisions for such an interlock, which will be safety significant, are established in the programmable logic controller."**

Response:
The proposed utility shaft surface supply fans will force air to the construction and disposal circuits on the underground north side.

Pushing air down the new utility shaft will convert the air intake shaft (AIS) to an exhaust shaft, ensuring return air from the construction circuit will be up-casted and exhausted through the AIS. As noted, if the SSCVS exhaust fans stop and the supply fans do not,

contaminated air could be exhausted through the waste shaft, salt shaft, or AIS. This type of accident was analyzed for the current mine configuration before the Supplemental Ventilation System supply fan was placed into service. The scenario is evaluated as event number NA-OA-10-001a in the Hazards Analysis for the WIPP Transuranic Waste Handling Safety Basis, WIPP-021. The analyzed event used a bounding source term and assumed the release occurred at the surface, discounting any deposition within the mine. Based on this preliminary assessment, such an event would result in low unmitigated consequences to all receptors, so the interlock would not need to be a safety-significant control.

To date, no hazard analysis of the future airflow configuration, to include potential mine expansion areas, has been completed. Once the utility shaft is completed and the new supply fans enter into service, mine airflow will be significantly re-configured. At that time, a final function classification determination of the supply fan interlock can be made. Before designing and procuring the interlock, this analysis will be completed, so the interlock can receive a definitive safety designation.

***The Radiological Protection Program Establishes CAM Locations and Setpoints*— WIPP currently uses CAMs as part of an occupational radiological protection program under Title 10, Code of Federal Regulations, Part 835 (10 CFR 835), *Occupational Radiation Protection Program.* This regulation requires monitoring of the concentrations of radioactive material in the air but does not discuss the application of instrumentation setpoints for initiating an automatic action (e.g., alarm) based on instrumentation performance criteria. The use of CAMs as a hazard control require they meet requirements under 10 CFR 830, *Nuclear Safety Management.* The CAMs WIPP uses to initiate SSCVS are safety significant components. The SSCVS project has identified DOE Standard 1195, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*, as the method to assure sufficient reliability of the safety significant instrumentation. DOE Standard 1195 requires that setpoint development follow the requirements of American National Standards Institute (ANSI)/International Society for Automation (ISA) standard ANSI/ISA 67.04.01, *Setpoints for Nuclear Safety-Related Instrumentation.* This setpoint methodology assures that SSCVS complies with analytical limits and, in conjunction with CAM placement, ensures that SSCVS properly performs its safety function for all hazards it is designed to prevent or mitigate. A radiological protection program established under 10 CFR 835 does not establish equivalent setpoints to ensure 10 CFR 830 requirements are met. This safety item results from the failure to properly consider the CAMs during the SSCVS design.**

Response:
A set point for the CAMs was not included in the PDSA. The request for proposals to design and build the SSCVS CAM interlock system (redundant iCAM-HDs, logic solver, damper actuators, safety relays and annunciator panel) is scheduled for release in first quarter of fiscal year 2020. The system should be installed in calendar year 2021, well before scheduled SSCVS startup in 2022.

Prior to SSCVS startup, the project will revise the WIPP DSA to provide the CAM set points and the bases for the set points to ensure the SSCVS complies with analytical limits and properly performs its safety function for all hazards it is designed to prevent or mitigate.

The staff review team identified the following observations.

***WIPP Does Not Specify CAM Performance Criteria*—WIPP must consider the long term effect of the underground salt environment on CAM performance, as well as the effects of a smoke environment that may co-exist with a radiological release event. Any impacts on CAM performance that result in a delay in the detection and signaling that a radiological release has occurred could affect the overall SSCVS performance and may prevent SSCVS from meeting its safety function. Many factors affect the total time from event initiation to completion of SSCVS response, including the location of the CAMs, the magnitude of the release event, and all performance factors that affect the ability of the CAM to detect the release.**

Response:
The CAM design and performance must account for failure modes to include degradation due to the environmental factors. As described in the PDSA, to meet a Safety Integrity Level (SIL)-2 or equivalent reliability, the UG radiological detection will have a minimum of three radiation detection instruments in service and set to alarm at a Derived Air Concentration-Hour (DAC-hr) threshold determined by the Radiological Protection Program. The current WIPP CAM set points is 8 DAC-hr. The radiation detection instrumentation will be connected to a Programmable Logic Controller that relies upon redundant control/voter logic to initiate an alarm signal to the Central Monitoring Room upon indication of an UG release. SIL analysis report REP-18137-001, Revision 0, dated July 17, 2018, shows that the proposed design and redundancy described in the PDSA is sufficient to achieve a SIL-2 reliability for commercially available CAMs.

The iCAM-HDs have been procured and were delivered to the WIPP Site in November 2019. A Failure Mode and Effects Analysis and a Commercial Grade Item Dedication (CGID), with 3 Critical Characteristics (CGID Plan # 19-008, Revision 0) were prepared for the receipt of the iCAM-HDs. Pending receipt inspection of component verification, functional verification of detector range (low), and operational verification of the detector sensitivity, the procured iCAM-HDs will meet the safety-significant criteria prescribed in the PDSA.

The design of the full safety-significant architecture for the control system necessary to meet the SIL-2 safety basis criteria (i.e., redundant iCAM-HDs, logic solver, damper actuators, safety relays and annunciator panel) is not yet complete. As noted above, the request for proposal should be released early in fiscal year 2020, and the system installed and commissioned in 2021.

***Redundancy Objectives Are Unclear*—The SER indicated that the radiation detection "instrument system will be connected to a PLC [programmable logic controller] with redundant voter logic to initiate alarm signals to the CMS [central monitoring system]." It is not clear if this redundant voter logic will be designed to maximize the probability of detection (e.g., one out of two logic), to minimize the probability of a false or spurious actuation (e.g., two out of two logic), or to use some type of an optimization scheme (e.g., two out of three logic). The selected design approach will affect actuation time as well as the calculated safety integrity level specified by DOE Standard 1195.**

Response:
According to the SIL-2 calculations, the programmable logic controller (PLC) voter logic (i.e. one-out-of-three [1oo3] redundant control) is designed to maximize the probability of detection. The DSA will be revised to further describe the 1oo3 PLC logic which allows, for example, one CAM to be taken off line for maintenance or repair without rendering the notification system inoperable.