Assessing the Vulnerability of Yucca Mountain Shipments: A Threat Matrix for Human-Initiated Events - 8152

J.D. Ballard, PhD (ballard@csun.edu)
Department of Sociology, California State University, Northridge
Northridge, CA 91330

R.J. Halstead (bearhalstead@aol.com)
State of Nevada Agency for Nuclear Projects
Carson City, NV 80906

F. Dilger, PhD (fcd5@cox.net)
Black Mountain Research
Henderson, NV 81012

H. Collins, PE, CHP (hankcollins2@yahoo.com)
Collins and Associates
San Ramon, CA 94583

M. Resnikoff, PhD (radwaste@rwma.com)
Radioactive Waste Management Associates
New York, New York 10001

ABSTRACT

In preparation for review of two Department of Energy (DOE) National Environmental Policy Act (NEPA) documents, the Draft Supplemental Environmental Impact Statement for Yucca Mountain (DSEIS) and the Draft Rail Alignment Environmental Impact Statement (RA DEIS), the State of Nevada sponsored a study of vulnerability methodologies which could be applied to Yucca Mountain shipments. This study examined various human-initiated events, including sabotage, terrorism, induced accidents, and protest demonstrations. This paper reports the findings of that study, and recommends a comprehensive threat assessment methodology for use in evaluating sabotage and terrorism events, pursuant to a resolution adopted by the Western Governors Association (WGA) in 2007. The WGA 07-2 Resolution called on the Nuclear Regulatory Commission (NRC) and DOE to "fully address the consequences of attacks against all components of the nuclear waste handling and transport system."

INTRODUCTION

This paper recommends a comprehensive threat assessment process for the proposed Yucca Mountain transportation system.. The recommended process could be used by DOE to assess repository transportation impacts as part of its NEPA requirements, and in responding to the WGA resolution on terrorism and sabotage. This paper identifies ways to improve current risk assessment techniques to meet the challenges of human initiated events, including terrorism, sabotage, induced or deliberate accidents, and violent protests. The recommended threat assessment process is presented as a series of industry standard methods and concludes with exemplar scenarios.The paper uses only open source data.

The DOE is continually revising their transportation concept for Yucca Mountain and could readily alter their current program to adopt the recommended process. Considering the currently delayed schedule for the repository and the proposed rail line, it seems unlikely that shipments to Yucca Mountain could begin earlier than 2017-2020. There is ample time for DOE to systematically address human-initiated events in the Draft Supplemental EIS, the Draft Rail Alignment EIS, in its Transportation Concept of Operations, in its National Transportation Plan, in its national routing studies, and in its implementation of Section 180© technical and financial assistance to affected States and Indian Tribes.

SHIPMENT VULNERABILITY DEBATE

For three decades, risk analysts have debated the vulnerability of spent nuclear fuel shipments to acts of terrorism and sabotage. The details of the debate are documented in studies prepared for the State of Nevada in 1998 and 2005. [1, 2] The attack scenarios evaluated in NRC and DOE analyses have changed little over the decades. The analyses assume that a single spent fuel shipping cask is attacked at one location, by one group of attackers, using one weapon. The analyses assume that the attack breaches the cask and releases some fraction of the contents. The analyses differ in estimates of the amount of radioactive material released, the details of the release and dispersal, the area contaminated, the population exposed, the resulting human casualties, and the economic impacts.

The first NRC regulations requiring physical protection of spent fuel shipments were issued in response to a 1977 draft assessment by Sandia National Laboratories (SNL). That assessment, and a follow-up study by SNL in 1980, indicated that sabotage of a shipment in an urban area could cause hundreds to thousands of casualties, and billions of dollars in economic losses and cleanup costs. The NRC issued interim physical protection requirements for spent fuel shipments in 1979, and adopted the current system of regulations (10CFR73.37) by rulemaking in 1980.

Subsequent studies sponsored by NRC and DOE sharply reduced the estimated causalities and economic losses. The debate over the consequences of a successful terrorist attack resumed in 1984, when the NRC, acting on the new studies, issued a proposed rule eliminating physical protection requirements for most spent fuel shipments. The NRC had concluded that the expected consequences of a successful attack in "a heavily populated area such as New York City would be no early fatalities and less than one (0.4) latent cancer fatality." This NRC proposed rule was opposed by state governments, environmental groups, and some nuclear industry sources. Three years later, the NRC terminated the proposed rule, without explanation. Throughout the 1990s, however, the NRC continued to downplay attack consequences. At the same time, public discussion of vulnerability and consequences temporarily subsided.

The controversy re-emerged nationally in 1995 as the DOE began the NEPA scoping process for the proposed Yucca Mountain geologic repository. State governments and other parties urged DOE to address terrorism and sabotage in the Yucca Mountain environmental impact statement (EIS). The State of Nevada filed detailed scoping comments on the impacts of terrorism against repository shipments during 1995, and published several supporting studies between 1996 and 1998. Based on these studies, Nevada's Attorney General filed a petition for rulemaking with the NRC in June 1999. The Nevada petition documented the vulnerability of shipping casks, and argued that shipments to a national repository would create greater opportunities for terrorist attacks and sabotage**.** The petition, which requested strengthening of the current regulations and a comprehensive reexamination of radiological sabotage, was endorsed by the Western Governor's Association. More than eight years later, the NRC has still not officially responded to the Nevada petition.

DOE acknowledged that shipping casks are vulnerable to terrorist attack in the 1999 Draft EIS for Yucca Mountain. [3] In support of the Draft EIS, DOE sponsored a 1999 SNL study of cask sabotage, which demonstrated that high-energy devices (HEDs) were "capable of penetrating a cask's shield wall, leading to the dispersal of contaminants to the environment." The SNL study also concluded that a successful attack on a truck cask could release more radioactive materials than an attack on a rail cask, even though rail casks would contain, on average, up to six times more SNF than truck casks. [4]

In the 2002 Final EIS for Yucca Mountain, DOE updated its sabotage analysis, assuming more highly radioactive SNF, a larger respirable release, and a higher future average population density for U.S. cities. [5] DOE estimated that a successful attack on a truck cask in an urbanized area under average weather conditions would result in a population dose of 96,000 person-rem and 48 latent cancer fatalities. For a successful attack on a large rail cask, DOE estimated a population dose of 17,000 person-rem and 9 latent cancer fatalities. In neither case did DOE evaluate any environmental impacts other than health effects, and ignored the economic impacts of a successful act of sabotage. While the DOE did not specifically estimate cleanup costs after such an attack, the FEIS states that clean-up costs following a worst-case transportation accident could reach $10 billion.

Analyses prepared for the state of Nevada by Radioactive Waste Management Associates (RWMA) calculated that sabotage impacts could be considerably greater. [6] RWMA replicated the DOE Final EIS sabotage consequence analyses, using the RISKIND model for health effects and the RADTRAN model for economic impacts, the SNL study average and maximum inventory release fractions, a range of credible values for the gap inventory of Cs-137, and a range of population densities and weather conditions. RWMA concluded that an attack on a truck cask using the same common military demolition device assumed in the DOE analysis could cause 300 to 1,820 latent cancer fatalities, assuming 90% penetration of the cask by a single blast. For the same device used against a large rail cask, RWMA estimated 46 to 253 latent cancer fatalities, again assuming 90% penetration. The major radiological health impacts of an attack would be caused by the downwind dispersion of respirable material (mainly particles with a diameter less than 10 microns) that could be ejected from the damaged cask. Depending upon the meteorological conditions present at the time of an attack, the respirable aerosol of radioactive materials could affect an area of 10 square kilometers (3.9 square miles) or more. RWMA estimated cleanup costs ranging upward from $668 million for the rail incident, and $6.1 billion for the truck incident, to more than $10 billion. Full perforation of the truck cask, likely to occur in an attack involving a state-of-the art anti-tank weapon, could cause as many as 3,000 to 18,000 latent cancer fatalities, and cleanup and recovery costs could far exceed $10 billion.

In October 2007, DOE published the Draft Supplemental Environmental Impact Statement for Yucca Mountain (DSEIS) [8] and the Draft Rail Alignment Environmental Impact Statement (RA DEIS) [9]. Both the DSEIS and the RA DEIS address the impacts of sabotage against repository shipments. In both volumes DOE states that it has “analyzed plausible threat scenarios, required enhanced security measures to protect against these threats, and developed emergency planning requirements that would mitigate potential consequences for certain scenarios. DOE would continue to modify its approach to ensuring safe and secure shipments of spent nuclear fuel and high-level radioactive waste, as appropriate, between now and the time of shipments. For the reasons stated above, DOE believes that under general credible threat conditions the probability of a sabotage event that would result in a major radiological release would be low.” [Ref. 8, p. 6-22; Ref. 9, p. 4-314]

Acknowledging "the uncertainty inherent in the assessment of the likelihood of a sabotage event," the DSEIS and RA DEIS evaluated events in which "a modern weapon (high energy density device)" is used to "penetrate a spent nuclear fuel cask." DOE evaluated the consequences of events occurring in representative urban, suburban, and rural areas. Based on new research by Luna [10] and on European studies, the DSEIS assumed that the single weapon attack studied would result in a smaller release of respirable material than DOE assumed in the 2002 FEIS. For a sabotage event against a truck cask in an urban area, the DSEIS reports consequences about half what DOE estimated in the 2002 FEIS - a population dose of 47,000 person-rem, and 28 latent cancer fatalities. For an attack on a large rail cask in an urban area, the DSEIS reports consequences double what DOE estimated in the 2002 FEIS - a population dose of 32,000 person-rem, and 19 latent cancer fatalities. As in the earlier DOE analyses, the DSEIS does not provide specific information on the land area contaminated, economic losses due to disruption of normal activities, and the cost of cleanup. The DSEIS does acknowledge the aforementioned State of Nevada analyses under the heading "Transportation Sabotage: An Opposing Viewpoint."

As of February 2008, the State of Nevada is preparing its own detailed reassessment of transportation sabotage impacts, scheduled for completion in May 2008. Nevada submitted comments on the DSEIS sabotage consequence analyses on January 10, 2008.
In those comments, Nevada emphasized that the DSEIS continues to ignore the consequences of a terrorist attack using one or more weapons that completely perforate the shipping cask, or a combination of weapons specifically designed to breach, damage, and disperse the cask contents. Such an attack could result in impacts more severe than those evaluated by DOE. The new references cited by DOE do not address such impacts. In fact, the Venturi effect created by full perforation of a shipping cask would likely negate the reduction in impacts claimed in the Luna study. In its key conclusion, DOE asserts that the factors identified by the State of Nevada "could affect the chances of success but not the outcome of the sabotage event." [Ref 8, p. 6-21] DOE presents no evidence in the DSEIS, the RA DEIS, or any of the cited references to support that assertion.

Moreover, the DSEIS ignores evidence, including terrorism studies funded by DOE, that DOE nuclear activities may be particularly attractive symbolic targets for sabotage or terrorist attacks. The DSEIS ignores past instances in which human errors in cask fabrication and cask loading actually occurred during NRC-licensed shipments, and created conditions that could have compromised cask performance in the event of a sabotage event. The DSEIS ignores Nevada's argument that unique local conditions such as proximity of the existing mainline railroads to downtown Las Vegas and Reno-Sparks must be factored into consequence assessments, resulting in multi-billion dollar cleanup costs and business disruption impacts.

In summary, all of the consequence assessments so far conducted by NRC, DOE and the State of Nevada assumed single-phase attack scenarios. None of these consequence assessments have evaluated the effects of an attack involving the simple impact-exacerbating tactics identified by the U.S. Army peer review report more than two decades ago: combined use of a breaching device and a dispersal device, or use of multiple breaching devices. None of these consequence assessments have incorporated insights obtained from the 1998 testing sponsored by International Fuel Containers, Incorporated, at the U.S. Army Aberdeen Test Center. Most significantly, none of these consequence assessments have evaluated any of the impact-exacerbating tactics studied by counter-terrorism experts in the post-September 11 environment. Credible hijack and control scenarios, specialized truck bomb scenarios, and/or concealed weapons (like improvised roadside devices) scenarios, coupled with insider assistance, diversionary attacks, and/or suicide tactics, could potentially result in radiological consequences far greater than those previously estimated by NRC, DOE or the State of Nevada. [7]

WESTERN GOVERNORS ASSOCIATION RESOLUTION

The primary motivation for this analysis, prior to publication of the DSEIS, was the Western Governors' Association (WGA) resolution regarding Yucca Mountain transportation. The WGA represents nineteen Western states and three territories. The association allows state political leaders to address critical policy issues in a wide variety of areas. The WGA organization thus helps state leaders develop strategies to address complex issues facing western states. [11] WGA has been actively involved in nuclear waste transportation planning for two decades. In 2007, WGA renewed and revised a policy resolution (07-2) on the risks of terrorism and sabotage against repository shipments. [12] The original resolution had been adopted in 1998.

WGA Resolution 07-2 notes that in the aftermath of the September 11, 2001 attacks, the altered threat environment calls for new, more comprehensive terrorism assessment tools. The resolution calls upon the U.S. Nuclear Regulatory Commission (NRC) to "fully address the consequences of attacks against all components of the nuclear waste handling and transport system, to include: attacks against transportation infrastructure, the theft of a shipment, use of high-energy explosives against a shipment cask, and direct attacks against a shipment cask using antitank missiles or other armament that could cause a loss of containment." WGA further requests that NRC "strengthen its efforts to share information with state and local governments regarding spent fuel shipment vulnerabilities and consequences, " recognizing that "sharing of information must be conducted within the framework of preventing the release of sensitive or classified information to individuals without a need to know."

The WGA resolution notes that DOE has acknowledged the vulnerability of shipments in the 2002 Final EIS for Yucca Mountain. The resolution states: "DOE should continue to address acts of sabotage and terrorism in its NEPA documents, and should incorporate terrorism/sabotage risk management and countermeasures in all DOE transportation plans, protocols, and practices relating to operation of a repository, interim storage facility, and/or intermodal transfer facility, including liability for costs and damages resulting from terrorism/sabotage against nuclear waste shipments. DOE should share security-related information with state and local governments to the maximum extent practicable." [12]

COMPREHENSIVE THREAT ASSESSMENT

Driven by regulations and the need to protect the public from catastrophic events, the nuclear industry has a continuous quality improvement process for security against human-initiated events. The two recently issued DOE NEPA documents, the Draft Supplemental EIS and the Draft Rail Alignment EIS, employ some of the methods used by the industry to protect fixed assets like reactors, but the analytical method employed by DOE for the Yucca Mountain transportation effort does not use state of the art assessment techniques, nor does the assessment effort meet industry standards for fixed site security.

The problem is two-fold: How to assess the threat of human-initiated events against spent fuel shipments to Yucca Mountain nationally, and secondly, for the proposed Caliente rail line in Nevada. Human initiated events refer to the range of malevolent acts that could be perpetrated on the shipments – including such events as terrorism, sabotage, deliberate accidents and violent protest movements. [13] Shipments refer to the various means that will be used to move spent nuclear fuel (SNF) and high-level radioactive waste (HLW) into the national transportation system/proposed Caliente rail corridor from their current storage facilities at commercial nuclear

power plants, DOE weapons production sites, and from other DOE serviced/regulated/owned source facilities.

This paper recommends specific and detailed methodologies that are used in social science and industry that, taken together, could constitute a comprehensive threat assessment for the proposed Yucca Mountain transportation system:

- The identification of relevant human-initiated events
- A systematic four level assessment of human-initiated event risks for the transportation modes, facilities, corridors, etc.
- The four step produces a matrix of human initiated events and attack scenario exemplars

HUMAN-INITIATED EVENTS

Several large categories of human-initiated events can be identified across the major components of the transportation system and relative to the known or expected characteristics of the Yucca Mountain transportation system. These include terrorism, sabotage, accidents and protests. [7,13] The table below lists these four event categories and notes how they may apply to the four major transportation components derived from the DOE Transportation Concept of Operations [14] and DOE Draft National Transportation Plan. [15]

Threat Categories	Origination Point	Transport Activities	Transfer Facilities	Destination Facilities
Terrorism Attacks	**X**	**X**	**X**	**X**
Sabotage	**X**	**X**	**X**	**X**
Deliberate Accidents	**X**	**X**	**X**	**X**
Violent Protests	**_**	**X**	**X**	**-**

Terrorism attacks are defined here as those malevolent actions that are designed to cause significant symbolic events, a significant incident that acts as a statement in opposition to the shipments or an act that directly attacks the transports, casks, facilities for handling shipment casks or the personnel that are involved in the four categories of transportation infrastructure noted above. These terrorism acts will range on a continuum from symbolic events that are not intended to result in a release of radioactive materials up to sophisticated full-scale assaults designed to release/disperse the casks radioactive contents. These attacks may be motivated by a political/social/religious agenda, attacks prompted by an anti-federal government agenda, attacks based on creation of economic dislocations in the energy sector, or attacks that are inspired by a social issue. These attacks may be perpetrated by foreign nationals, American citizens, or any combination of the two.

Sabotage is defined herein as those malevolent activities that could interfere with the safe and secure loading and transportation of the nuclear wastes. Examples may include the use of insider information, employee tampering with casks, large scale labor problems, and/or deliberate contamination of casks/transports to delay shipments. Sabotage can also be defined as other

activities detrimental to the safe and secure transport of these materials. Sabotage acts will also exist on a continuum from attacks not intended to damage a cask up to an act designed to release/disperse the inventory of radionuclides. The motives for such attacks are considered to be the same as for the terrorist attacks and acts of sabotage may be perpetrated by the same adversaries.

Deliberate Accidents are defined here as those malevolent human-initiated events that result in endangerment of the shipments, their casks, or the overall shipment campaign. These may come from deliberate acts by the public interfering with shipments and from negligent acts of those within the system that can create a potential, minimal or significant release of the highly radioactive contents. These deliberate accidents may result in limited damage to the cask and release of their contents upwards to a release that could be deemed a significant radiological event. Like terrorism and sabotage, these acts will also exist on a continuum from attacks not intended to damage a cask up to an act designed to release the inventory of radionuclides. The motives are considered to be the same as for the terrorist attacks and they may be perpetrated by the same parties.

Violent Protests are defined as those potentially malevolent activities that could interfere with the safe and secure transportation of the nuclear wastes. These protests may also be used as a rouse to hide the intentions of malicious actors who seek to commit acts of terrorism or sabotage by hiding their actions in the larger protest group. This category is included to recognize the fact that these shipments will face significant opposition from protesters, based on the experiences of other shipment campaigns around the world. Such large scale protests may endanger the shipments and/or public health by delaying shipments and increasing routine doses to the population. These acts will also exist on a continuum from attacks not intended to damage a cask up to an act designed to release the inventory of radionuclides. The motives for such attacks are considered to be the same as for the terrorist attacks and they may be perpetrated by the same parties.

THREAT ASSESSMENT PROCESS

A range of threat assessment procedures should be conducted prior to commencement of shipments and continued during the shipping campaign, in a way that measures risks over time, and enables assessments to be continually updated. [13] The longitudinal risks may need to be assessed because of a rise in energy related terrorism acts, [16] and as part of the on-going DOE obligation to operate under procedures equivalent to the NRC physical protection regulations (10CFR73.37), although DOE is not subject to the NRC regulations. The authors of this paper offer the following four-step, analysis-in-depth process as a means to make such assessments (noted as analysis-in-depth).

Step One – Meta Threat Analysis

The analysis-in-depth protocol's first step would be to consider a wide range of potential threats and consequences via-a-vie shipments of SNF and HLW to Yucca Mountain. Such a systematic assessment would first involve an exhaustive meta-analysis of the literature relative to attacks on shipments of hazardous materials, including SNF and HLW. This process would need to account for emerging threats and tactics being employed by terrorists/adversaries around the globe. It would also include IAEA (2007) guidance documents on the subject and documentation of threats that have arisen in the global theater where terrorists/adversaries operate. This data should then be vetted with outside experts, not just internal DOE security personnel, to define the various challenges that the Yucca Mountain transportation effort could face over the five decade life span

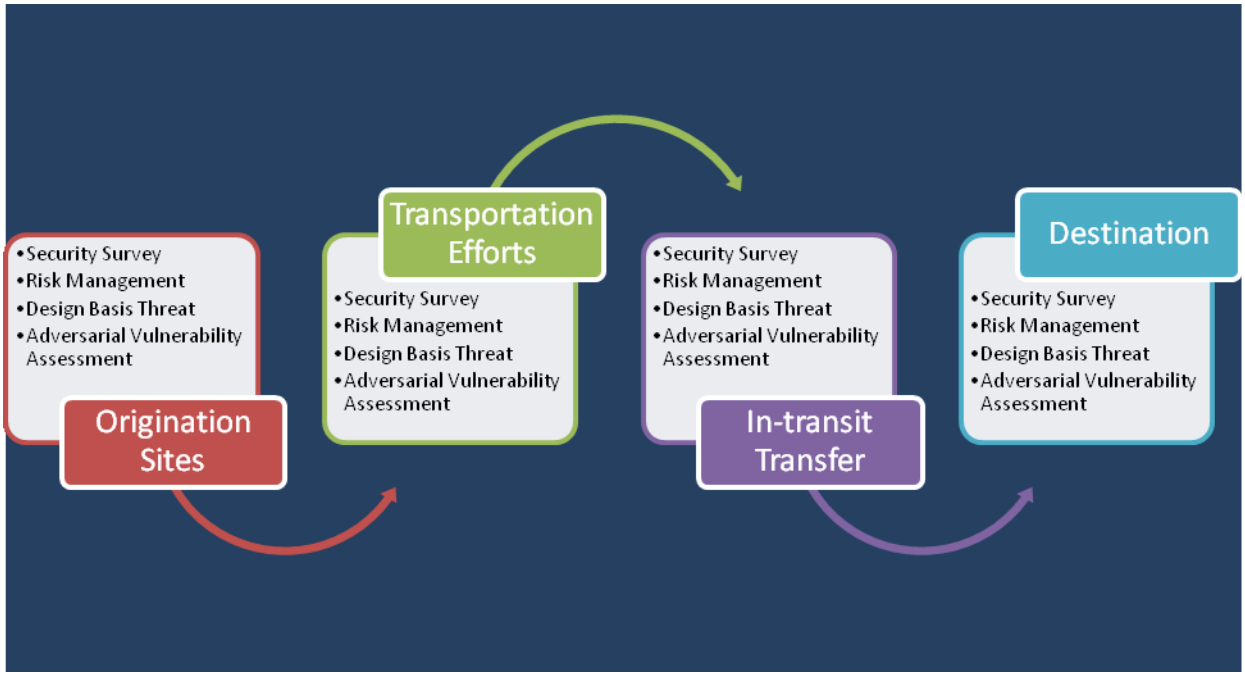
of the proposed project. Emerging from this effort would be a pro-active catalogue of transportation risks and issues that would inform a NEPA analysis, not just cherry-picked scenarios that react to the latest criticisms from Nevada studies, government analysis and/or those generated by the National Academy of Sciences. [1, 2, 7, 13, 17, 18, 19]

Step Two – Vulnerability Assessment Process

Transportation security for a cargo as dangerous as the highly radioactive SNF and HLW should prompt planners to use the best available techniques to reduce threats from human-initiated events. Typically security professionals use four levels of vulnerability assessment techniques to protect nuclear facilities and other critical industrial applications. [20, 21] Each technique has strengths and weaknesses but with the combined (sometimes referred to as triangulated) use of all of these techniques, as a research strategy, allows for improvements in security. That is, the use of more than one of these offers a more robust methodological approach to the task at hand, all four allows for a form of defense-in-depth, a common principle in nuclear security.

These four techniques offer a comprehensive risk identification and mitigation potential for security (and safety) issues relative to the proposed Yucca Mountain transportation program. In order to use these techniques for the Yucca Mountain project it is first useful to identify where they may apply to the overall transportation effort. The following chart helps situate these four techniques relative to the four major components of the transportation infrastructure.

TRANSPORTATION ANALYSIS-IN-DEPTH
RISK REDUCTION STRATEGY



The examination of how these four identification, reduction and mitigation techniques can be used in the systematic assessment of risk for the Yucca Mountain project, the analysis-in-depth risk reduction concept noted above, will require some details on what each technique will entail in real world practice.

First, it is critical that they should be considered an integrated system of analysis, albeit one with some level of analytical hierarchy. The following chart demonstrates their interrelationship and the preferred hierarchy.

Analysis-In-Depth Concept

Security Surveys. Security surveys are the first level in this overall transportation risk assessment schema. These surveys represent a physical examination of the transportation security arrangements and typically use a check list approach to the examination of risks. This allows for the standardization and management of the assessment process. [22] These checklists aid security efforts and provides for a consistent, albeit unimaginative examination of risks. [21] This form of security management is typical for any number of industrial applications and has a long tradition in security. At a minimum this survey technique needs to be performed at various levels of the proposed Yucca Mountain transportation effort (for example at origination sites, for transportation efforts, at in-transit transfer facilities, and for destination conveyance infrastructures).

The problem with this technique is that it is typically not focused on the adversaries and does not necessarily encourage thought relative to new countermeasures as risks change over time. In fact surveys become reified and represent a binary (good/bad, black/white) approach to security and risk mitigation. They seem to imply that risks will somehow emerge from the world and show themselves during such surveys. Checklists are also fixed lists of observations to be conducted and typically closed to emerging risks that have heretofore not been known or overlooked. The

list becomes what human assets are fixated on, not focusing security personnel on the creative protection of the cargoes, rather making them focus on paperwork. These surveys are often misused, especially when they come to represent ways to manage people and ensure compliance to a security regime or regulations. [21]

Security surveys have a place in the overall transportation efforts but they are not in and of themselves a cure for the risks that transportation efforts to Yucca Mountain will face. They represent a tool that should be employed by those involved in the transportation effort and at all levels of the transportation infrastructure. They are the first line of defense since they are carried out traditionally by line staff and management. They also require periodic updates, monitoring and analysis as to their ability to meet current challenges and contemporary threats. They represent the first line of a transportation specific defense-in-depth concept yet to be adopted by DOE.

Risk Management. The second step in the analysis-in-depth risk assessment process is to use well understood and common place risk management techniques. The process of risk management is fairly straightforward. In the first phase of the risk management process the analyst begins with identification of the assets in need of protection and ends with the identification of safeguards and countermeasures. [21, 23, 24, 25, 26] Thus, the organization using the risk management technique should basically follow the flow of the following interrelated items:

After this largely abstract task is completed, the organization then uses an expert opinion process to rank order priorities and probabilities are assigned to each sub-phase noted above. Typically this involves predominantly quantitative outcomes and these outcomes are summarized in tables, charts, and the like. Thereafter the transportation management team would appropriate, and field, security resources accordingly. As implied by the chart, the process begins anew once this final task is completed and in practice should become a never ending series of assessments designed to improve the overall robustness of security.

Risk management is not without critics in the nuclear field and elsewhere. Some argue that the traditional ways of conducting risk management need to be more quantitative or address more aspects than are traditionally used in such analysis, [27, 28] while others note the political nature of the use of risk management. [29, 30] A systematic examination of risk management also reveals some issues of concern. [21, 31] Once again this technique is typically binary and closed to outside input. For example, there is rarely outside input on contemporary threats and vulnerabilities since risk management rests on known (historic) security issues. This means that risk management is reactive, not proactive in mitigating risks. This also usually means that risk management is done without the creative spirit that the terrorists/adversaries bring to the table. It is initiated, managed and used by organization staff in agencies (for example the NRC and DOE) and represents the collective consensus of these sometimes limited perspectives.

Risk assessment is rarely the creative expression of alternatives. Risk management is management of risks by managers and for managers. It is not done from alternative perspectives (for example the adversaries). The assignment of probabilities in risk management is often based on fantasy-like numbers that are created out of thin air to placate internal constituencies and/or to serve political purposes. Once these probabilities are codified in tables, charts and the like, they become real in their consequences as everyone involves start to believe they are real and act accordingly. [32] The process itself and especially the documents that emerge create overconfidence in the numbers, a false sense of security that is problematic in the face of real world creativity from adversaries.

Risk management has its place in transportation planning for the potential Yucca Mountain program and the problems noted here do not negate its usefulness. As a technique it is not a be all and end all in risk assessment. The use of quantitative data helps policy makers believe in a program, but that is a two edged sword.

Design Basis Threat (DBT). The third level of the analysis-in-depth paradigm is the DBT. In some respects the DBT is a technique not that unrelated to risk management. [33, 21] A DBT is a proxy threat, a scenario based on descriptions of the threats found in the current world environment, at least at the time of its articulation. [33, 34, 35, 36] The DBT sets the standards for security personnel by defining the training, weapons and tactics that a terrorist/adversary group could use to attack nuclear facilities. The best practices of DBT usage call on its proponents to design security to face the contemporary threats, recognizing vulnerabilities and to allocate resources accordingly. [33, 37] DBTs tend to focus on infrastructure and physical security hardware, more so than risk management. [21]

The published DBT details for nuclear power plants serve as an illustration of this process and its outcomes. The DBT has been used since the 1970's in the United States and is not a single process. It has been used in various ways by different countries as the IAEA seeks to standardize the process around the globe. First and foremost it is the basis of physical protection systems (PPS) for *fixed* sites. It also serves as the means by which an evaluation of that PPS is conducted. Since 2000 the IAEA has promoted the DBT and provides (in conjunction with Sandia National Labs) nine steps for the process of development, use and maintenance of a DBT system. Besides the basic facts noted in this paragraph Blankenship [34] says that a DBT generally includes:

- ✓ Identification of the roles and responsibilities within and connected to the organization.
- ✓ Development of operating assumptions for the usage of the DBT.
- ✓ Identify a range of potential generic adversary threats.
- ✓ Identify a list of threat characteristics.

- ✓ Identify sources of threat information.
- ✓ Analyze and organize threat-related information. (Steps one to six create a threat assessment document).
- ✓ Develop threat assessment and gain consensus about said.
- ✓ Create a national level DBT.
- ✓ Introduce the DBT into the regulatory framework.

The DBT process, and specifically its first six steps, should yield both motivations for attacks, intentions of the attackers and characteristics of the attacking force. These are then matrixed across a range of adversaries (protesters, activists, extremists, criminals and terrorists). In most cases these are created from assumptions based on historic data and firmly rooted in a philosophy that insists that all threats must be "credible." This may blind the creators to new/emerging threats or threats that are evolving as past threats change to meet new circumstances. The DBT philosophy does promote the continuation of the status quo.

The NRC and DOE have updated their DBT in the aftermath of the 9/11 attacks, once in 2003 and again in 2004, both times in a process outside the normative framework for such adjustments. Specific details are not known for these most recent classified documents but the expectation is that they will take years to implement and that the final product was diluted as a result of industry concern over costs. Likewise the DBT has been criticized since it does not meet the threat threshold the 9/11 attacks presented. [38, 39, 40, 41, 42]

DBTs have their critics and the criticisms run along similar lines to those for the risk management techniques. [21] The DBT is a typically binary process and closed to outside input, primarily for security reasons. Because of the closing of discussion for security reasons there is rarely outside input on contemporary threats and vulnerabilities. Like risk management the DBT becomes a reactive device. As a proxy attack strategy it is not proactive in mitigating risks. Similar to risk management the DBT process is dominated by the organization staff. The DBT represents the collective consensus of these limited and sometimes self-serving perspectives. It does not represent a creative expression of alternatives. Once the DBT is determined it becomes real in its consequences for the agencies using this technique. The threat is what the DBT says it is, nothing more or nothing less. The DBT provides organizations, although not the public and other stakeholders, with a sense of confidence that may be disproportional to the risks and reality of a changing world. It allows the existing organization to define what the threats are, and once the DBT is constructed, to maintain a faith in their assessments, a self fulfilling belief system that can be dangerous when one is protecting something as potentially dangerous as highly radioactive wastes.

In some cases critics have argued for a layered approach to DBT implementation, a strategy that recognizes financial resource differentials in government's responsible for implementation. [43] This criticism is primarily focused on less developed nations where the resources necessary to protect nuclear assets are not readily available. In the case of advanced industrial nations the AHARA – as high as reasonably achievable - principle behind such debate suggests that these nations should achieve the IAEA's goals of securing radioactive materials against human-initiated events. These debates do not apply to the United States, a country rich in resources.

Additionally, as noted DBTs are supportive of the status quo. They seem to say to everyone involved we are doing good, look how hard we worked to define the threats and our perceptions of the vulnerabilities we face. It ignores alternative threats since they are deemed too improbable or they are not perceived at all – they are deemed a very subjective 'uncreditable.' The DBT seems to communicate to one and all that whatever terrorists/adversaries can do poses a lesser

threat than our proxy measure (DBT), a dangerous oversimplification in the world of nuclear security.

DBTs also take time to change, they are not assessed systematically but rather on an as needed basis. The DOE mandated and NRC inspired changes in implementation for weapons production facilities and commercial nuclear power plants after the 9/11 terrorist attacks illustrate this delay – changes in the DBT were revised in 2003, changed again in 2004 and are still undergoing implementation as of the sixth anniversary of those attacks with an expected date for completion being in 2008.[41,42] Supporters argue that a change in the DBT is costly but critics point out so too would be a successful attack.

The DBT is a step forward from past practice and one that allows managers to create a realistic proxy for security to train against. It is different than security surveys and risk management, not the single magic bullet to security, but rather one tool in the overall toolbox for risk mitigation. The fourth technique, adversarial vulnerability assessment, helps with some of the limitations noted for DBTs.

Adversarial Vulnerability Assessments (AVA). One critical omission of all three of the techniques detailed above is bringing the motives, mindset and creativity of the adversary into the risk equation. Those who would wish to perpetrate a human-initiated event are far more resourceful than the security surveys, risk management and DBT techniques seemingly give them credit for. To accomplish the task of recognizing such creativity Johnson [21] advises that it is necessary to conduct a "mental coordinate transformation." This means that when assessing risks for critical SNF and HLW transportation infrastructure it is necessary to think like the perpetrators, not like security professionals, not like energy company officials, and not like oversight agency management.

The major barrier faced by security professionals and risk managers in doing this task is that they are rarely prepared for this mental transformation. As a result of organizational socialization they cannot, or will not, use the opportunity to actively look for threats, to engage in the alternative and/or to think like the terrorist, saboteur or other perpetrator of human initiated events. They have difficulty letting the opponent define reality, a reality that is securely planted in their professional lives by the very industry they seek to protect – one that for many reasons does not admit gleefully to risks, threats or terrorism as a potentiality. Altering Johnson [21] for the proposed Yucca Mountain transportation project would entail the necessary mental transformation for the NEPA assessment. This is best accomplished by the following steps:

- Understand the full scope of the transportation effort. This includes all aspects, parts, components and variables in the transportation system. This is difficult since the totality of the system is enormous and in many cases individuals are asked to transform their thinking while working on small parts of the overall picture. Still it is necessary since the parts are integrated and the risk synergy for the total system far outweighs the singular transportation component risk level.

- Brainstorm in a creative, innovative, and multi-level manner that allows you to not just identify a threat, but to focus attention to a range of threats. [44] Once the totality of the program is recognized, members of a risk focus group are gathered to work on the issues, share their insight into the risks, and to brainstorm on threats facing this transportation system. These discussions would reveal attack exemplar scenarios tied to risks, not singular as is the case of a DBT, but multiple threats and with multiple consequence profiles.

- Once attack sceneries are identified, the group starts to edit these down to essential elements and exemplars that demonstrate vulnerabilities of the system, not just a single part of this complex transportation effort. This group would prioritize potential attacks which represent a range of possibilities, consequences and potential responses. These alternatives must be developed, articulated and vetted with a wide range of constitutes/stakeholders to gain additional insight and to reduce the problems of group think and collective risk blindness that sometimes arise in small groups.

- The last step is to determine the feasibility of these attacks by means of a range of attack articulations, analyze radiological consequences of these alternatives and devise countermeasures to mitigate these risks.

Several provisos are offered to those considering adopting AVA methods. First and foremost, let those involved be creative. [21] In the case of terrorism threats, the changes in technology, availability of information and tactical knowledge of adversaries demand that those involved be allowed freedom to achieve this creative approach to risk assessment. Historical data, and historically situated risk perceptions, are less significant in the face of global social challenges like currently are transpiring, a point often missed by those who work in formal organizations. AVA risk measurement is predicated on creativity which must be combined with organizational experience, technological skills and bureaucratic imagination. All of these tasks are difficult for many formal organizations to engage in but the challenges they pose are important to overcome.

Johnson [21] advises that creativity is the domain of individuals, not formal organizations. Good group dynamics can enhance this individual creative spirit and groups need to be involved to prioritize and determine feasibility. One of many techniques to help this creative process is to reverse engineer the attacks in an effort to solve problems that have yet to arise. This is a particularly cogent piece of advice given the elongated timeline for the proposed Yucca Mountain project and points out the need for a systematic longitudinal analysis paradigm so that data can be gather to inform the processes.

One of the most interesting advisements offered is that the system conducting this analysis must bring in outsiders and not use the typical cast of insider characters who have vested interests in the status quo. The use of the same old energy industry insiders and the same supporting industrial infrastructure insiders ensures the same old results. It does not offer a creative analysis of threats. Furthermore it is necessary to combine these outsiders with *creative* insiders in the brainstorming groups and set ground rules for all the contributors. These ground rules have to allow for all manner of input and treats each contribution as significant, be it from inside or outside the typical organizational patterns of thought. Johnson [21] offers some AVA imperatives as guidance. These have been modified to the Yucca Mountain project and include:

- Minimize the conflicts of interest and reduce wishful thinking on the parts of group members.

- To promote creativity in the group processes, the system must not punish those who creatively deconstruct its assumptions, bias, and working relationships.

- The overall group and its work product need to be assessed by a second group of outsiders, called assessors. These assessors should be independent from the Yucca

Mountain project, experienced in finding problems and offering solutions, and in no small measure represent the public stakeholders for the project.

- All parties involved must discard the binary way of viewing risks. This means individuals need to be able to work within the gray areas of life, not the rigid confines of an engineering perspective or other professional paradigm that promotes the status quo philosophy.

- The group members are tasked with finding vulnerabilities and risks, which is their primary purpose. As such they should not be encouraged to find no vulnerabilities or no risks, a philosophy that is counter-productive to the AVA process.

- AVAs are not a pass or fail technique for the group as a whole and the group participants must be encouraged to reject this form of thinking. The point is to find vulnerabilities and risks, not fix them per say. Thus, finding these vulnerabilities and risks is a good outcome, not a negative outcome of the group process.

- The process must be done before transportation planning is fixed in policy, done again when plans are finalized but before transport begins, and done periodically thereafter (for example bi-annually or annually).

- AVAs are a holistic approach to vulnerability identification and risk mitigation. They should not be done in isolation (for example for the rail system alone).

- The conveners, participants and/or the assessors should not be restricted as to time, budget or attack possibilities. They should be allowed to creatively face the social context of global conditions relative to terrorism, sabotage and other human initiated events.

- The group should be encouraged to never underestimate the resourcefulness, creativity or commitment of the adversary. They should remember it is the adversary that defines the threat, not the protectors.

- The group should establish a hierarchy of threats, simplest to most complex, least severe radiological consequences to most severe radiological consequences. They need also look at contingencies that would take a second tier threat and make it a major radiological event. This is one area where DBTs seem to fail, they are based on one threat and do not necessarily account for such upgrades and modifications.

- Everyone should assume that adversaries know what security arrangements are in place, have the creativity to overcome these and/or will exploit those instances where the system does not meet its presumed minimum operation levels. Systems fail and human security systems fail to protect even the most critical of assets over time.

- A range of attacks should be considered by this group: terrorism, sabotage, probes of the security system, insider/outsider/insided-outsided threats, social engineering, and the many other varieties of human initiated events that could transpire.

- The longer a system is in place, the higher its vulnerability and risk to attack. Vigilance decreases with familiarity, hence the systematic reevaluation of risks becomes

increasingly important over the lifespan of the program. It is equally important to note that once an AVA is complete, perhaps even deemed excellent by all involved, it is not the end product and cannot stand alone in the face of the ever-changing security threats faced. Once the AVA is complete it is then systematically and periodically subject to challenges from the original group, from new group participants and from new human initiated events/tactics.

- The group should avoid common nuclear industry fallacies. For example, many believe that all vulnerability will be discovered and thus all risk mitigated. Likewise they should be cautioned to avoid mindsets that see compliance as good security, layers of mediocre security equals good security, and/or that high-tech security is the answer for all vulnerabilities and risks.

AVAs are not the final and best answer to the reduction of risk, just as security surveys, risk management and DBTs do not tell the whole risk story. They are also not unknown to the nuclear industry. For example, they have already been used in the nuclear waste field for low level waste and relative to interim storage. [45] They also were advocated as one means to increase security after the terrorist attacks of September 11, 2001, [46] and for use in critical infrastructure sectors like the chemical industry. [47] These techniques have even been around a sufficient length of time to note development in their applications. [20, 21] Regarding their use in environmental policy debates, as has been the case with Yucca Mountain, Busenberg [48] notes they are effective in reducing policy disputes, a quality lacking in many suggestions for the proposed Yucca Mountain project. Lastly, these have been used in the energy industry for security considerations relative to oil and gas pipelines, a similar security dilemma to that posed by transporting nuclear waste across country to Nevada. [49]

The AVA is one tool in the overall risk assessment tool set necessary to secure the transportation of highly radioactive materials like SNF and HLW. Used in conjunction with the other three techniques it allows a different perspective on the problems the system may face, a valuable perspective not offered at any other time in the lifecycle of the transportation program.

Step Three – Scenario Exemplars

Analysis-in-depth is a management paradigm and an analytical imperative necessary to accomplish the formable task of vulnerability and risk assessment for the complex, decades-long transportation effort that would be necessary for the proposed Yucca Mountain repository. The following sections provide a risk matrix and corresponding threat scenarios that could emerge from an AVA process, if applied. The details and threats noted therein are gleamed from the literature and used to represent best practices in risk assessment for the proposed Yucca Mountain project. They do not directly correspond to the issues noted above; rather they examine a subset of the overall risk of human-initiated events for transporting nuclear wastes.

The following matrix shows some of the potential human-initiated events identified for further study:

Potential Events	Origination Sites	Transport Issues	In-transit Transfer	Destination Facilities

1. Labor disruptions with deliberate tampering of transports and/or casks. (SAB)	**X**	**x**	**x**	**x**
2. Deliberate contamination of transports and/or casks. (SAB)	**X**		**x**	
3. Disabling of shipment safeguards. (SAB)	**X**	**x**	**x**	
4. Actions meant to delay the shipment process and creating significant media attention. (PRO)		**x**	**x**	
5. Actions meant to delay transport and create increased routine radiological impacts. (PRO)		**x**	**x**	
6. Actions meant to create a dislocation of transport, cask or transportation infrastructure. (PRO)		**x**	**x**	
7. Use of geographically disadvantageous features along the transportation routes to impact shipments. (ACC)		**x**	**x**	
8. Exploitation of steep grades, tunnels, and bridges to create accident conditions potentially challenging cask integrity. (ACC)		**x**	**x**	
9. Inducement of inadvertent collisions involving toxic, explosive or flammable chemicals. (ACC)	**X**	**x**	**x**	**x**
10. Use of man-portable missiles to penetrate the cask and disperse the contents into the environment. (TER)	**X**	**x**	**x**	**x**
11. Use of military weapons/tactics to penetrate the cask and disperse the contents into the environment. (TER)	**X**	**x**	**x**	**x**
12. Use of adjacent transportation infrastructure and cargos to augment an attack and increase consequences.		**x**	**x**	
13. Capture of the cargo.		**x**	**x**	

Abbreviations: SAB = sabotage, PRO = protests, ACC= accident, TER = terrorism

Step Four – The Risk Matrix

Considering the Yucca Mountain transportation options identified by DOE, [3, 5, 8, 9, 14, 15] five modes of transportation could potentially be used for repository shipments over the projected 50-year operations period. These include:

- Rail Casks Shipped by Rail.
- Rail Casks Shipped by Barge.
- Rail Casks Shipped by Heavy Haul Truck.
- Truck Casks Shipped by Rail.
- Truck Casks Shipped by Legal Limit Truck.

These five transportation modes, traveling to Yucca Mountain from 76 shipping sites in more than 30 states, with an average shipment distance greater than 2,000 miles, will be subject to many possible attack strategies over five decades. This paper uses a range of exemplar human-initiated event strategies as an illustration of the risks associated with the transportation of these materials. These include:

- Theft of the Cargo.
- Transportation Infrastructure Attacks.
- Anti-tank and/or Stand-off Weapons Attacks.
- Capture of Shipment and use of High-Energy Density (HED) Weapons.

These exemplars suggest that a range of consequences must be factored into risk assessment since they present a range of potential attack outcomes. These outcomes include:

- Attacks to Disrupt Shipments (Minimum Radioactive Dispersal).
- Attacks to Disperse the Cask Contents (Moderate Radioactive Release).
- Attacks for Maximum Consequences (Catastrophic Radioactive Release).

The following chart allows for the analysis of these various factors simultaneously and has estimates of the consequences listed in bold as they relate to the scenario analysis that follows.

Yucca Mtn. Risk Matrix	Rail Casks Shipped by Rail.	Rail Casks Shipped by Barge.	Rail Casks Shipped by Heavy Haul Truck.	Truck Casks Shipped by Rail.	Truck Casks Shipped by Legal Limit Truck.
Theft of the Cargo.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.	**Disrupt** Disperse Max. Cons.
Transportation Infrastructure Attacks.	Disrupt **Disperse** Max. Cons.	**Disrupt** Disperse Max. Cons.	Disrupt **Disperse** Max. Cons.	Disrupt **Disperse** Max. Cons.	Disrupt **Disperse** Max. Cons.
Anti-tank and/or Stand-off Weapons Attacks.	Disrupt **Disperse Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt **Disperse** Max. Cons.

Capture of Shipment.	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**	Disrupt Disperse **Max. Cons.**

Taken together these modes, human initiated event strategies, and hypothesized consequence outcomes can be conglomerated into a risk matrix for simplified use by risk managers, security personnel and for the specific purposes of risk identification, analysis and mitigation. A radioactive dispersal, whether it is considered minimum, moderate or catastrophic for the purposes of analysis, depends on many variables, including the age of the fuel, the burn-up history of that fuel, the crud inventory in the transport cask, the degradation of the cladding, the number of assemblies in a given cask, and so forth. However, a properly constructed assessment process can address these variables, and recommend appropriate countermeasures and mitigation strategies.

CONCLUSION

This paper examined the current state of risk assessment for human-initiated events against SNF and HLW shipments to the proposed repository at Yucca Mountain, Nevada.
The attack scenarios evaluated in the Draft Supplemental EIS for Yucca Mountain, and the Draft Nevada Rail Alignment EIS, repeat the methods used by DOE and NRC over the past three decades. Those analyses assumed single-phase attack scenarios. None of these consequence assessments have evaluated impact-exacerbating tactics, such as combined use of a breaching device and a dispersal device, or use of multiple breaching devices. None of these consequence assessments have evaluated the impact-exacerbating tactics studied by counter-terrorism experts in the post-September 11 environment.

The paper offers an alternative methodology to the current DOE assessment techniques. The paper advocates use of an analysis-in-depth method that uses current risk assessment methods, but adds the well known Adversarial Vulnerability Assessments (AVA) as an extra layer of protection. The purpose of this technique is to harness the creatively and ingenuity of people outside an organization like the DOE and in doing so improve the risk analysis. Such an approach would respond to the WGA resolution on transportation terrorism risks.

The DOE Draft Supplemental EIS for Yucca Mountain, and the DOE Draft Nevada Rail Alignment EIS, underestimate both the likelihood and consequences of terrorism and sabotage against repository shipments. DOE has not employed a comprehensive threat assessment methodology like that recommended in this paper The methodology used in the DSEIS and the RA DEIS will not yield information useful to decision makers. Rather, it will tend to reinforce beliefs about the safety and security of the shipments that may be false. The assessment method advocated in this paper has two objectives: First, to provide decision makers with actionable information that will materially improve the security of shipments; and second, provide insight about flaws in the shipment method that may not be clear within a formal regulatory and/or oversight organization. Current policy discussions of Yucca Mountain shipment risks overlook the critical contribution that can be made by these external sources.

REFERENCES

1. R. J. HALSTEAD, J. D. BALLARD, "Nuclear Waste Transportation Security and Safety Issues: The Risk of Terrorism and Sabotage Against Repository Shipments," Prepared for State of Nevada, Agency for Nuclear Projects (October 1997; Revised, December 1998). This report can no longer be accessed on the web, but can be requested in writing from Mr. Joseph Strolin, Administrator, Agency for Nuclear Projects, Suite 118, 1761 E. College Parkway, Carson City, NV 89706
2. J.D. BALLARD, R.J. HALSTEAD, F. DILGER, H. COLLINS, "Planning for an Unpredictable Event: Vulnerability and Consequence Reassessment of Attacks on Spent Fuel Shipments," revised version of a paper presented at Waste Management 2005. The revised paper was not included in the proceedings, but it is available on line at http://www.state.nv.us/nucwaste/trans.htm. The majority of the contractor reports cited in the references can be found at the same website. However, most reports dealing specifically with transportation terrorism and sabotage issues must be requested in writing from Mr. Joseph Strolin, Administrator, Agency for Nuclear Projects, Suite 118, 1761 E. College Parkway, Carson City, NV 89706.
3. DOE, "Draft Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada," DOE/EIS-0250D, U.S. Department of Energy, Washington, DC (July 1999).
4. R. LUNA, et al., "Projected Source Terms for Potential Sabotage Events Related to Spent Fuel Shipments," SAND99-0963 (1999).
5. DOE, "Final Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada," DOE/EIS-0250 (February 2002). (Available on the web at http://www.ymp/gov/documents/feis_a/index.htm).
6. M. LAMB, et al," Potential Consequences of a Successful Sabotage Attack on a Spent Fuel Shipping Container: An Analysis of the Yucca Mountain EIS Treatment of Sabotage." Prepared by Radioactive Waste Management Associates for the State of Nevada, Agency for Nuclear Projects (April 2002).
7. J.D. BALLARD, R.J. HALSTEAD, F. DILGER, H. COLLINS, "Yucca Mountain Transportation Security Issues: Overview and Update," WM'07 Conference, February 25 – March 1, 2007, Tucson, AZ.
8. DOE, "Draft Supplemental Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada" DOE/EIS-0250F-S1D (2007).
9. DOE, "Draft Supplemental Environmental Impact Statement for a Geologic Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada – Nevada Rail Transportation Corridor," DOE/EIS-0250F-S2D, and "Draft Environmental Impact Statement for a Rail Alignment for the Construction and Operation of a Railroad in Nevada to a Geologic Repository at Yucca Mountain, Nye County, Nevada," DOE/EIS-0369D (October 2007).
10. R. LUNA, "Release Fractions from Multi-Element Spent Fuel Casks Resulting from HEDD Attack," WM'06 Conference, February 26 –March 2, 2006, Tucson, AZ.
11. WGA, Making the West the Best: Western Governors' Association 2007 Annual Report. Download date: August 25, 2007. Available online at: http://www.westgov.org/wga/publicat/annrpt07.pdf.
12. WGA, "Western Governors Association Policy Resolution 07-02: Assessing the Risks of Terrorism and Sabotage against High-Level Nuclear Waste Shipments to a Geologic Repository or Interim Storage Facility."
13. J.D. Ballard, J. D. "Asymmetrical Sabotage Tactics: Nuclear Facilities/Materials and Vulnerability Analysis." Conference proceedings. (2002) Publication available at www.numat.at, download date August 28, 2007.
14. DOE, "Transportation System Concept of Operations," DOE/RW-0584 (April 2006).
15. DOE, "National Transportation Plan," pre-decisional draft (July 16, 2007).

16. T. MARENKO, "Terrorist Threat to Energy Infrastructure Increases," Jane's Intelligence Review, Download date July 28, 2007. Available online at http://www.ciaonet.org/wps/mat04/mat04.pdf
17. CRS, "Nuclear Power Plants: Vulnerability to Terrorist Attack," RS 21131 (August 8, 2007).
18. NAS, "Going the Distance? The Safe Transport of Spent Nuclear Fuel and High-Level Radioactive Waste in the United States," Washington, DC: The National Academies Press (2006).
19. R.J. HALSTEAD, F. DILGER, J.D. BALLARD, "Beyond the Mountains: Nuclear Waste Transportation and the Rediscovery of Nevada," WM'04 Conference, February 25 – March 1, 2004, Tucson, AZ.
20. R.G. JOHNSON, "Adversarial Safety Analysis: Borrowing the Methods of Security Vulnerability Assessments," Journal of Safety Research 35: 244-248 (2004).
21. R.G. JOHNSON, "Unleashing Your Inner Mother-in-Law: How to do an Adversarial Vulnerability Assessment," Presentation at ASIS annual conference, Orlando, FL (2005). Download date: July 23, 2007. Available at: http://pearl1.lanl.gov/external/c-adi/seals/images/AVA.ppt
22. J.F. BRODER, Risk Analysis and the Security Survey. Boston: Butterworth-Heinemann (1999).
23. H. KUMAMOTO, E.J. HENLEY, Probabilistic Risk Assessment and Management for Engineers and Scientists. Hoboken, NJ: Wiley. (2000)
24. C. ROPER, Risk Management for Security Professionals. Boston: Butterworth-Heinemann (1999).
25. R. KNIEF, Risk Management: Expanding the Horizons in Nuclear Power and Other Industries, Boca Raton, FL: CRC Press (1991).
26. C. STARR, "Risk Management, Assessment, and Acceptability." Risk Analysis, Volume 5 (1985).
27. R.P.HAMALAINEN, M.R.K. LINDSTEDT, K. SINKKO, Multiattribute Risk Analysis in Nuclear Emergency Management. Malden, MA: Blackwell Publishing (2000).
28. S. RAYNER, R. CANTOR, "How Fair is Safe Enough.: The Cultural Approach to Societal Technological Choice." Risk Analysis, Volume 7 (1987).
29. N. PIDGEON, R.E. KASPERSON, P. SLOVIC, The Social Amplification of Risk, New York: Cambridge University Press (2003)
30. P. SLOVIC, "Perceived Risk, Trust, and Democracy." Risk Analysis, Volume 13 (1993).
31. H.H. WILLIS, A.R. MORRAL, T.K. KELLY, J.J. MEDBY, Estimating Terrorism Risk. Santa Monica: Rand Corporation (2005).
32. L. CLARKE, Mission Improbable: Using Fantasy Documents to Tame Disaster. Chicago, Illinois: University Of Chicago Press (2001).
33. NRC, "Design Basis Threat." (2007) Download date August 5, 2007. Available online at http://www.nrc.gov/
34. J. BLANKENSHIP, "International Standard for Design Basis Threat (DBT)." Paper presented at the NUMAT Conference, 2005, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
35. S. CHETVERGOV, "Evolution of Nuclear Security in the Republic of Kazakhstan." Paper presented at NUMAT Conference,2005, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
36. D. ELLIS, "Training Programs for the Systems Approach to Nuclear Security." Paper presented at NUMAT Conference, 2005, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
37. I. KHRIPUNOV, "Nuclear Security Culture: A Generic Model for Universal Application." Paper presented at NUMAT Conference, 2005, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
38. IAEA, "Requirements for Physical Protection Against Sabotage of Nuclear Facilities and Nuclear Material During Use and Storage." (2007) Download date: August 5, 2007. Available online at http://www.iaea.org/
39. NRC, 2005. "Design Basis Threat," (2005).Federal Register, Volume 70, Number 214.
40. D. HIRSCH, D. LOCHBAUM, E. LYMAN, "The NRC's Dirty Little Secret: The Nuclear Regulatory Commission is Still Unwilling to Respond to Serious Security Problems." Bulletin of Atomic Scientists, Volume 59 (May-June 2003).

41. GAO, "Nuclear Security: Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environmental Sites: Statement of Gene Aloise, Director, Natural Resources and Environment." Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, United States House of Representatives. July 26, 2005.
42. GAO, "Nuclear Power: Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve its Process for Revising the Design Basis Threat: Statement of Jim Wells, Director: Natural Resources and Environment." Testimony before the Subcommittee on National Security, Emerging Threats and International Relations, United States House of Representatives. April 4, 2006.
43. S. KONDRATOV, F. STEINHAUSLER, "Why there is a need to Revise the Design Basis Threat Concept." Paper presented at NUMAT Conference, 2005, Salzburg Austria. Download Date August 4, 2007. Available online at http://www.numat.at/
44. E.G. BITZER, R. JOHNSON, "Creative Adversarial Vulnerability Assessments," Journal of Physical Security, Volume 2 (2007). Download date: August 7, 2007. Available on-line at http://jps.lanl.gov/.
45. J. BIBLE, R.J. EMERY, T. WILLIAMS, S. WANG, "A Security Vulnerabilities Assessment Tool for Interim Storage Facilities of Low-level Radioactive Waste," Health Physics 91: 566-573.
46. J.O. LUBENAU, D.J. STORM, "Safety and Security of Radiation Sources in the Aftermath of 11, September 2001." Health Physics 83: 155-164 (2002).
47. D.A. MOORE, B. FULLER, M. HAZZAN, J.W. JONES, "Development of a Security Vulnerability Assessment Process for the RAMCAP Chemical Sector," Journal of Hazardous Materials 142: 689-694 (2007).
48. G.J. BUSENBERG, "Collaborative and Adversarial Analysis in Environmental Policy," Policy Sciences 32. (1999) Download date: August 8, 2007. Available on-line at: www.springerlink.com.
49. T. VAN HINTE, T.I. GUNTON, J.C. DAY, "Evaluation of the Assessment Process for Major Projects: A Case Study of Oil and Gas Pipelines in Canada." Impact Assessment and Project Appraisal 25: 123-137 (2007).
50. J.BETTIE, "NRC Takes Two Roads on Terror Review Issue." The Energy Daily, February 27, 2007.