The MIAN Security Enhancement Process

A Program for Assessing and Enhancing Security at Sites that Use or Store Radioactive Materials for Medical, Industrial and Academic Applications

Final Report for Phase II

J. William Jones, Ph.D., Principal Investigator

Robert E. Nickell, Ph.D., Subject Matter Expert

John Haygood, M.S., Health Physicist, Subject Matter Expert

January 2013

Final Report to the Alfred P. Sloan Foundation in Fulfillment of Grant Number 2011-6-31

The MIAN Security Enhancement Process

By

J. William Jones, Robert E. Nickell, & John R. Haygood

Executive Summary:

Under a Phase II grant from the Alfred P. Sloan Foundation, the firm of J. William Jones Consulting Engineers (JWJCE) extended the results of a Phase I effort on the security of medical, industrial, and academic nuclear (MIAN) sources to include three significant deliverables: (1) a MIAN security self evaluation package, referred to as the Security Enhancement Program; (2) a website supporting the MIAN security efforts; and (3) a MIAN security awareness effort aimed at both the general public and at critical professional and government-sponsored organizations. In particular, the Security Enhancement Program contains both a screening tool that can help MIAN custodians to determine the desired security profile for their facility or facilities, as well as a security self-assessment software package that guides the custodians in determining the adequacy of existing security measures, and the risk-reduction benefits of potential enhanced security measures.

The Phase II grant represents a follow-on to a Phase I effort suggested to the Sloan Foundation by the Federal Bureau of Investigation (FBI) and the International Criminal Police Organization (ICPO), widely known as Interpol. That Phase I effort was conducted by the same team of three investigators, then working under the auspices of the ASME Innovative Technologies Institute (ITI), also on a grant from the Sloan Foundation.

The major thrust of both the Phase I and Phase II efforts has been the specific application of a risk-based methodology called Risk Analysis and Management for Critical Asset Management (RAMCAP^{TM}), originally developed by the U.S. Department of Homeland Security (DHS), and adapted in this specific case for situations involving separate locations for the radioactive source material and the potential consequences to targets from dispersal of that source material. That adaptation has led to a much more complex risk assessment procedure that includes risks related to acquisition of the source material, transport of the acquired source material to one or more staging points, preparation of the dispersal device, and transport and deployment of the device to the selected target(s). Within the risk assessment phases, Phase II concentrated on the risk self-assessment at the source custodian's facilities, first providing guidance on establishing the level of source security required – based on prevention of unauthorized removal of source material, minimizing the likelihood of unauthorized removal of source material, or merely reducing the likelihood of unauthorized removal of source material. Then, with the desired risk profile selected or assigned, the source custodian may use the MIAN Security Status Evaluator to quantitatively review the existing security system, which is provided at no cost, and then may consider the potential benefits of enhanced security measures.

The Phase II approach takes the position that, while regulators and licensees generally believe that a large radioactive source is needed to field a radioactive dispersal device (RDD), the authors feel that a more expansive security strategy should be adopted that covers the potential for terror and fear from relatively small sources and possibly accumulated small sources[1]. While the public information component of the Phase II effort attempts to address realistic consequences, it is also recognized that the secondary and tertiary consequences of even small RDDs would be profound, especially during the period of uncertainty following a dispersal event before the magnitude has been determined. The Phase II approach also takes the position that, in addition to regulatory oversight, custodians of radioactive sources are serious about their custodial responsibilities and dedicated to reasonable, self-administered security principles. The Security Enhancement Program is intended to take advantage of that dedication. The public information component of the Phase II effort is intended to reach that dedicated audience and guide the source custodians in their security self-assessments.

[1] Consider that a terrorist event involving a 100-Curie source of Co-60 would cause an area to be contaminated such that its closure and subsequent control for some length of time would create fear and concern for those in or near to that area. Also consider that a source of only 50 millicuries might be involved, but with terrorist claims that the source was 100 Curies;, by the time authorities could determine that a much smaller source was involved, with minimal need for recovery and remediation, a nearly equal level of terror would be realized.

Section 1. Introduction and Overview

There are thousands of medical, industrial, and academic facilities in the United States that are licensed to use radioactive materials and many more similar sites can be found around the world. These materials are used for various purposes, including medical and veterinary treatments, industrial applications, and academic research. (The abbreviation MIAN refers to radioactive materials from medical, industrial, and academic nuclear sources.) There is continuing concern that these nuclear materials pose a serious danger to the public in case of a lapse of security or a natural event such as an earthquake, hurricane, or other naturally occurring event. A lapse in security can result in radioactive material falling into the hands of terrorists and being used for sinister purposes. If these materials should fall into the wrong hands, they could be used in radioactive dispersal devices (RDD), so-called dirty bombs, or be released into the environment by other means. Under extreme conditions, they can potentially cause fatalities, serious injuries, and environmental damage, which could require costly decontamination or abandonment of valuable locations. In virtually all cases, deployment of an RDD would cause disruption of commerce and/or denial of service, or loss of access to public locations.

In 2009 the Alfred P. Sloan Foundation (Sloan) was approached by the FBI and Interpol and asked to consider providing funding to assess the risk posed by terrorists utilizing radioactive materials in an attack on the public. Sloan contracted with ASME-ITI, a division of ASME International, to attempt to quantify the risk and propose methods by which risk could be reduced. A report was delivered to Sloan in February 2011, the Phase I report[2], that provided a methodology for risk assessment using RAMCAP[3]. A second phase (Phase II) contract was initiated in July 2010 with J. William Jones Consulting Engineers, Inc. to develop a voluntary self-assessment tool that would be provided to all interested parties at no cost. The deliverables from the Phase II contract, all of which are provided free to potential users, include the following:

1. MIAN Security Enhancement Process (this document)
2. Security Enhancement Program (Microsoft Word document and an Excel spreadsheet)
3. MIAN Narrated PowerPoint Overview

[2] Methodology for Assessing Risk from Radioactive Materials Found in Medical, Industrial and Academic Sites, Final report to the Alfred P. Sloan Foundation in Fulfillment of Grant Number 2009-10-18

[3] Risk Analysis and Management for Critical Asset Protection (RAMCAP *Plus*), with Jerry P. Brashear, Wiley Handbook of the Science and Technology of Homeland Security, in press (February 2010), John Wiley & Sons, New York. Voeller, John (ed.).

4. MIAN PowerPoint presentation (longer version of above without narration)

5. IAEA publication- Code of Conduct for on the Safety and Security of Radioactive Sources

6. IAEA publication- Security of Radioactive Sources

7. Weapons of Mass Disruption (Book by Jones and Haygood, both PDF and eBook formats)

8. Phase I MIAN report (PDF format).

Upon receiving this package, the recipient should listen to the narrated overview, item 3 above. This short PowerPoint presentation introduces the project and describes the contents of the Security Package. The longer PowerPoint presentation is useful for obtaining a more thorough understanding of the Security Enhancement Process and can be used to explain the MIAN project scope and objectives to other interested parties.

The Security Enhancement Program (Item 2 above) provides an easy to use tool for first determining the need for further assessment (screening tool) and a more comprehensive evaluator for determining the current security status of a facility. This program includes guidelines for security requirements based upon the quantity and type of materials at the facility. Suggestions for increasing security are also included. The program can be used to perform "what if" evaluations to assess the value of added security measures. This process is key to understanding the cost of "buying down" risk by adding additional preventative measures. It allows the user to weigh the cost of enhancements against the increase in security. This program is designed to be used by site security personnel who have the responsibility for preventing the unauthorized use of all radioactive materials used or stored by the licensee. Using this program is completely voluntary and there are no reporting requirements; all work products are confidential and are produced solely for the use of the licensee. The program goes beyond NRC Increased Controls and considers that the terrorist can "stockpile" quantities of material and accumulate quantities that exceed the danger levels currently prescribed as a lower bound for having to meet the NRC increased controls requirements. This program does not evaluate individual security devices, systems, and methods for efficacy, but assumes that selected ones will be adequate to accomplish the desired effect.

It was our goal to provide a useful tool for security personnel that is not onerous to use. The authors believe that a voluntary program such as this is greatly preferred by licensees over additional regulation. Further, an attack by terrorists using radioactive material would almost certainly result in draconian security measures by the government (such as have been promulgated for air travel) which would greatly increase the cost to licensees. The best way to prevent further governmental regulation, as well as to avoid the devastating consequences of such an attack, is to prevent terrorists from obtaining these materials.

Two important IAEA publications have been included in the package. These documents should be read and retained, as they are excellent sources of information. They are discussed in greater detail in the following section of this report.

The next item in the package is a book[4] written by two of the investigators working on this project. This book attempts to provide realistic scenarios that illustrate how terrorists can utilize radioactive materials to destroy and disrupt the lives of our citizens. The goal of the terrorist is to wage war using unconventional means to achieve large consequences at a relatively small cost. This is often described as an asymmetric war since the terrorist does not have the means to fight a conventional battle, matching their enemy armament for armament, weapon for weapon. The inherent fear of nuclear materials combined with the relative ease of obtaining enough radioactive material to cause panic and disrupt commerce, makes them highly desirable weapons. Book files are included in both PDF and EBook reader formats.

Section 2 describes the Security enhancement tools in more detail, with examples of tool application provided in Appendix 1.

Section 3 contains a discussion of how the RAMCAP risk assessment methodology was applied to the MIAN project. This section, combined with the Phase I report, also included in the package (Item 8), provides the interested user with a more detailed explanation of the risk assessment process. Section 3, combined with Appendix 2, summarizes how the RAMCAP risk assessment methodology employed leads to the need for developing the Enhanced Security Assessment tools. It also explains why the MIAN risk analysis procedure differs from prior RAMCAP applications, which are directed toward fixed targets such as chemical plants, water treatment plants, nuclear power plants, etc.

Section 4 contains our conclusions and recommendations as well as suggestions for further reducing risk through a public awareness program.

[4] The Terrorist Effect, Weapons of Mass Disruption, The Danger of Nuclear Terrorism, by James William Jones and John R. Haygood. The authors are making this book available free of charge in digital format. Hard copies can be obtained from Amazon, Barns & Noble, and other booksellers. More information is available at the web site JWJCE.com.

Section 2. Enhanced MIAN Security Tools

The emphasis of the Security Enhancement Program is on two applications to be used by MIAN custodians for voluntary self evaluation. The first application is referred to as the MIAN Security Screening Tool. This application was introduced in the Sloan Foundation Phase I final report (see page G-5, footnote 1), and is intended to be used by the MIAN custodian to determine the general boundaries of the security program elements at the site or sites under the MIAN custodian's control, and to determine the need for any further security self-assessment. The second application has been developed during Phase II of the Sloan Foundation effort, and is referred to as the MIAN Security Status Evaluator (ESP Calc). This tool permits the MIAN custodian to self evaluate the various and myriad elements of each site security program, develop a quantitative measure of the current status of that site security program, and then review the effect of selected security enhancements on that quantitative measure, should such enhancements be deemed desirable and cost effective. These tools have been combined seamlessly into the Security Status Evaluator (Item 2 in the MIAN package), with four examples provided in Appendix 1.

The quantitative measure that is obtained from the MIAN Security Status Evaluator is not intended to establish the acceptability of the current site security program per se, nor is that measure intended to require enhancements in the case of a relatively low self-assessed value. Instead, that quantitative measure should enable the MIAN custodian to determine whether the current site security program is commensurate with the selected or assigned ***risk profile***, as discussed below, and to review a wide variety of potential security program enhancements to determine which, if any, of those potential security program enhancements represent essential improvements.

Therefore, the first step in the self assessment process is to determine the ***risk profile,*** either self-assigned or assigned by a regulatory authority**.** Following the guidance provided by the International Atomic Energy Agency (IAEA)[5], the goal for the security program depends upon whether the ***risk profile*** intent is to completely ***prevent*** the unauthorized removal of a source (called Security Level A), or to ***minimize the likelihood*** of unauthorized removal of a source (called Security Level B), or to ***reduce the likelihood*** of unauthorized removal of a source (called Security Level C). Clearly, prevention of risk of removal requires a much more robust security program than does minimization of risk of removal, and minimization of risk of removal requires a much more robust security program than does reduction of risk of removal.

[5] IAEA Nuclear Security Series No. 11, Security of Radioactive Sources: Implementing Guide, International Atomic Energy Agency, Vienna, Austria, 2009, p. 15

The risk profile choice is generally established through consideration of the danger posed by the source or sources, called a D-value[6], which is defined as the radionuclide ***specific activity*** of a source. The D-value is then used to normalize the ***total activity*** of the radioactive source material, defined by the symbol A and measured in Terabecquerel units (TBq). The normalization process permits a direct risk comparison with other normalized sources. Based upon this A/D ratio and other factors (e.g., half-life of the sources), Table 5 of the IAEA guidance recommends the assignment of security levels for certain source categories. For example, radioisotope thermoelectric generators (RTGs), panoramic irradiators, large self-shielded irradiators, medical teletherapy units, and fixed multibeam teletherapy units (gamma knives) are all recommended to be placed in Security Level A, which requires the ***prevention*** of unauthorized removal of a source – the most stringent security category. Typical sources recommended for Security Level B are those for smaller self-shielded irradiators, industrial gamma radiography units, and high/medium dose rate brachytherapy devices. In this case, the security program is intended to ***minimize*** the likelihood of unauthorized removal of a source, still a moderately severe requirement. Typical sources recommended for Security Level C are those for such items as well logging devices. Table 5 of the IAEA guidance also describes other source categories that have sufficiently low A/D ratios that they fall beneath the levels for which even Security Level C elements are recommended.

It should be noted that, in 2005, the U.S. regulator – the U.S. Nuclear Regulatory Commission (NRC) -- ordered that certain radioactive materials (or isotopes), above certain quantities, be provided with more robust security arrangements to limit the likelihood of unauthorized removal for possible use as a terrorist weapon. These new requirements are referred to as "Increased Controls (IC)" and are applied to all U.S. licensees, whether directly monitored by the NRC or by one of the Agreement State (AS) assignees. At a minimum, the security systems for sources subject to IC must continuously monitor the materials and notify local law enforcement agencies (LLEA) of any breach of security, which thereby provides for a timely armed response by the LLEA. In addition, background checks and fingerprinting of persons authorized to deal with the materials are required. More stringent security, such as alarmed vehicles, is also now required for transport of IC level nuclear material. Nuclear power plants, certain sterilization irradiators, and some source manufacturers are under a higher level of security called "Safeguards." The requirements for IC lead naturally into a discussion of IAEA Security Levels A, B, and C, and eventually to the MIAN Security Status Evaluator.

Since the goal of Security Level A is to ***prevent*** the unauthorized removal of radioactive sources, the requirements for the security program elements of **Detection**, **Delay**, **Response**, and **Security Management** emphasize immediacy (see Table 6 of the IAEA security program guidance), such as "*immediate detection of any unauthorized access to the secured area/source location,*" "*immediate detection of any attempted unauthorized removal of the source (e.g., by an insider),*" "*immediate*

[6] EPR-D-Values, Dangerous Quantities of Radioactive Material (D-Values), International Atomic Energy Agency, Vienna, Austria 2006. p. 3

assessment of detection," and "*immediate communication to response personnel*." Such requirements would nominally require electronic intrusion detection systems, electronic tamper detection equipment, and continuous surveillance by operator personnel. Immediate communication might imply diverse means of communication, such as combinations of telephones, radios, and automatic alarms. The **Delay** security program elements also emphasize time, but in a quite different way. In this case, the security system would nominally be required to have at least two barriers between the sources and unauthorized personnel, thereby introducing a sufficient amount of delay to enable timely action by response personnel. Security Level A **Response** also has the objective of being "*immediate*," and with sufficient resources of size, equipment, and training to successfully interdict the attack. Security Level A **Security Management** includes such items as access controls, trustworthiness verification, and protection of sensitive information.

Since the goal of Security Level B is to minimize the unauthorized removal of radioactive sources, the requirements for the security program elements of **Detection**, **Delay**, **Response**, and **Security Management** have lesser but still important emphasis on immediacy (see Table 7 of the IAEA security program guidance). In this case, "If an attempt of unauthorized access or unauthorized removal were to occur, the response must be initiated immediately upon detection and assessment of the intrusion, ***but the response is not required to arrive in time to prevent the source from being removed***."[7] This represents a substantially less rigorous site security program, in that immediate detection of unauthorized access is required, but not "immediate" detection of an unauthorized attempt to remove a source, which permits periodic, as opposed to continuous, surveillance by operator personnel. However, Security Level B does not preclude the use of electronic tamper detection equipment that could provide immediate notification of an attempted source removal. In such a case, it should be noted that "immediate assessment and immediate notification" ***is*** required for Security Level B should **Detection** be triggered. With respect to **Delay**, **Response**, and **Security Management**, the differences between Security Levels A and B are minimal. Two types of barriers are still required to **Delay** access by separating the source from unauthorized personnel (e.g., a locked device in a secure area), immediate initiation of **Response** is required to interrupt an attempt at unauthorized removal, and controls are required to effectively restrict source access to authorized persons only as an element of **Security Management**.

When the site security goal is reducing the risk of unauthorized removal of radioactive sources, as it is for Security Level C, the emphasis on timeliness essentially disappears (see Table 8 of the IAEA security program guidance). **Detect** only requires some method for indicating attempted unauthorized removal, such as tamper detection equipment, and periodic checks to confirm source presence; however, immediate notification of any detection event is still required. **Delay** now only requires a single barrier against unauthorized removal or some form of direct observation by operator personnel. **Response** has been reduced to only a set of defined actions to take place in the

[7] IAEA Nuclear Security Series No. 11, Security of Radioactive Sources: Implementing Guide, International Atomic Energy Agency, Vienna, Austria, 2009, p. 36

event of unauthorized removal of a source, with appropriate actions to be implemented, but no emphasis on immediacy. Finally, **Security Management** for Security Level C requires the usual security plan, procedures to identify and protect sensitive information, identification measures, and methods for establishing the trustworthiness of authorized personnel with unescorted access to radioactive sources and sensitive information.

As stated previously, the MIAN Security Screening Tool, ESP Calc, is intended to assist the radioactive source custodian in a self determination of an appropriate site security level, whether that level is Security Level A, Security Level B, Security Level C, or at a level that is even below Security Level C. If the site security level has already been assigned through regulatory action, the radioactive source custodian may choose to proceed directly to the MIAN Security Status Evaluator. Additional guidance for using the MIAN Security System Evaluator is provided in Appendix IV of the IAEA security program guidance[8]. It should be pointed out that no attempt has been made to classify any site security program as either a *prescriptive* program or a *performance-based* program, although the evaluation of security program elements is generally considered a prescriptive evaluation[9].

[8] IAEA Nuclear Security Series No. 11, Security of Radioactive Sources: Implementing Guide, International Atomic Energy Agency, Vienna, Austria, 2009, p. 57 et seq.

[9] The radioactive source custodian is unlikely to have a basis for determining the potential performance of a particular site security program element without some form of defined Design Basis Threat (DBT) and some means of testing that program element against the DBT.

Section 3 Risk Assessment Methodology

The RAMCAP methodology was originally developed for use by the Department of Homeland Security and other organizations as a means of estimating the risk of a terrorist attack on a particular target. Targets, termed "assets", were defined as physical infrastructure installations, such as a chemical plant, refinery, bridge, dam, building, nuclear plant, etc. The attack typically had a two-pronged mission: first, destroy the facility and deprive users of the output from the facility and, second, to "weaponize" the target, if possible. For example, hazardous materials used or produced at the facility might be released, causing secondary consequences to the community. The key concept is that the target facility or infrastructure component was both the site of the attack and its destruction resulted in malicious consequences. The RAMCAP seven step process, illustrated by Figure 1, sought to reduce risk in a number of ways, given that the attack was only directed to that particular facility.

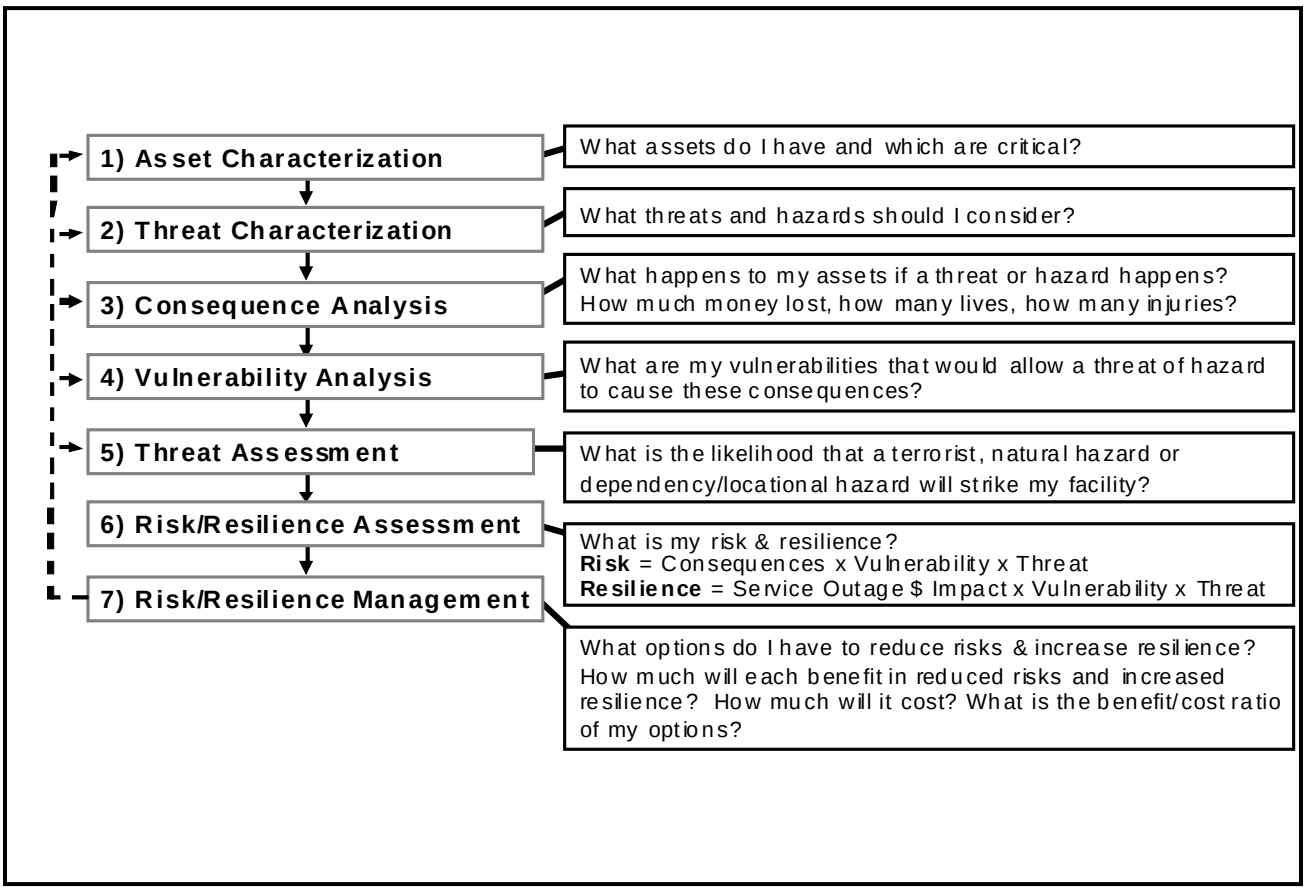

Figure 1. RAMCAP Seven Step Process

As can be seen from Figure 1, every step of the process considers only the particular target or asset. Step 1 is to identify hazards assets (at the facility being evaluated) that can result in adverse consequences. Step 2 considers how a list of possible predefined threat scenarios can be perpetrated against the asset to cause the most severe consequences, which are evaluated in step 3. Consequences considered were primarily those associated with the actual facility and the surrounding region. There is some attempt to include secondary (cascading) consequences, but only in a limited way. Step 4 attempts to identify vulnerabilities at the facility that will allow the terrorist to be successful in the attack. Steps 5 through 7 provide a methodology for calculating the risk for each attack scenario and managing risk. Risk can be reduced by either making the site more resistant to an attack (reducing the vulnerability) or mitigating the consequences of an attack. Risk management seeks to minimize risk by the lowest cost combination of these approaches.

MIAN risk assessment is significantly more complex to quantify. The most salient difference between the standard RAMCAP methodology and assessing terrorist risk using radioactive materials is that the latter must consist of two distinct acts. The terrorist must first obtain the material and then successfully deploy this material at the site of the attack while avoiding interdiction by law enforcement. . This is illustrated in Figure 2.

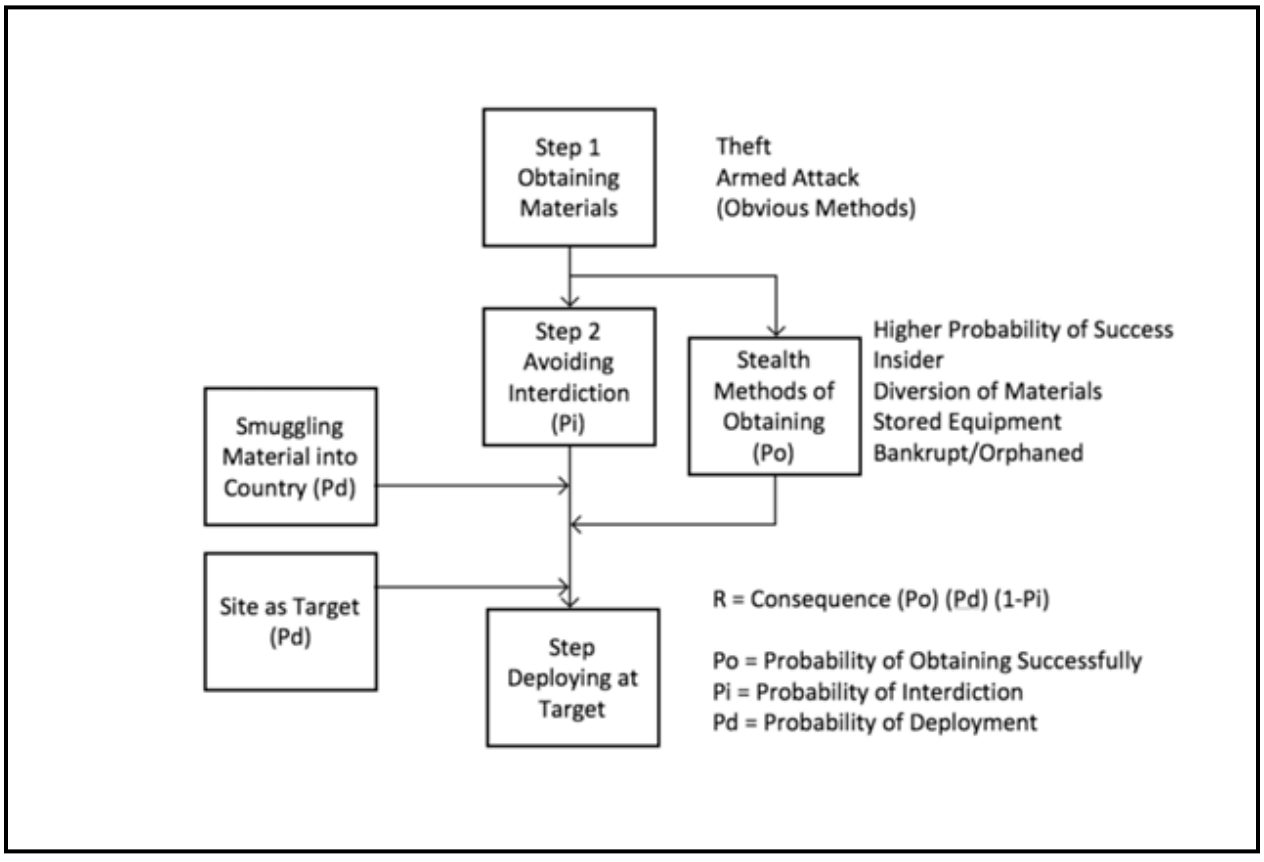

Figure 2. Risk Assessment Schematic for MIAN Materials

The terrorist must first obtain the radioactive material (Step 1). This can be done by forcible means or clandestine methods. If a forcible attack is used, it is highly likely that law enforcement will be aware of the fact that the terrorist has obtained this material and will immediately attempt to interdict the terrorist before the material can be deployed. Clandestine removal of radioactive materials from a storage or use site will almost certainly preclude or delay active interdiction for a considerable time, providing the terrorist a grater probability of successfully deploying the material at an attack site. If material is smuggled into the country undetected or obtained by other undetected means, the probability of successfully deploying the material is greatly increased.

Calculating the overall risk for a particular site that uses or stores radioactive materials is either extremely difficult or next to impossible. There are virtually limitless possibilities that could be postulated given the large number of sites where materials are stored and the number of possible targets. The number of possible scenarios is essentially unlimited and the authors could not determine a method by which they could be approximated or even how an upper bound could be placed on the problem. To further complicate the problem, there are at least three separate security organizations directly involved. These include the personnel at the sites that use or store radioactive materials, law enforcement responsible for interdiction, and security personnel at target locations. (Additional organizations such as Homeland Security, the intelligence community, Interpol, the FBI and Customs and Immigration, to name only a few, also contribute to securing radioactive materials.) The overall risk must include assessment of all security personnel and how they interact. The RAMCAP methodology was developed and applied to sites that are secured by a single organization, considering, of course, first responders as backup. However, in spite of these challenges, risk assessment using RAMCAP still provided very useful results.

Appendix 2 contains a more detailed discussion of risk and how the RAMCAP methodology was modified to address these additional considerations. Because of the aforementioned difficulties, it was concluded that the most effective means to reduce risk is to concentrate on increasing security at the licensee's sites. If access to radioactive materials from domestic sources can be denied, the overall terrorist risk will be greatly reduced.

Section 4. Conclusions and Recommendations

Because of the complex interaction between several security organizations as well as the virtually unlimited number of possible scenarios for obtaining and deploying radioactive materials for malicious attacks, it is concluded that a quantitative method of estimating the risk at any particular use or storage site is not feasible. However, our work clearly shows that the most effective way of reducing risk from domestic sources of radioactive material is to increase security at all sites. If dangerous materials from sites inside the United States can be denied the terrorist, the probability of an attack is greatly reduced. A voluntary program that will increase security is outlined herein and tools for its implementation are provided.

It is also shown that the probability of interdiction by law enforcement increases as the time of reporting missing material is reduced. If materials are obtained by force or through theft, the event must be reported immediately. Periodic accounting of material should be performed. Reducing the time between inventories will reduce risk. The more dangerous the material, and the greater the amount stored, the more critical the time to report losses. Traditionally, inventory intervals have been quarterly, six months, or annually, depending on types of use. Perhaps inventory time intervals should be based on the dangerous nature of the source. Inventories must be physical – not simply paper accounting.

Orphaning of radioactive materials should be prevented. Bankruptcies, for example, can lead to situations in which there is no responsible individual to account for radioactive materials. College instructors moving from one institute to another often fail to secure quantities of material brought from a previous position. Obsolete machines may be stored rather than being properly disposed. A common experience has been for gauges containing radioactive material to be stored in back lots at plants – forgotten for years. Then, they become "re-discovered" when accidently sent as scrap steel to a steel recycling plant.

The above suggestions for reducing risk are examples of ways to reduce the *vulnerability* of storage and use facilities. Risk can also be reduced by *mitigating the consequences* of an attack. An obvious approach to reducing the consequences of a nuclear material event is to prepare beforehand, coordinate first responders, and plan for remediation at the earliest possible time, thereby returning the attack site to normal as soon as practicable.

However, studies[10] indicate that there is a strong psychological component that exacerbates the consequences of an attack when radioactive materials are involved. Every effort should be made to educate the public regarding the actual dangers. Further, experience indicates that government officials tend to overreact to such events by increasing security at all sites and imposing new and perhaps draconian requirements. This can only be avoided by insuring that both the public and our

[10] Assessment of the Regional Economic Impacts of Catastrophic Events: CGE Analysis of Resource Loss and Behavioral Effects of and RDD Attack Scenario, J. A. Giesecke et al, Risk Analysis, Vol. 32, No. 4, 2012

public officials understand the physics of this problem and are courageous enough to act in accordance with the actual risk.

The authors would like to strongly encourage those who are entrusted with the security of radioactive materials to utilize the materials provided in this package. We are convinced that an attack will eventually happen unless everyone involved in making these materials secure is diligent and proactive. The evidence presented herein is too compelling to ignore. Now is the time to act so that we don't use hindsight as a lens for revealing what we knew beforehand.

Appendix 1. MIAN Security Status Evaluator Examples

In addition to the trial use and feedback comment by custodians of MIAN materials, the Alfred P. Sloan Foundation team reviewed the MIAN Security Status Evaluator critically through application to four examples that varied widely in terms of the potential consequences from terrorist acquisition and deployment. The four examples included:

- An external beam radiotherapy device, such as a Gamma Knife®, with 2,885 curies of Co-60[11] source material, with the source sufficiently large to be a Category 1[12] source;
- A blood irradiation system with 1,700 curies of Cs-137 source material, with a source strength such that it falls just below Category 1 and at the high end of a Category 2 source;
- A well logging device with 20 curies of Am-241 source material, with a source strength at the low end of Category 2 sources; and
- An industrial gauge with only 5 curies of Cs-137 source material that lies clearly within the range of a Category 3 source.

These four examples offer the opportunity to test the MIAN Security Status Evaluator in terms of an initial security program assessment, based on current standard security program elements, as well as a follow-up security program assessment, based on judicious selection of enhanced security program elements appropriate for the perceived consequence risks associated with the respective categories. It should be pointed out that an effort was made to implement, to some extent, increased controls as required by the U. S. Nuclear Regulatory Commission (USNRC) for the Category 1 example and the high Category 2 example, but not for the other two examples. Those increased controls require: (1) limiting access to only approved individuals through the use of background checks that include fingerprinting; (2) enhancing physical barriers and intrusion detection systems; (3) coordinating with local law enforcement to respond to an actual or attempted theft, sabotage, or diversion of radiological material; (4) promptly notifying authorities of incidents; and (5) monitoring shipments of radiological material during transit. The only one of these increased controls not implemented was the second one – enhanced physical barriers and intrusion detection systems – since specificity is not provided in the requirement.

In each of the four examples, the same starting procedure for the security assessment was used, with the evaluator quantifying the "existing" security program quantitative ranking by identifying security program elements that would nominally be expected to be deployed by the custodian, such as a locked room and periodic inventory, but with no particular security enhancements. For such "existing" security program elements, the evaluator expected that the initial security program quantitative ranking would be between 55 and 65, and these expectations were confirmed. The Category 1 radiotherapy device was scored at 64, and the "needed" score was set at 78, which

[11] The source strength was taken from a misplaced radiation therapy machine incident in Juarez, Mexico, in December 1983.

[12] Based upon the five categories defined in INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

implied a substantial enhancement in security program elements. The high Category 2 blood irradiator was also treated as an increased controls facility, and was initially scored as a 73, with a "needed" score of 73. Therefore, the existing security program needed no additional enhancements. The low Category 2 well logging device was initially scored 78 out of a "needed" 73, while the Category 3 industrial gauge received an initial score of 29 out of a "needed" 66. These initial scores implied that the security program for the industrial gauge required fairly substantial enhancements, while the security program for the well logging device needed no enhancement.

The security assessments of the two medical devices and the one well-logging device demonstrate that their security is adequate when compared to IAEA minimum recommendations, while the industrial gauge appears to need considerable security enhancement. Following these initial security assessments, and recognizing that the security level goals are minimum acceptable security levels, the evaluator selected several different approaches to enhance the security programs for the example facilities. **First**, for the Category 1 Co-60 source needing significant security program upgrades, the guidance recommended by the International Atomic Energy Agency (IAEA)[13], for Security Level A (***prevention*** of unauthorized removal of a source) was used – which was interpreted to mean the implementation of the security program enhancements of the National Nuclear Security Administration's (NNSA's) Domestic Material Protection program. These security program upgrades involve such elements as remote monitoring systems, biometric access controls, security cameras, and other features. When a sampling of these enhanced elements was recognized in the follow-up use of the MIAN Security Status Evaluator, the quantitative score was easily raised to 103, well above the "needed" score of 78.

Second, for the two Category 2 sources, relatively minor adjustments to the security program could be tried, since the minimum capability to ***minimize the likelihood*** of unauthorized removal of a source (called Security Level B) has already been demonstrated.

Third, for the Category 3 industrial gauge source, which is deemed to be subject to the security goal of ***reducing the likelihood*** of unauthorized removal of a source (called Security Level C), significant enhancement would be required in order to bring the MIAN Security Status Evaluator follow-up score up to the "needed" level of 66. While specific security program enhancements are not proposed here, the MIAN Security Status Evaluator offers a large number of alternatives that can be implemented in order to improve the score.

These four example applications lead us to offer several observations and a few recommendations that need to be further confirmed through trial use of the MIAN Security Status Evaluator by experienced custodians of MIAN materials.

[13] IAEA Nuclear Security Series No. 11, Security of Radioactive Sources: Implementing Guide, International Atomic Energy Agency, Vienna, Austria, 2009, p. 15

- A major observation is that the MIAN Security Status Evaluator provides an extremely useful, easily-used tool for assessing the current security program at a MIAN facility in a quantitative sense, and permits the user to quickly evaluate the quantitative value of a variety of security program enhancements; the Evaluator would be even more useful if the individual quantitative values for the various security program elements were confirmed through expert usage and through confirmation of their risk reduction effectiveness.
- A second major observation is that the NNSA Domestic Material Protection program security enhancements can be shown to significantly improve the quantitative value of a security program, readily improving the MIAN Security Status Evaluator score for Category 1 and high-end Category 2 sources from the mid-50s to over 100, to a level that seems appropriate for sources subject to increased controls; this observation leads to a recommendation that the "needed" security program score for a Category 1 source or a high-end Category 2 source should be raised from the current value of 78 to a number above 90 and possibly to 100; another recommendation would be to consider the possibility of dividing the range of Category 2 sources into a Category 2a and a Category 2b, with the intent that both Category 1 and Category 2a sources would be subject to the IAEA Security Level A, which has the goal of prevention of unauthorized removal of a source, which seems to be consistent with the intent of the security program upgrades sponsored by the NNSA Domestic Material Protection program[14].
- A third observation is that, provided the "needed" score for Category 3 sources of 66 can be justified through trial use by expert custodians, current security program elements seem to be well positioned to satisfy the IAEA Security Level C goal of reducing the likelihood of unauthorized removal of a source; in addition, very few improvements seem to be needed to enable current security programs for low-end Category 2 sources to achieve a "needed" score of 73.

[14] Both the NNSA Domestic Material Protection program and the IAEA Security Level A have the goal of prevention of unauthorized removal of a MIAN source, with enhancements of security program elements that immediately detect unauthorized access, introduce delay devices into the security system through multiple barriers, and provide immediate notification of unauthorized access.

Appendix 2. Risk Assessment Using RAMCAP Plus

The use of MIAN materials by terrorists can result in extremely high monetary consequences and, at a lower probability, large numbers of deaths and serious injuries. The RAMCAP methodology was originally developed for use by the Department of Homeland Security and other organizations as a means of estimating the risk of a terrorist attack at a particular "target[15]". For example, terrorist acts include the bombing of the Murrah Federal Office building in Oklahoma City by Timothy McVeigh, a "homegrown" terrorist. The motive was not to destroy the Federal Government agencies that were housed in the building, but to make a political statement and possibly to incite others to perpetrate similar attacks, thereby crippling the governance of the United States. The September 11, 2001, attacks are an example of terrorism by foreign terrorists. There are actually hundreds of terrorist attacks each year throughout the world. Most take place in foreign countries such as Afghanistan, Iraq, Israel, and many African countries. However, the United States and our allies are not immune to such attacks, as evidenced by the recent events in France and the London Underground bombings.

Clearly, the 9-11 attacks marked a step change in awareness and adversely affected the lives of United States residents. This event prompted the establishment of the United States Department of Homeland Security and marked the beginning of a new era in security regulations and requirements. Air travel has been impacted significantly and apparently permanently. The Transportation Safety Administration (TSA) has established security checkpoints at all airports and travel times and convenience have been adversely affected. The use and storage of MIAN materials has also been affected by new regulations. Increased controls on these materials has imposed additional requirements that are time consuming and costly.

As the "war on al Qaeda" continues to make progress in destroying the leadership of this well-known terrorist organization, and the wars in Afghanistan and Iraq continue to wind down, these events continue to produce an even greater asymmetry between the capabilities of ourselves and our terrorist adversaries. However, even though we have crippled our enemies, history teaches us that they will continue to stubbornly and relentlessly attack our way of life. As we eliminate their conventional tools of terrorism, the use of MIAN materials may become an increasingly attractive weapon. In fact, MIAN materials could become the weapon of choice for inflicting both economic and personal damage to the United States. The fear of radioactivity is recognized by experts in risk tolerance as one of, and possibly the greatest, of all tools that can be weaponized and used by terrorists. Even the threat of biological attacks appears to hold less dread than the threat of malicious radioactive material use. Even though nuclear power in the United States has an outstanding safety record and has resulted in no fatalities and few acute injuries it is constantly scrutinized and vilified

[15] A target is defined as a site or infrastructure component that could be attacked by a terrorist organization for the purpose of causing serious consequences and thus achieving a political or religious goal. The purpose of the terrorist is typically not directed to achieving a tactical advantage but to inflict fear and disrupt the normal lives of their adversaries.

by detractors and feared by the general public. No other commercial power generation sector can match the safety record of nuclear power[16], yet it is by far the most feared. The use of radioactive material may prove to be a highly effective weapon of terror, especially in the hands of "home grown" terrorists such as Major Nidal Hasan who killed 13 and wounded 32 people at Fort Hood in November 2009. Major Hasan and others like him could easily gain access to MIAN materials and either use them or provide them to a terrorist.

As discussed briefly above, the RAMCAP Plus methodology was developed as a means of identifying targets that would be most attractive to a terrorist, i.e., those targets of highest risk. RAMCAP attempts to provide a quantative means of ranking targets so that the limited funds available to protect infrastructure can best be utilized. RAMCAP Plus includes risk due to both terrorism and natural hazards such as earthquake, tornado, hurricane, etc. The methodology seeks to estimate the risk of each component of threat so that the relative risk of terrorism can be compared with the "ambient" risk that is constantly present. This allows the owner, as well as regulatory authorities, to determine if terrorism risk is significant compared to ongoing, and tolerated, risks. By quantifying risk in this fashion, rational decisions can be made regarding whether additional security measures should be taken and how much additional funding, if any, should be allotted to "buy down" terrorist risk. Thus, the role of RAMCAP Plus is to provide an assessment tool that will allow the user to make the "right" decision regarding whether to spend additional funds to further reduce risk. The assessment tool, combined with analyses of proposed increased security measures, may show that additional spending does not significantly reduce the overall risk to a particular infrastructure component.

Before discussing how to apply RAMCAP methodology to MIAN security, it is instructive to review the basic RAMCAP methodology[17]. RAMCAP risk assessment is based on a simple equation:

Risk = (Threat) x (Vulnerability) x (Consequence) or R = T * V * C (1)

Where:

Risk = The potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences. When the probability and consequences are expressed as numerical point estimates, the expected risk is computed as the product of those values.

[16] More deaths and acute injuries are sustained in the coal and oil industry, for example. Coal mining has a poor safety record for mining and the oil refining industry has sustained numerous fatalities, for example. Additionally, burning coal and oil causes environmental concerns and contributes to respiratory problems as well as proliferating known carcinogenic materials.

[17] For additional information, see "Risk Analysis and Management for Critical Asset Protection (RAMCAP *Plus*)", Jerry P. Brashear and J. W. Jones, Wiley Handbook of the Science and Technology of Homeland Security, John Wiley & Sons, New York. Voeller, John (ed.),

Threat (T) = The likelihood that an adverse event will occur within a specified period, usually one year. The event could be any with the potential to cause the loss of or damage to an asset or population.

Vulnerability (V) = The probability that, given an adverse event, the estimated consequences will ensue.

Consequence (C) = The outcomes of an event occurrence, including immediate, short and long-term, direct and indirect losses and effects. Loss may include human fatalities and injuries, economic damages and environmental impacts, which can generally be estimated in quantitative terms, and less tangible, non-quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness or military readiness, etc. RAMCAP Plus estimates economic losses to the infrastructure owner and to the community served, respectively, and can readily be extended to state, multi-state regions or the nation.

This methodology allows the user to calculate a single number for risk based on cost, fatalities, acute injuries', or any other meaningful metric as long as it can be resolved into a consequence of the terrorist event. However, as for most complex problems, the devil is in the details. Each of the three variables in the equation, threat, vulnerability, and consequences, are difficult to quantify. While it is difficult to obtain a single, exact, value for any of the variables, it is possible to determine a range of values that has a high probability of containing the exact value. Instead of using a point value for each of the variables, a range of values can be used and a distribution curve can be defined. In that case, the simple equation for risk now becomes a more complex integration over the range of each variable. While this approach is arguably more ascetically pleasing, it is difficult to use at a security assessment level. Thus, a single point estimate for each variable is used to calculate risk.

For the purposes of determining the effectiveness of security measures, it is prudent to overestimate rather than underestimate the actual risk. The RAMCAP risk calculation should always overestimate the actual risk, but not to the extent that the results are not so conservative that they are unreliable and thus useless to decision makers. The approach taken by the RAMCAP developers is to assume the most conservative *reasonable* point value for each variable. For example, the consequences of an attack on a large city should assume that the terrorist will time their attack such that the wind is blowing toward the most populated area. This is a reasonable but conservative assumption. It may also be prudent to assume that the attack will happen on a holiday or event that will result is a large gathering. However, it may not be reasonable to assume a favorable wind, a large gathering, and a rainstorm that will precipitate out the material over the crowd. Thus, the user must use common sense in estimating the variables. The resulting risk estimate should, in general, be conservative in almost all cases. It is not practical nor useful to assume the "perfect storm" of events. Using these simple principles, risks can be estimated with sufficient certainty that they can be compared and ranked.

This simplified approach was used to provide detailed guidelines for risk assessment in a number of industries including nuclear power plants, spent nuclear fuel facilities, chemical plants, petroleum refineries, liquefied natural gas storage facilities, water and waste water treatment plants. Clearly, the RAMCAP methodology does not provide an exact answer and is based on a simplified approach. However, given the millions of potential targets in the United States alone, a more complex methodology would be impossible to apply in a reasonable time and budget.

Applying the RAMCAP Plus Process

A schematic of the RAMCAP seven step process was shown in Figure 1.

Each step is described below:

Step 1. Asset Characterization analyzes the organization's mission and operational requirements to determine which assets, if damaged or destroyed, would diminish the facility's ability to meet its mission. Critical assets are identified and a preliminary estimate is made of the gross potential consequences from various threats or hazards, in ordinal terms (e.g., "very small" to "very large" in five to seven intervals). The assets evaluated include those that are directly engaged in performing the most important missions or functions, the assets that support these and the infrastructures on which they depend. These assets may include physical plant, cyber systems, knowledge base, human resources, customers, or critical off-site suppliers.

Step 2. Threat Characterization is the identification and description of reference threat scenarios in enough detail to estimate vulnerability and consequences. As summarized in Table 1, there are a wide variety of threat scenarios. Each is specified in more detail in actual application.

One key to comparability of results is the use of a common set of reference threats. These threat scenarios are not "design basis threats," which imply that the organization must take steps to withstand the threat to continue operations. Rather, these are "benchmark" or "reference" threats that span the survivable range of possible threats across all critical infrastructure sectors. Five distinct types of reference threats have been defined:

1. Terrorism – attacks by enemies, as suggested by the U.S. Department of Homeland Security (DHS) based on analyses by DHS and others as an understanding of the means, methods, motivations and capacities of terrorists.

2. Natural hazards – currently including hurricanes, floods, tornadoes and earthquakes, based on the physical location of the facility and federal data.

3. Product or waste stream contamination – suggested by the water sector and also applicable to food and pharmaceuticals, to address concerns of intentional or accidental contamination.

4. Supply chain hazards – immediate dependencies, mostly supply chain issues such as suppliers, labor, customers, etc., included as an initial step toward dealing with dependencies on other organizations for critical elements of the organization's mission.

5. Proximity hazards – potential to become collateral damage from events at nearby sites.

Table A1. **Summary of RAMCAP *Plus* Reference Threat Scenarios**

Attack Type	**Tactic/Attack Description**			
Marine	**M1** Small boat	**M2** Fast Boat	**M3** Barge	**M4** Deep draft shipping
Aircraft	**A1** Helicopter	**A2** Small Plane (Cessna)	**A3** Medium, Regional Jet	**A4** Large Plane Long-Flight Jet
Land-based Vehicle	**V1** Car	**V2** Van	**V3** Mid-size Truck	**V4** Large Truck (18 wheeler)
Assault Team	**AT1** 1 Assailant	**AT2** 2-4 Assailants	**AT3** 5-8 Assailants	**AT4** 9-16 Assailants
Sabotage	**S(PI)** Physical-Insider	**S(PU)** Physical-Outsider	**S(CI)** Cyber-Insider	**S(CU)** Cyber- Outsider
Theft or Diversion	**T(PI)** Physical-Insider	**T(PU)** Physical- Outsider	**T(CI)** Cyber-Insider	**T(CU)** Cyber- Outsider
Product Contamination	**C(C)** Chemical	**C(R)** Radionuclide	**C(B)** Biotoxin	**C(P)** Pathogenic
	C(W) – Weaponization of waste disposal system			

Attack Type	Tactic/Attack Description			
Natural Hazards	**N(H)** Hurricanes	**N(E)** Earthquakes	**N(T)** Tornadoes	**N(F)** Floods
Dependency & Proximity Hazards	**D(U)** Loss of Utilities	**D(S)** Loss of Suppliers	**D(S)** Loss of Employees	**DI** Loss of Customers
	D(T) Loss of Transportation		**D(P)** Proximity to other targets	

Step 3. Consequence Analysis is the identification and estimation of the *worst reasonable consequences* generated by each specific asset/threat combination. This step examines facility design, layout and operation in order to estimate fatalities, serious injuries and economic impacts.

RAMCAP Plus defines "economic impacts" for risk management at two levels: (1) the financial consequences to the organization; and (2) the economic consequences to the regional metropolitan community the organization serves. Economic consequences for communities larger than the metropolitan area, e.g., the state, multi-state region or the nation, may also be estimated, using the same methods, as needed by decision-makers. For many critical infrastructures and facilities, interdependencies make the metropolitan region most relevant to decision-makers.

Financial consequences to the organization include all necessary costs to repair or replace damaged buildings and equipment, abandonment and decommissioning costs, site and environmental clean-up, net revenue losses (including fines and penalties for failing to meet contractual production levels but excluding avoided variable costs)) while service is reduced, direct liabilities for casualties on and off the property and environmental damages. These costs are reduced by applicable insurance or restoration grants and must be corrected to account for tax effects for tax-paying organizations.

Step 4. Vulnerability Analysis estimates the conditional likelihood that the estimated consequences will occur, *given* the occurrence of the specific threat or hazard. Vulnerability analysis involves an examination of existing security capabilities and structural components, as well as countermeasures and their effectiveness.

A variety of rigorous tools can be used to estimate vulnerability, such as those described in Table A2. Direct elicitation often seems to be easier and less time-consuming, but the time to reason through each threat/asset pair can lead to long discussions and it is difficult to maintain logical consistency across a number of such judgments. In some RAMCAP sector-specific applications, direct elicitation often seems to be easier and less time-consuming, but the time to reason through each threat/asset pair can lead to long discussions and it is difficult to maintain logical consistency

across a number of such judgments. Some RAMCAP sector-specific guidance documents provide pre-specified structure of vulnerability logic, event or decision trees for users to populate with estimates of the required elements to enhance comparability and reliability.

Table A2. **Frequently Used Vulnerability Tools**

Method	**Description**
Direct Expert Elicitation	Members of the evaluation team discuss the likelihood of success and their reasoning for their estimates; in its more formal form, a statistical "Delphi" processor Analytical Hierarchy Process can be used to establish a consensus
Vulnerability Logic Diagrams (VLDs)	Plot of the flow of events from the time an adversary approaches the facility to the terminal event in which the attack is foiled or succeeds, considering obstacles and countermeasures that must be surmounted, with each terminal event associated with a specific likelihood estimate. This is frequently complemented with an estimate of the reaction time of a counterforce once the attack has been detected
Event Trees (also called "failure trees")	Tree with branches representing the sequence of events between the initiation of the attack and the terminal events The evaluation team estimates the probability of each outcome. Multiplying the probabilities along each branch, from the initiating event to each terminal event, calculates the probability of each unique branch, while all branches together sum to 1.0. The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate.
Decision Trees	Very similar to event trees except that the decisions by the adversary are modeled at each node in the unfolding tree to capture the adaptive behavior of the adversary; a sophisticated variant is to conceive the tree as a two-player game
Hybrids of These	Often used by the more sophisticated assessment teams

Step 5. Threat Assessment estimates the probability that a particular threat – terrorist, natural, contamination, dependency, or proximity – will occur in a given timeframe (usually one year). The approach differs depending on the type of hazard, as characterized in Table 3.

Terrorism likelihood (and its contribution to contamination, proximity and even dependency hazards) is the most difficult to estimate and is still being refined. In its most advanced formulation, it recognizes that terrorists are cognizant, near-optimizing adversaries in a contest perhaps best modeled by game theory. Because of RAMCAP's specification to keep the process simple and brief, however, simpler techniques of approximation based on observable or previously estimated factors are used. RAND Corporation has contributed relative likelihood of attack based by metropolitan region and asset type. The previously estimated conditional risk (consequences times vulnerability) aptly characterizes the expected value to the terrorist of the asset/threat pair, while the asset's size and prominence relative to other assets of the same type in the region can indicate attractiveness. The adversary might also consider the likelihood of pre-attack detection and the "cost" in resources.

***Table 3*. Estimation of Hazard Likelihood**

Hazard Type	Likelihood/Probability Estimation
Terrorist attack	Based on the terrorists' objectives and capabilities, generally (provided by intelligence and law enforcement agencies), and the attractiveness of the facility relative to alternative targets, the asset's expected value (vulnerability x consequences), and the cost/effectiveness of the attack.
Natural hazards	Based on the historical Federal frequency data for various levels of severity at the specific location of the asset. Can be adjusted if there is reason to believe that the future frequency or severity will differ from the past.
Dependency hazard	Based on local historical records for the frequency, severity and duration of service denials as a baseline estimate of "business as usual," incrementally increased if they may be higher due to terrorist activity or natural events on required supply chain elements. Confidential conversations with local utilities and major suppliers can inform these estimates.
Product contamination	Treated the same as terrorism and dependency likelihood, except additional consideration is given to accidental contamination of inputs and the vulnerability of critical processes to accidents.
Proximity hazard	Based on asset's location relative to other assets that may incur adverse events leading to collateral damage, using the same logic in estimating terrorist and natural hazard threats.

Comparison of terrorism risk with natural hazard risk uses a natural hazard risk that is accepted by the organization to deduce a terrorism threat likelihood equating the two risks. The analyst and decision-maker then judge whether the deduced likelihood is reasonable or not. If the likelihood in the deduced risk is equal to or less than the judged reasonable level, then the terrorism risk is as tolerable as the natural hazard risk and the likelihood is moot. If, on the other hand, the likelihood in the deduced risk is greater than the accepted level, the judgment of the reasonable level sets a minimum and the asset/threat pair's risk justifies taking the next steps.

Step 6. Risk Assessment creates the foundation for prioritizing and selecting among risk-reduction and resilience enhancement. The risk assessment step is a systematic and comprehensive evaluation of the previously developed estimates. The risk for each threat for each asset is calculated from the risk relationship expressed in Equation 1, above.

Step 7. *Risk Management* is the step that actually reduces risk. Having determined the risk of each important asset/threat pair, this step defines new security countermeasures and consequence mitigation options and evaluates them to achieve an acceptable level of risk at an acceptable cost.

Risk Assessment for MIAN Materials

The use of RAMCAP methodology for the MIAN project requires some modification of the basic seven-step process for many scenario's of interest. As previously discussed, RAMCAP was originally developed in response to the need for critical infrastructure protection. Initial applications of RAMCAP were designed for assessing the risk due to terrorist attack on infrastructure "targets," i.e., infrastructure such as nuclear power plants, chemical plants, dams, navigational locks, water treatment plants, and other fixed "assets." The asset, i.e. the plant or infrastructure component, was the target of the attack. In some cases, for example nuclear plants, chemical plants, etc., a successful attack on the plant could result in damage (consequences) to surrounding population and other infrastructure components. However, the destruction associated with damage outside the fence was included as be part of the consequences of an attack on the primary target and which occurred simultaneously or as a continuation of the initiating event. Cascading effects, such as loss of revenue, deprivation of plant output, loss of use of the affected adjacent real estate, etc. were included in the overall assessment; however, they emanated from the initiating event.

Another significant difference between the MIAN procedure and RAMCAP Plus is that the probability of an event occurring in a given year is assumed to be unity (1.0). The primary purpose of this current project is to evaluate the *relative* risk resulting from the acquisition and deployment of radioactive materials. Presumably, a terrorist would attempt to maximize the consequences of his/her actions and decide to perpetrate an event that would pose the highest risk to the adversary. Rather than attempt to assign a value for likelihood to each event considered for analysis, it is more convenient to assume all events have the same likelihood of being attempted and calculate the conditional risk for comparison. Thus, MIAN risk assessments are "normalized" by initially

assuming equal likelihood. Once all events of interest are evaluated (assuming that is actually possible given the almost infinite number of permutations), then a "true" risk can be estimated by multiplying the conditional risk by the probability of occurrence. The "true" risk can then be compared to other risk assessment results.

The MIAN assessment methodology requires additional steps to determine both the consequence and the probability of success for a terrorist attack. (Operational accidental incidents and natural hazards will be discussed later.) In many of the terrorist scenarios that are considered, the location, or facility that contains the radioactive material is not the "target" of the attack. For example, radioactive material used for well logging or radiography may be located in a relatively rural area, remote from high population areas or extensive infrastructure. The terrorist "attacks" the facility only to obtain the radioactive material with intent to utilize it at another location that will produce higher monetary consequences, human fatalities, serious injuries, or psychological effects. Thus, the initial "attack" is only a first step in the overall scenario. It is necessary to capture the overall risk for a scenario, thus, the additional steps must be included in the risk assessment. This is accomplished by including additional terms in the basic risk equation. These include the ***probability of interdiction*** and the ***probability of success of deploying*** the material to achieve the assumed worst-case consequences.

Consider the term for interdiction. For the purposes of this analysis, it is assumed that the probability of obtaining the material at the initial attack location includes the potential for interdiction at the initial site of the attack. Thus, for example, if the terrorist attempts to steal material from a laboratory and mounts an armed attack using firearms, it is assumed that the probability of success of obtaining (P_o) includes the probability of finding the material, defeating all security measures including armed guards and gaining egress from the building with possession of the material. Once out of the building, the process of formal interdiction assessment begins.

Interdiction probability is defined as the probability of stopping the attacker(s) before they can reach the site of the planned attack with the material and the opportunity to deploy. There is a remaining question of whether the attackers are captured, the material recovered, or both. However, for the purpose of calculating the probability of interdiction for a particular scenario and estimating the overall risk for that scenario, it is sufficient to determine only the probability of stopping the perpetrators from reaching the attack site with the material and the opportunity for deployment. Thus, the "stopwatch" on the interdiction continuum begins when the attackers leave the site after successfully obtaining the material and stops when they reach the site "with opportunity to deploy". Further, a "dirty bomb" or RDD, may not be the intended deployment. The terrorists may decide to hide the material, use it to contaminate food/water supplies, or deploy it in public places for exposing members of the public to dangerous, perhaps fatal, levels of radiation.

The assessment of accidents and incidents caused by natural events, such as hurricane, tornado, flood, fire and earthquake, will not include a term associated with interdiction. Further, in these

cases, the storage site of the material becomes the “target” of the event. Since radioactive materials are almost always contained in protective containers that are very robust, there is only a small probability of causing high consequences that are of the same order of magnitude as those caused in terrorist events. Another ameliorating effect inherent in natural and accidental events is that the form of the material is normally unaltered by the event; thus, the material remains intact, is easy to detect, and is readily removed from the site.

Since the storage or use site is the “target” of the accidental/natural hazard event, the consequences are normally expected to be quite low. Further, the risk tolerance of the public to such events, and even release of small quantities of radioactive materials, is expected to be much higher than if the event were caused by a terrorist, especially when the threat of additional attacks cannot be ruled out. The psychological effect of a premeditated release of radioactive material cannot be overstated. Since there have been few major releases of such material, the only examples that might be used to gauge public reaction are the Chernobyl and Three Mile Island events. Both events had a profound effect on the acceptance of nuclear power. Chernobyl, of course, was far worse in real or physical consequences. However, the Three Mile Island event arguably changed the course of the nuclear power industry in this country.

The 2011 earthquake off the Pacific coast of Japan, also known as the 2011 Tohoku earthquake and the Great East Japan Earthquake, occurred on Friday, 11 March 2011. It was the most powerful known earthquake ever to have hit Japan, and one of the five most powerful earthquakes in the world since modern record-keeping began in 1900. The earthquake triggered powerful tsunami waves that reached heights of up to 40.5 metres (133 ft) in Miyako in Tōhoku's Iwate Prefecture, and which, in the Sendai area, travelled up to 10 km (6 mi) inland.

The tsunami caused a number of nuclear accidents, primarily the ongoing level 7 meltdowns at three reactors in the Fukushima Daiichi Nuclear Power Plant complex, and the associated evacuation zones affecting hundreds of thousands of residents. Many electrical generators were taken down, and at least three nuclear reactors suffered explosions due to hydrogen gas that had built up within their containment buildings after cooling system failure. Residents within a 20 km (12 mi) radius of the Fukushima Daiichi Nuclear Power Plant and a 10 km (6.2 mi) radius of the Fukushima Daini Nuclear Power Plant were evacuated. In addition, the U.S. recommended that its citizens evacuate up to 80 km (50 mi) of the plant.

On 12 March 2012, the Japanese National Police Agency report confirmed 15,854 deaths, 26,992 injured, and 3,155 people missing across twenty prefectures, as well as 129,225 buildings totally collapsed, with a further 254,204 buildings 'half collapsed', and another 691,766 buildings partially damaged. All deaths and serious injuries were caused by the earthquake and resulting tsunami. The earthquake and tsunami also caused extensive and severe structural damage in northeastern Japan, including heavy damage to roads and railways as well as fires in many areas, and a dam collapse.

To date, no fatalities have been reported as a result of radioactivity released from the plant and acute injuries are few, especially in light of the devastating toll exacted by natural hazards. However, as a result of the events, it appears that most, if not all, nuclear power plants in Japan will be closed. The fear of radiation will result in billions of dollars in consequences to the power generation industry in Japan, a cost that will eventually be paid by the public in higher electricity rates.

Given the relatively small amount of material actually released, it is conceivable that a terrorist attack that utilized radioactive material could have an effect at least as great as Three Mile Island and perhaps even greater. It is difficult to predict public reaction to such an event. It would be interesting to calculate the cost of the September 11, 2001, event considering the additional security worldwide, the loss of time associated with security checks at the airport and other cascading costs including airline losses, bankruptcies, and other services. Would an attack on public transportation such as subways, for example, result in passenger security screening?

When considering accidents or natural hazards, the site where the material is stored is the focus of the risk assessment. The standard RAMCAP Plus methodology is employed. Natural hazard assessment is performed in exactly the same way as the methodology is used for all other target or asset based assessments. The asset considered is the facility at which the material resides and the attack scenarios are the various natural or accidental events that can occur at that location. The radioactive material is considered to be the focus of the event. Consequences of these events primarily involve release of material and/or exposure to personnel. Clean-up costs and loss of use of the facility are included in the consequences. Secondary or cascading effects are considered. However, natural or accidental hazard events are not likely to result in or create undue panic or concern outside of the local area. Further, the public risk tolerance for natural or accidental events is far greater than for than terrorist events[18].

A terrorist event has the potential to create panic and disrupt the conduct of business as usual, thus resulting in far higher consequences than a naturally-occurring or accidental event. A terrorist event involving MIAN materials typically requires several steps to achieve. The terrorist must obtain an appropriate form of material, avoid interdiction, and deploy the material at a different site in order to achieve a high consequence event. A major difference between a natural/accidental event and a terrorist event is that the site at which the radioactive material resides is seldom the target of a terrorist attack.

Thus, it is necessary to consider terrorist risk assessment in three distinct steps. Figure 2 provides a schematic of the MIAN risk assessment procedure.

[18] The fact that 40, 000 traffic deaths occur annually bears witness to the high tolerance for some forms of risk.

Step 1 consists of acquisition of the material from a source. Radioactive materials are available from thousands of possible sites throughout the United States, as well as from sites in foreign countries, especially those that may support terrorist activities. Table 2 in Appendix 1 provides a list of materials that are considered to rise to the level of concern and a discussion of how these materials can be obtained. Historically, it has been assumed that some materials were "self protected," since the material itself would cause significant injuries or death if handled without proper shielding. However, it has been demonstrated numerous times recently that religious zealots are willing to risk bodily injury or death to carry out their terrorist missions. Thus, it must be assumed that danger to the perpetrator will not deter a terrorist organization.

If material is obtained without the knowledge of law enforcement, then the terrorist has a much higher probability of successfully deploying the material and achieving the maximum possible consequence. If theft or unauthorized removal of radioactive material is discovered immediately, law enforcement agencies have a much greater probability of interdicting the terrorist. Thus, the overall probability of success for the terrorist is greatly increased by stealthy acquisition. Materials obtained from sources that are not monitored frequently, such as storage locations or university repositories for example, may be deployed before the theft is discovered. Smuggled materials likewise pose a increased threat. Another scenario that must be considered is accumulation of material from more than one source. Increased Controls are required when the amount of material exceeds the limits defined by the NRC. The same materials can be obtained from two or more sites that have much less security and combined to achieve a quantity that exceeds the IC level.

Step 2 is to avoid interdiction by authorities before the material can be deployed. When material is obtained, and the authorities are aware of the event, every effort will be made to apprehend the terrorist and recover the material. The probability of interdiction will reduce the overall probability of successful terrorist deployment. Once radioactive material is obtained and the law enforcement agencies are alerted, there is little that can be done by the general public to increase the probability of interdiction before the material is deployed. In fact, alerting the public that material is missing, and that a terrorist plot to deploy the material is suspected, may result in large economic consequences. The terrorist ends can be achieved through the use of credible threats to deploy the material and expose the public to radiation.

Step 3 is to deploy the material in a RDD in such a manner as to have the maximum reasonable consequence. Table 3 of Appendix 2 of the Phase I MIAN report[19] provides a discussion of how various isotopes can be deployed and an estimate of consequences.

Securing an amount of radioactive material that is large enough to be of concern is tantamount to obtaining a weapon for a contemplated attack. Clearly, multiple groups can be employed in such an

[19] Jones, J. William, Nickell, Robert E., and Haygood, John, Methodology for Assessing Risk from Radioactive Materials Found in Medical, Industrial, and Academic Sites, ASME Innovative Technologies Institute, LLC, Final Report to the Alfred P. Sloan Foundation, Grant number 2009-10-18

operation, one for obtaining the material, one for transporting it to the target, and another for deploying it.

Another possible scenario that must be considered is the case in which the radioactive material residence site, such as a major hospital, would be the target of the attack. Consider a site containing radioactive materials that could be weaponized by an explosion at the site. For example, assume an irradiation facility attack using a truck bomb in order to cause release of the material in the explosion or a subsequent conflagration. This attack scenario can be addressed by the existing RAMCAP Plus methodology. The facility is the asset and the attack scenarios are contained in the standard threats considered by RAMCAP Plus. Additionally, in an attack on an existing facility, the direct consequences are limited to the area near the facility (Of course there will be cascading effects because of the attack. However, it can be reasoned that cascading effects are proportional to the consequences of the initiating event and all events will have cascading effects.). The highest overall risks will result when a device is deployed in locations that have the potential for causing the greatest consequences. This is seldom, if ever, the location of sources of radioactive material sources. Additionally, RAMCAP Plus considers all hazards when calculating risk. The site containing the material should also be evaluated for natural hazards to determine the total risk.

The MIAN Risk Assessment Methodology (RAM) begins with selecting a facility for evaluation that contains radioactive material. It is assumed that the user of MIAN RAM is the owner or operator of the facility. MIAN RAM is a self-assessment tool by or for that owner/operator. Nine potential sources of material have been identified. These include:

1. Field Sources - Radiography sources, well logging sources, etc.
2. Nuclear Pharmacy - Locations that provide stores of radioactive materials for legitimate buyers
3. Medical Facility - Used for treatment or diagnosis
4. Irradiation Facility - Medical and food and packaging sources
5. Universities - Research materials, test reactors
6. Research Laboratory - Research materials
7. Stored Equipment - Any type from above that has been taken out of service
8. Bankrupt/abandoned - Sites that have no viable owner or caretaker
9. Industrial facilities - Large gauging and radiography devices

Additional information concerning risk assessment of MIAN facilities is contained in the Phase I MIAN report. For example, Table 2 of Appendix 1 provides a discussion of radioactive materials of concern, the use and location of the material, and typical scenarios that should be considered for

obtaining the material. Table 3 of Appendix 1 provides a discussion of how each material of concern could be used in a terrorist attack and the probability of success.

Detailed Assessment Methodology

As stated above, the site owner/operator will be responsible for assessing the location where radioactive materials are used and/or stored. The first step is to determine if the site contains one or more materials that are listed in the Phase I report (see Reference 5, Table 1 of Appendix 1) and in quantities that rise to the level of concern. This step is essentially a screening tool that will provide the assessor with a list of materials that should be considered for further assessment. Additional guidance is available in IAEA-EPR-D-Values, "Dangerous Quantities of Radioactive Material," published in 2006, which defines a D value as the quantity of radioactive material which is considered a dangerous source. A dangerous source is one that, if uncontrolled, could result in death or a permanent injury which decreases the affected person's quality of life.

Having compiled this list of site materials, the next step is to determine all possible methods that could be employed by a terrorist to obtain the materials. For this evaluation, it should be assumed that the terrorist is willing to risk his/her life to achieve the goals. The fact that the material could be harmful to the perpetrator should not be assumed a sufficient deterrent. The most likely methods of obtaining the material (Po) should be listed in the spreadsheet starting with the highest probability of success and considering all reasonable scenarios. For example, material could be obtained by armed attack, theft, or insider diversion. Each of the possibilities should be listed of each material on site. If it is assumed that an armed attack provides the highest probability for success, for example, this will have the highest ranking for the site for that material. However, an armed attack will undoubtedly trigger an extensive search for the terrorists and attempts to recover the material. A stealth attack, such as theft by an insider, could go unnoticed for enough time that the terrorists could transfer the material to the target and execute the attack. This scenario could therefore have the highest overall probability of success since the probability that the terrorist would be interdicted would be minimal and there would be no warning that could prevent the attack on the target. Thus, it is important to consider all modes of obtaining the material.

The above processes are repeated for all materials of interest. The site owner/operator is not responsible for determining the probability of success of interdicting the terrorist or the consequence level. This is beyond the scope of the facility assessor and will be performed by others.

The risk assessment for this scenario can be continued by law enforcement, homeland security or any other knowledgeable evaluator as follows. Having determined that a specific material or materials, as well as the quantity of material, can be obtained from the particular site being evaluated, the risk to the public can now estimated. The information obtained from the site operator is used to estimate the maximum reasonable consequence that could be caused by the deployment of the material. The remaining parameters in the risk equation are determined by the risk assessor.

References to consequences from exposure to radioactive materials normally emphasize the health effects. When considering the use of radioactive materials for terroristic activities, other considerations would be distraction and long-term denial of access or infrastructure. The terrorists' plans may include all outcomes. When outcomes are viewed separately, it becomes apparent that some radionuclides can be more damaging when used for one activity than the other.

As a general rule, the alpha-emitting radionuclides, when inhaled, ingested or otherwise incorporated into the body, will deliver higher doses than the same activity of gamma or beta emitting radionuclides. Some high-energy, beta-emitting radionuclides may also deliver very high doses when taken into the body. The reader is advised that these are general rules of thumb and the dosimetric consequence of any intake of radioactive material should be routinely reviewed and verified before taking protective measures. In general, gamma and beta emitting radionuclides pose a greater hazard as an external source of radiation. Doses do increase if a gamma-emitting radionuclide is taken into the body due to beta and other radiations which are often emitted by them. These doses rarely rise to the dose levels that equal activities of internally deposited alpha emitting radionuclides will produce.

Whether the intention of a terrorist is to cause injury to people or to deny access, the controlling parameter in recovery is dose. The magnitude of dose to an individual or group of individuals will determine the number of deaths and debilitating injuries. The levels of radioactive contamination in debris and on surfaces of still useful structures and equipment will determine the potential doses to the workers. The dose rates will limit the duration of exposure to the workers. This will increase the length of time and cost of recovery.

Numerous factors must be considered in determining the dose from a particular radionuclide.

- The quantity of radioactive material.
- The type(s) of radiation it emits.
- Whether it is inside or outside the body.
- If radioactive material is inside the body, the isotope's radiological and biological half-lives, the effective half-life, determine the length of time the radioactive material will remain inside the body and expose the individual.
- The radioactive isotope's specific activity (number of Becqerels/Curies per gram). As the specific activity of a radionuclide increases, the physical amount (grams) of that radionuclide that equals a Curie will decrease.
- If inside the body, route of entry (ingestion, inhalation, wound contamination, etc.) will also play a role in determining dose.

- The chemical form of the material and its solubility (transportability in extra-cellular fluids, plasma and blood) will determine in what organs or tissues it will tend to concentrate (pharmacokinetics).

- Mass of the organ or tissue - mass of the organ or tissue can have significant dosimetric consequence since dose is directly proportional to the concentration of the radionuclide in units of radioactivity per unit mass of the organ, i.e., the same amount of radioactivity in a small organ will produce a higher dose to that organ than to a larger one.

- Function of the organ or tissue - the function of the organ determines what compounds or elements it may use. If an organ utilizes or concentrates a specific element or compound containing that element and the material introduced into the body contains a radioactive isotope of that element or compound containing a radioactive isotope of that element, then the organ could receive a significant dose.

- Location of the organ or tissue - an organ located close to another that has incorporated a radioactive element will receive a higher dose than one more distant.

As is described in the discussion below concerning Alexander Litvenenko, the most desirable radioactive material for an attack with the purpose killing or injuring humans would be a radionuclide has a very high specific activity (Becquerels/Curies per gram) and emits a particle that deposits a large amount of energy. The material would have to get into the body by one of the mechanisms mentioned earlier. If stealth is also a consideration, another desirable property would be that the material would not emit other radiations which could be easily detected or could be easily shielded to prevent detection of other types of radiation it might emit.

Gamma-emitting radionuclides can be used to expose individuals with a source external to their person. With the exception of ^{226}Ra and a few transuranic radionuclides, most alpha-emitting radionuclides do not emit gamma radiation of sufficient intensity or energy to pose an external radiation hazard. ^{226}Ra produces radioactive progeny within a short period of time that emit high energy and intensity gamma radiation and additional alpha-emitting progeny. It, therefore, represents a threat as both a significant external and internal contributor to dose. The most commonly available gamma emitting radionuclides are ^{137}Cs and ^{60}Co. If exposed to gamma radiation from either radionuclide, even from a source that is approximately a D-value (at a distance of one meter for one hour), a significant dose can be delivered. A dose of approximately 1 R can be delivered in one hour for each radionuclide. If exposed to the radiation for an 8-hour workday, doses can begin to approach those expected from a quantity of concern in one hour.

A gamma-emitting source, once removed from its shield, may be readily deployed as a radiation exposure device (RED). Because gamma rays may be easily detected remotely with more sophisticated detection equipment or within several tens of meters using more commonly available

detection equipment, they have a much higher probability of early detection assuming a monitoring program is in place.

If the goal of the terrorist is to deny access or disable infrastructure, then he/she will most likely seek to contaminate facilities or areas with enough radioactive material to necessitate a long clean-up project. This activity will more than likely be conducted in a manner to also produce sufficient destruction to require rebuilding. In other words involve the use of a radioactive dispersal device (RDD) or bomb. Contamination by itself does not necessarily require an explosive device. An air conditioning system, fogger or any number of other methods may be used for dispersal if the radioactive material is already in a dispersible form. Alpha-emitting or beta-gamma emitting radionuclides could be used in this type of attack. A successful attack would require a lower activity of an alpha-emitting radionuclide than a beta-gamma emitting radionuclide. Much smaller quantities of alpha-emitting radionuclides that are inhaled will generally cause a greater dose per unit intake than small quantities from dispersed, beta-gamma emitting radionuclides (taking into consideration the contribution to dose from both external exposure and from inhalation).

Although alpha emitting radionuclides are more effective weapons in terms of the amount of radioactivity necessary to produce a high dose weapon, ^{137}Cs and ^{60}Co are more readily available. The increased availability of the beta/gamma emitting radionuclides increases the probability of their use in a radiological weapon.

Knowing the amount of material that could be obtained from a particular site and the worst-case consequences that could be reasonably expected to be produced by deployment, a consequence bin is determined from Table A2 of the Phase I report (see footnote 5). The consequence is measured in dollars, fatalities, and serious injuries. There is also a probability of successful deployment (Pd) associated with each bin. The more difficult the event is deemed to be, the lower the probability of success. The probabilities are subjective and the values provided in Table A2 are suggested only. If the assessor has additional information, the suggested value can be overridden.

The probability of interdiction (Pi) is estimated by others. This is an estimate of the probability that the perpetrators will be prevented from deploying the device assuming that the authorities know the material was obtained. Obviously many variables can affect the probability that the terrorist will be interdicted. It is logical to assume that the shorter the time between obtaining the material and deploying it, the more likely the terrorist will be successful. Additionally, it would be reasonable to assume that material obtained close to the target would increase the probability of successful deployment. If no information is available from law enforcement or other reliable sources, it is conservative to assume a value of zero (0.0).

Once these values are determined, the overall conditional risk is estimated as follows:

Risk = Po x Pd x (1 - Pi) (Consequence Values) (2)

Where:

Po = Probability of Obtaining the Material

Pd = Probability of Deploying the Material

Pi = Probability of Successful Interdiction and Preventing Deployment

Materials Considered

A radionuclide is an isotope (one of two or more atoms of an element that have the same atomic number [the same number of protons] but a different number of neutrons) in which the nucleus is unstable. The instability is the result of excess energy. The primary mechanism for the atom to achieve stability is to change the number of protons or neutrons by emission of a particle. The emission of the particle is frequently accompanied by the emission of a gamma ray. The type of particle emitted is a function of the atomic number of the radionuclide and other factors. Larger atoms of a 200+ atomic mass units (AMU) emit alpha and beta particles. Lower atomic weight radionuclides will decay by emission of beta particles and likely a gamma ray. Interaction of these particles and gamma rays with other matter will transfer energy to that matter. The energy transferred often causes ionization of atoms and the ionization can result in a chemical change in the matter. Chemical change inside the cell can result in changes in critical molecules within the cell that in turn result in cell damage. The deposition of energy when described in terms of energy imparted per gram of target material is called the dose. This is a slightly different concept of dose than that used for chemical toxicology. Chemical dose refers to a quantity of a chemical that has been ingested, inhaled or otherwise incorporated into the body.

Radionuclides not only differ in the types of radiation they emit, but also the energy of the radiation they emit. Thus, some radionuclides are capable of delivering a higher dose per unit activity than others. Also, the different particles are capable of delivering different amounts of energy. Alpha particles, because they are capable of creating more ion pairs per unit distance traveled, deposit more energy. Beta particles create fewer ionizations per unit path length and consequently deposit less energy. Gamma rays will produce even fewer ionizations per unit path length and therefore, deposit the least energy of the three emissions discussed.

Because the alpha and beta particles interact with matter more frequently along a specified path length, and transfer energy with each interaction, they lose energy faster than gamma rays and, as such, have shorter ranges. For instance, the range of an alpha particle in air is limited to 5 to 10 cm. A beta particle's range in air may be a meter or two depending on the kinetic energy of the particle, usually expressed in megaelectron or kiloelectron volts (MeV or keV). The gamma ray has a much longer range in air and can penetrate through solid materials easily. As the material becomes denser, the range of its gamma rays rapidly decreases. Dense materials such as lead are very good shields for gamma rays.

Alpha particles cannot penetrate the layer of dead skin cells and therefore do not pose a radiation hazard as long as the radionuclide emitting them resides outside the body. If that radionuclide, however, is near or inside a cell, the alpha particles it emits can damage the cell internally and possibly the nucleus directly. Therefore, alpha-emitting radionuclides can deliver a dose, only if ingested, inhaled or otherwise incorporated into the body.

Beta particles can pose both external and internal dose hazards. Depending on their energy, beta particles can deliver a dose to shallow, subcutaneous tissues if close to the body. They can also deliver dose if incorporated into the body.

As many gamma-emitting radionuclides also emit beta particles, they can deliver dose from outside or inside the body. The gamma ray can deliver a dose from a significant distance (meters) outside the body to organs located deeper in the body.

Dose is also directly proportional to the particulate or electromagnetic (gamma ray) radiation's energy. Therefore, higher energy beta particles are capable of delivering a higher dose than lower energy betas.

Another key factor in dose is the pharmacokinetics (the body's reaction to drugs, including their absorption, metabolism, and elimination) of the particular radionuclide (element). Thus the chemical form of the radionuclide may dictate that it will be concentrated in a specific tissue or organ. The energy might then be concentrated in a small organ (low mass) and the dose (energy deposited per gram) to that organ can be much greater. Another factor that is directly proportional to dose is the half-life of the radionuclide. This is related primarily to radionuclides once incorporated into the body. Since the residence time for a particular chemical form of a radionuclide is a function of its biological half-life, the dose becomes a function of an expression of the combined radiological and biological half-lives (called the effective half-life). For a radionuclide with a long radiological half-life and a long biological half-life, the total dose delivered will be large. Decreasing the biological half-life, the radiological half-life, or both will result in a lower dose.

Specific activity is a property of a radionuclide that is generally inversely proportional to its half-life. Specific activity is defined as the amount of radioactivity associated with one gram of that radionuclide. In general, the shorter the half-life of the radionuclide, the higher its specific activity. This property may make the use of a particular radionuclide for an attack on an individual more efficacious than use of another radionuclide with a lower specific activity. The high specific activity means that a very small physical amount of material is all that would be required to provide a lethal dose to an intended victim. If the radionuclide produced only a type of radiation that is difficult to detect, such as alpha radiation, then it could be smuggled through a sophisticated security screen with little chance of discovery. Scans to detect alpha radiation would be useless if the material was packaged as a pill in a blister pack, commonly used for over the counter drugs. The assassination of Alexander Litvenenko demonstrates the efficacy of this approach. After his death scientists determined that Mr. Litvenenko had approximately 1.85 MBq (50 mCi) of Po-210 in his body at the

time of his death. In terms of mass this would equate to 10 micrograms of material. In terms of toxicity, it represents about 200 times the amount of Po-210 necessary to kill a person.

Thus, taking their individual properties into account, the dose from a given amount of one radionuclide can have a high consequence to exposed individuals, and the dose from the same amount of another radionuclide have a much lower, possibly even negligible consequence to individuals.

Because some radionuclides do represent a greater hazard than others to humans (that is they are considered more radiotoxic), they are assigned much lower allowable contamination limits. Thus, any clean-up requiring decontamination of materials will be more expensive if the radionuclides involved are considered to have high radiotoxicity.

In view of the above, it is necessary to choose the isotopes and minimum quantities that need to be considered as "useful" for terrorist acts or dangerous in the event of an accident or natural disaster. In 2006, the International Atomic Energy Agency (IAEA) published IAEA-EPR-D-Values, with its list of isotopes and quantities that are considered dangerous. A more complete discussion of the IAEA D-values can be found in Appendix 3 of this document. The IAEA listed D-values are the threshold isotopes and quantities used in this study.

Examples of Risk Assessment

While it is possible to develop a risk assessment procedure that will provide the user of MIAN self-assessment tools to estimate the risk posed by the actual materials for which have the responsibility to secure, it is more efficient and practical to provide examples to illustrate the magnitude of risk. It will be shown that the consequences of allowing MIAN materials to fall into the hands of terrorists are so great that there is no doubt that they should be as secure as practicable.

First, consider the Risk Assessment Schematic of Figure 2. Step 1 is to obtain the materials. Consider the materials that are under your control. Can they be taken without the knowledge anyone at your site? How much material can be removed? How long would it take to discover that material is missing? Consider trusted employees as well as guards and users. An armed attack would definitely result in an alert to police and increase the chance of interdicting the terrorist before the material can be deployed, at least in the manner that will cause the greatest consequences.

It will be assumed that an armed attack on your site will result in the terrorist obtaining materials. An armed attack will also guarantee that the authorities will know the material has been stolen and they will actively pursue the terrorist. A stealth attack, in which the material is taken without the knowledge of on-site security, will greatly decrease the probability that the terrorist plot can be interdicted before the material is deployed. Based on these assumptions, we will use the following assumed parameters for estimating risk.

Step 1: Obtaining the Materials

Assume a moderate amount of material is taken. Assume 100,000 curies and in a form that can be used for a dirty bomb. Assume two attack modes.

1. The first mode is an armed attack. The terrorist uses weapons to overcome security personnel and takes the material with the knowledge of site personnel. The authorities are notified immediately when the terrorist leaves the building.

2. The second is a stealth attack. The theft is discovered at least eight hours after the material is taken.

Step 2: Avoiding Interdiction

1. The armed attack mode will result in immediate police activity to interdict the terrorist. There is a high probability that the authorities will be able to stop the terrorist from reaching the intended deployment location. Estimate 90% probability of interdiction. However, the terrorist will probably have a back-up plan to detonate a device either at the site where the material was obtained or en route to the planned deployment location. This event is assumed to have a probability of 1.0 but reduces the consequences by 50%.

2. A stealth attack in which the terrorist is able to obtain the material and the theft is not reported for eight hours or more will result in a low probability of being interdicted and a high probability of successful deployment. Assume a deployment success of 90% and interdiction probability of only 10%. The consequences in this case are assumed as the maximum reasonable consequence for the scenario.

Step 3: Deploying at the Target:

This probability depends upon whether the theft is discovered quickly and interdiction activities can prevent the terrorist from deploying the material as planned. The assumed values for deployment were discussed above.

Target and Consequence Estimate:

For the purposes of illustrating risk estimation, two deployment scenarios will be assumed. The first is a dirty bomb attack on the Ports of Los Angeles and Long Beach. The second is a dirty bomb attack in downtown Manhattan. Other possible scenarios will be discussed at the end of this section.

1. The first example is based on a comprehensive study by H. Rosoff and D. vonWinterfield[20] . This article analyzes possible terrorist attacks on the ports of Los Angeles and Long Beach using a radiological dispersal device (RDD, also known as a "dirty bomb") to shut down port operations and cause substantial economic and psychological impacts. The authors

[20] H. Rosoff and D. vonWinterfeldt, A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach

examined 36 attack scenarios and reduced them to two plausible or likely scenarios using qualitative judgments. For these two scenarios, they conducted a project risk analysis to understand the tasks terrorists need to perform to carry out the attacks and to determine the likelihood of the project's success. The consequences of a successful attack suggest that the chances of a successful dirty bomb attack are about10–40% and that high radiological doses are confined to a relatively small area, limiting health effects to tens or at most hundreds of latent cancers, even with a major release. However, the economic consequences from a shutdown of the harbors due to the contamination could result in significant losses in the tens of billions of dollars, including the decontamination costs and the indirect economic impacts due to the port shutdown. The implications for countering a dirty bomb attack, including the protection of the radiological sources and intercepting an ongoing dirty bomb attack are discussed.

Conclusions:

This study concludes that a terrorist attack using a dirty bomb in the United State is possible, perhaps even moderately likely, but would not kill many people. Instead, **such an attack primarily would result in economic and psychological consequences.**[21] Moreover, it would not be easy to carry out a dirty bomb attack. Considering the difficulties associated with obtaining and transporting radioactive material, building the dirty bomb, and detonating the device successfully, preliminary analyses suggest that the chances of a successful attempt are no better than 15–40% for the medium radioactivity scenario, and less likely for the high radioactivity scenario. Of course, multiple independent attempts would increase these chances. While our probability estimates are mostly illustrative, the chances of terrorists succeeding with an attack that involves relatively low-level radioactive material from a U.S. facility are larger than their chances of succeeding with the import of a large quantity of foreign sources. If a dirty bomb attack is successful, the consequences depend primarily on the amount of radioactive material in the detonated source term, the amount released into the air, weather conditions, and the population density in the impacted region.

The medium radioactivity scenario analyzed in detail suggests there would be some, but fairly limited, health effects and possibly significant economic impacts. The most costly economic impact would result from a lengthy shutdown of the ports and decontamination efforts. The length of the harbor shutdown would in part depend on the decision to declare access to the ports as safe. In a national emergency, standards of safety different from those promulgated by the EPA may be appropriate. For example, worker safety standards may be more appropriate than public safety standards. The same also holds true for clean-up standards. Because it is not known how policymakers and harbor workers will react in such an emergency, the authors parameterized the length of the harbor shutdown, from 15 days to one year, corresponding to roughly $130 million to $100 billion in costs. The economic consequences of evacuations, property value impacts, and business losses due to stigmatization in the plume area are in the billions, but not in the tens or hundreds of billions. People and the economy are likely to respond in a resilient way. Many people

[21] Emphasis added (bold) by the authors of the MIAN methodology.

would relocate for some time out of the areas with relatively high levels of radioactivity (100 mrem or more), but they would not stop working. Also, businesses may relocate and later return to their original location. Similarly, effects on property values may be severe in the short term but, like in many other disasters, return back to normal in a year or so. Regarding countermeasures, our analysis clearly supports ongoing programs to install radiation detection technology around the harbor. In addition, the analysis raises concerns regarding the security risks associated with cargo material as it is offloaded from ships but not yet transported through the portals, incoming containers from the U.S. mainland (by truck, small boat, or air), and harbor perimeter control. Finally, the analysis suggests preventing terrorism by interdicting vulnerable activities during the planning and preparing stages of an attack scenario. **Such action might include being more proactive in controlling and protecting the original sources of radioactive material.**

Discussion of conclusions:

The MIAN authors agree with the conclusion that such an attack is moderately likely and that such an attack would not kill many people. The purpose of such an attack is to disrupt, not destroy. **It is difficult to estimate the psychological effects.** The estimate of an overall probability of success of between 15 to 40 percent is actually quite high considering the complexity of the attack and the size of the facility. Their suggestion that multiple attacks would increase the probability can be argued. Once an attack is attempted at one location, the probability of success will be reduced significantly. One lesson learned by the terrorists is that the United States has an excellent record of "closing the barn door after the horse has been stolen." Of course, this greatly increases the cost of the consequences of an attack, so one of the purposes of terrorist is realized, i.e., causing a large financial impact. This observation should be considered when estimating the cost of consequences.

The cost estimates for consequences varied over a wide range, i.e.,

$130 Million < Consequences < $100 Billion

Further, the consequences calculated by H. Rosoff and D. vonWinterfeldt do not appear to include secondary or cascading effects. For example, if such an explosion were to occur it is reasonable to assume that other ports would be immediately shut down and all container inventory checked. Only a few percent of shipping containers are actually opened and inspected currently. Would this become a requirement in the future? Given that over six million containers enter the United States each year, what would be the cost of inspecting even a significant percentage of them? What additional regulations would be promulgated because of an event of this magnitude? Draconian regulations could cripple the shipping industry, not to mention the additional requirements for storing or using MIAN materials. If the airline security regulations are an indication of how the shipping industry might be affected, the long term consequences will be much greater than the estimates provided by Rosoff and vonWinterfeldt.

However, for illustrative purposes, assume the worst reasonable consequences calculated by Rosoff and vonWinterfeldt. For the high end, assume 40% overall probability of deployment and consequences of $100 Billion. Thus:

Step 1- Armed attack to obtain-

Pi = .90, C = (.5) $100Billion = $50 Billion

Steps 2 and 3 result in risk

Risk = Po x Pd x (1 - Pi) (Consequence Value)

= (1.0)(1-.9)($50 Billion) = $5 Billion

Step 1- Stealth to obtain

Pi = .1, Pd = .9, C = $100 Billion

Steps 2 and 3 result in risk

Risk = Po x Pd x (1 - Pi) (Consequence Values)

= (1.0)(1-.1)(.9)($100 Billion) = $81 Billion

The second scenario, attack by dirty bomb on Manhattan, would follow a very similar pattern. The only significant difference is the consequence estimation. On one hand, one can argue that a dirty bomb explosion in a large city will not cause nearly as much monetary consequential damage as an attack on a major port. The clean-up of the affected area can be performed relatively quickly and the residual radiation is low. One would expect to get back to normal usage in days to weeks rather than months or years. In addition, the number of fatalities and acute injuries, including latent cancers, would be expected to be relatively small. Fatalities would presumably be caused by the explosion rather than from radioactivity. However, the most difficult consequence to estimate is the longer-term effects, the cascading effects, caused by the attack. How would the politicians react? Would we see a plethora of new requirements for security for entering the city and other metropolitan areas? Would we be subjected to searches of automobiles, and personal belongings? What about access to public transportation? How would such an event affect the security requirements for MIAN materials?

Because the answers to these questions are unknown and will not be known until we are faced with an event of this type, it is reasonable, for illustrative purposes, to assume that the risk is at least as great as previously calculated for the port event. The monetary risk alone would be in the tens of billions dollars at least, considering cascading effects. Given that these events have such high associated risk, one must consider ways to reduce the risk level.

Referring again to Figure 2, it is clear that MIAN sites and security officers cannot have any direct impact on interdiction of the terrorists once law enforcement is alerted nor can they mitigate the consequences of an attack. The only plausible ways to reduce overall risk are:

1) Decrease the probability of obtaining MIAN materials

2) Alert law enforcement officers as quickly as possible to increase the probability of interdiction

Thus, the role of site security is to make the site as secure as possible and to account for the materials on site and in use by field employees.

The actual risk associated with each site is, of course, much lower that the cumulative risk, which is calculated above. Equation 1 above contains an additional term, threat. Threat is defined as the probability that your particular site will be attacked. Equation 2, used for the above calculations, assumes that the value of threat is unity. The actual risk that can be attributed to any particular site is much less than the cumulative risk. Assuming that there are, say, 10,000 sites in the United States that have sufficient radioactive materials to cause risk of this magnitude, and assuming an equal attack probability for all sites, the risk for any one site is simply the cumulative risk divided by the total number of sites. This reasoning, while correct, leads to the conclusion that the risk for each site is relatively small. However, having a large number of sites is a two edged sword. Having so many sites practically insures that the terrorist can find a poorly protected source of material. The material from one site can cause extreme consequences from an actual event, and it will result in increased costs for everyone for many years. Thus, it is important to prevent even one occurrence.

There are numerous additional ways that a terrorist can utilize MIAN materials to attack the United States. The authors have found that all of these scenarios result in a similar conclusion; if possible, we cannot afford to allow such an event to happen.

The security screening and assessment methodology developed by this project, if used voluntarily and effectively, will greatly reduce the cumulative risk of terrorist attack. The cost, in terms of manpower, to perform the security assessment is minimal. The program is free. The benefit to everyone clearly outweighs the cost. If one such event occurs the consequences for everyone, including those who use and store MIAN materials as well as the public, will be costly. If new and stricter regulations and requirements are imposed, the probability of having them relaxed or removed is quite low.

Brief resumes of the investigators follow.

JAMES WILLIAM JONES, Ph.D., P.E

Principle Investigator

5561 Ocean Terrace Drive, Huntington Beach, CA 92648

www.jwjce.com bill@jwjce.com (m) 714.585.4820

EDUCATION

1973 University of Pittsburgh Ph.D., Mechanical Engineering

1968 University of Texas M.S., Mechanical Engineering

1966 University of Texas B.S., Mechanical Engineering

RESENT EXPERIENCE

2003 - Present	Consultant, J. William Jones Consulting Engineers, Inc., Senior Fellow, ASME-ITI, LLC
2004 - 2005	ASME Washington Fellow
2002-2003	ASME White House Fellow, Office of Science and Technology Policy Executive Office of the President of the United States

AREAS OF SPECIALIZATION

Corporate Management, Corporate Marketing & Business Development, Risk Analysis and Antiterrorism, Container Security, Protection of Vulnerable Infrastructure Systems, Risk Analysis, Finite Element Analysis Methods, Stress Analysis, Dynamic Analysis, Thermal Analysis, Pressure Vessel Design & Analysis, Design & Analysis of Spent Nuclear Fuel Shipping Containers, Petrochemical and Chemical Vessel Design, Expert Witness Testimony, Failure Analysis, Electronic Packaging.

PROFESSIONAL SOCIETIES AND HONORS

Fellow - American Society of Mechanical Engineers (Elected 1984)

Fellow - National Academy of Forensic Engineers (Elected 2011)

Fellow - Institute for the Advancement of Engineers (Elected 1985); Sigma Xi (Scientific Research Society)

Registered Professional Engineer - Pennsylvania, California and Illinois

T.U. Taylor Award - University of Texas (1967)

Three Patents and Numerous Patent Disclosure Awards (from various employers.)

CURRENT STATUS

Dr. Jones is a consultant to government and industry in the areas of expertise detailed in this resume. He is currently engaged in several projects in several diverse areas including homeland security, expert witness testimony, petrochemical industry consulting. Until 2008 he was a consultant on contracts with the Department of Homeland Security (DHS) to develop a general risk based guideline which is used to determine how best to allocate resources for prevention and mitigation of terrorism. In this capacity he was retained as a consultant to ASME-ITI. Formerly, he was a Senior Fellow at the ASME Innovative Technology Institute. The development of the RAMCAP© and RAMCAP Plus℠ methodologies emanated from conceptual investigations initiated during the year he spent as an ASME Fellow at the Office of Science and Technology (OSTP), Executive Office of the President. More information concerning RAMCAP© and RAMCAP Plus℠ is available from ASME-ITI.

When Dr. Jones served as an ASME White House Fellow (2002) in OSTP, he was assigned to work on issues involving protection of critical assets from terrorist attack. In this one year assignment, he assembled a working group consisting of representatives from ten departments of government. A five-year program for R&D requirements for antiterrorism was produced which contains the strategic plans for the agencies represented in the Protection of Vulnerable Systems (PVS) Subgroup. He was also assigned to follow the technology for inspection of intermodal cargo shipping containers. The main thrust of this project was to implement new technology that could significantly reduce the time necessary to inspect each container for weapons of mass destruction. He developed a risk-based strategy to rank terrorist threats to the infrastructure and to assess the efficacy of proposed solutions.

Dr, Jones maintains offices in Huntington Beach, California, where he provides consulting services to the petrochemical, legal, and commercial products sectors.

Robert E. Nickell, Ph.D.

2500 Sixth Avenue, Unit 204, San Diego, CA 92103

(619) 255-3533 (H); (619) 255-9930 (O/F); (858) 945-2781 (M)

RNickell@cox.net; NickellR@asme.org

Education: Dr. Robert E. Nickell received his B.S. (1963), M.S. (1964), and Ph.D. (1967) degrees in Engineering Science from the University of California, Berkeley.

Professional Career: After receiving his doctorate in 1967, Dr. Nickell was employed by Rohm & Haas Company at the Redstone Arsenal in Huntsville, AL, where he worked on solid propellant rocket motors and related explosive munitions for the United States Army. When Rohm & Haas closed their Huntsville operations, he was hired by Bell Telephone Laboratories, Whippany, NJ, where he worked from 1968-1971 on the SPRINT and SPARTAN defensive missile systems, plus classified work on spy satellite systems. When Bell Telephone Laboratories exited the missile defense business in 1971, he was placed on an industrial sabbatical teaching assignment at Brown University, Providence, RI, as an Associate Professor of Engineering (1971-1973). During this period he was given the AIAA/ONR Naval Structural Mechanics Award for his work on dynamic bucking of naval structures from external explosions. After this (1973-1977) Dr. Nickell returned to the Bell System at the Sandia National Laboratories (operated by Western Electric at that time) in Albuquerque, NM, where he worked on nuclear weapons design and analysis and was promoted to Supervisor of Design Technology in the Transportation Technology Department, with responsibility for radioactive material transport packaging design and analysis. This assignment also involved interactions with other units at Sandia National Laboratories carrying out experiments and analyses on preventing terrorist acquisition of nuclear weapons and weapons-grade material. Dr. Nickell left Sandia in July 1977, becoming a private consultant to industry and government, except for direct assignments as a Project/Program Manager for the Electric Power Research Institute (EPRI), Palo Alto, CA, from September 1980 to October 1984, and as the Technical Director for SGI International, La Jolla, CA, from April 1992 to March 1995. Dr. Nickell provides his consulting services through Applied Science & Technology, a California C corporation.

Codes and Standard Activities: Dr. Nickell has been involved in various ASME Boiler and Pressure Vessel Code activities for the past thirty-seven years, and is currently the Chair of the Task Group on Impulsively Loaded Vessels of the Working Group on High Pressure Vessels (Section VIII, Division 3). He was the founding Chair of what is now the ASME Code Section III Subgroup NUPACK that has developed rules for the design and fabrication of containment systems for nuclear spent fuel and

high-level waste transport packagings. He is also a member of ASME Code Section XI Special Working Group on Nuclear Plant Aging Management, and is the Secretary, RAMCAP Standard Committee, reporting to the ASME Board on New Development. He was the elected Chairman of the three Consultants Service Meetings (CSMs) that developed criteria for the evaluation of brittle fracture for radioactive material transport packagings, under the auspices of the International Atomic Energy Agency (IAEA).

Other Professional Activities: Dr. Nickell is a member of ASCE, ANS, and ASTM, and is a Fellow of the ASME and of the AAAS. Among his many activities within ASME, he was a Member-At-Large of its Board of Governors from 1992-1994, chaired the Board's Committee on Finance & Investment from 1994-1998, served as its 118th President from 1999-2000, served as Secretary-Treasurer from 2001-2004, and currently chairs its Pension Plan Trustees. He is also a member of the Board's Committee on Honors and currently chairs the ASME Headquarters Facilities Task Force.

Honors and Awards: Dr. Nickell was the 1972 recipient of the Office of Naval Research/American Institute of Aeronautics and Astronautics (ONR/AIAA) Naval Structural Mechanics Award, and was appointed by U.S. Secretary of Energy Hazel Rollins O'Leary to the National Coal Council for the period 1993-1995, and reappointed for the periods 1995-1997 and 1997-1999. He was selected to present the Robert D. Wylie Memorial Lecture at the Ninth International Conference on Pressure Vessel Technology in April 2000. He has authored or co-authored some 100 papers in refereed journals. He was elected to the National Academy of Engineering in 2007.

Experience in Risk Assessment:

Dr. Nickell has been a consultant to the Electric Power Research Institute (EPRI) since 2001 on vulnerability of nuclear power plant structures, including containment structures and spent fuel pools, to terrorist attack, with major emphasis on aircraft impact, and has served for the past four years on the EPRI Expert Panel on Aircraft Impact Assessment (10 CFR 50.150).

He also consulted with EPRI during the period from 1986-1988 on probabilistic risk assessment of spent radioactive fuel rail and truck casks subject to transport accidents.

He was a member of the original team at ASME ITI working under a grant from the Department of Homeland Security to develop RAMCAP, and was a consultant to ERIN Engineering during the application of RAMCAP to the nuclear power sector.

He was a member of the six-person task force reporting to the Secretary of Energy Advisory Board (SEAB) in 2005-2006 on the reorganization of the DOE/NNSA weapons complex, which included the review of security against terrorist attack at the various sites throughout the complex.

He has been a consultant to Los Alamos National Laboratory since 1998 on the design and operation of containment vessels for dynamic explosive experiments, including the potential need to reduce risk from explosive fragment penetration.

He has been a consultant to Kobe Steel, Ltd., for ten years on the design and operation of detonation chambers for the explosive destruction of chemical weapons, including detonation chambers at Port Kanda in Japan (non-stockpile WWII chemical weapons); in Poelkapelle, Belgium (non-stockpile WWI chemical weapons); Toele, Utah (U.S. Army stockpile chemical weapons); and more recently Nanjing, China (non-stockpile WWII chemical weapons).

He is currently a consultant to Amtrak on the vulnerability of railroad tunnels and bridges to terrorist attack.

He consults with ASME ITI on the MIAN/RAMCAP project for the Sloan Foundation.

Other Professional Activities: Dr. Nickell is a member of ASCE, ANS, and ASTM, and is a Fellow of the ASME and of the AAAS. Among his many activities within ASME, he was a Member-At-Large of its Board of Governors from 1992-1994, chaired the Board's Committee on Finance & Investment from 1994-1998, served as its 118th President from 1999-2000, served as Secretary-Treasurer from 2001-2004, and currently chairs its Pension Plan Trustees.

John R. Haygood, MS, TLMP

2228 Mockingbird Dr
Round Rock, TX 78681
Phone: (512) 551-2153
Cell: (512) 656-2832
Email: jhaygood@swbell.net
Website: radiationsafety.net

Education

BA, Physics, 1972, University of Texas at Austin, Texas

MS, Environmental Health (Health Physics), 1979, University of Texas Health Science Center, Houston, Texas

Licenses

Texas Medical Physics License #MP0327, Texas State Department of Health Services (DSHS), Austin, Texas

Professional Experience

Radiation Safety Consultant (Health Physicist): John R. Haygood, Consultant in Radiation Safety and Regulatory Processes, Austin, Texas, Mar 2009 – Present and Dec 1997 – Jan 2002

Own and operate a radiation safety consulting business. Working with various types of radiation users, such as well logging, industrial radiography, portable M/D gauges, medical, educational licensees and registrants, consult with customers throughout Texas and the United States with services designed to meet the collective and individual regulatory requirements of the Nuclear Regulatory Commission (NRC) or any Agreement State (AS) -- especially Texas. Prepare new, renewal, and modification license and registration applications with safety procedures. Assist licensees and registrants with compliance and enforcement actions by evaluating violations and problem areas to determine best course of action to achieve timely compliance. Interpret state and federal rules and laws and advise clients. Consult with officials and staff of the TDH, NRC, and other state/federal agencies. Conduct radiation safety officer, hazmat, and two (2) gauge training courses for customers and customer personnel. Perform radiation safety program audits, including radiation surveys, and prepare reports assessing risk to humans. Consult in security requirements and procedures for increased controls (new NRC security requirements). Assist with radiation accidents/incidents.

Radiation Control Program: Texas Department of State Health Services, Austin, Texas

Radioactive Materials License Inspector - Health Physicist I, and Quality Assurance Reviewer - Environmental Specialist V (Health Physicist) Feb 2002 – Aug 2008: Performed inspections of all types of radioactive materials licenses and non-healing arts x-ray registrations in the Austin area (26 counties). Responded to and investigated radiation incidents. Submitted comprehensive reports listing violations if found. Provided radiation safety training to radiation control staff. Prepared notices of violation and compliance; and reviewed responses to notices of violation to assure compliance with the Texas rules. Participated in enforcement procedures. Performed periodic accompaniments of inspectors to evaluate their performance. Managed reciprocity program. Interpreted state and federal radiation control rules and rules of the US DOT and provided information to others.

Deputy Director, Radioactive Materials - Environmental Quality Specialist VI (Health Physicist) (Title was Branch Administrator from 1981 to 1995, retired from program in 1997), Jul 1981 – Oct 1997: Directed/managed/administered operations of a statewide radioactive material, non-healing arts x-ray, nonionizing radiation inspection program and a field environmental surveillance program, with up to 15 central office personnel and 15 regional inspectors. Presented training courses in the meetings to central office and regional staff on radiation safety and regulatory matters. Performed inspections of operations of all types of licensees and registrants (well logging, industrial radiography, accelerators, medical, etc.). Performed investigations of radiation incidents. Performed as a member of the state radiation emergency response team in accident assessment. Developed and implemented the enforcement program.

Assistant Chief of Compliance and Supervisor of Isotope Program, 1979 – 1981: Set inspection schedules for staff and directed state wide radiation control inspection/compliance activities. Performed inspections of well-logging, industrial radiography, broad license, major processor and uranium mill licenses and operations, and all other types of licensed programs and performed incident and complaint investigations.

Radioactive Materials License Inspector and X-Ray Inspector, 1972 – 1979: Performed inspections of medical, industrial (esp. well-logging and industrial radiography) and educational radioactive material licenses and registered x-ray producing and laser devices.