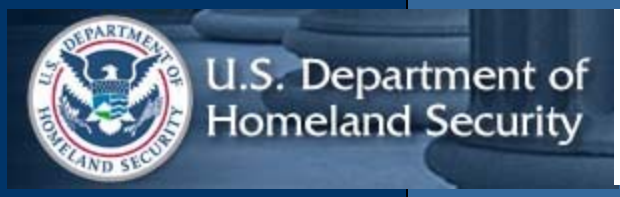

VULNERABILITY ASSESSMENT METHODOLOGIES REPORT

July 2003

This report is confidential and intended solely for the use and information of the organization to whom it is addressed.

Phase I Final Report

Office for Domestic Preparedness
Department of Homeland Security

FOREWORD

In July 2002, the President approved the *National Strategy for Homeland Security*, establishing a road map for the national effort to prevent and respond to acts of terrorism in the United States. The *National Strategy* recognizes the vital role of state and local public safety agencies in providing for the security of our homeland. In February 2003, the President signed into law the Consolidated Appropriations Resolution, 2003, Public Law 108-7 that provides state and local governments with the vital funding they require to participate in the national effort to combat terrorism. In April 2003, the Emergency Wartime Supplemental Appropriations Act, 2003, provided additional funds to expand and continue these efforts.

The U.S. Department of Homeland Security (DHS), Office for Domestic Preparedness (ODP) reflects the intent of Congress and the Administration to enhance and quantify the preparedness of the nation to combat terrorism. Whereas most states and municipalities have strengthened their overall capability to respond to acts of terrorism involving chemical, biological, radiological, nuclear or explosive (CBRNE) weapons, there continues to be room for improvement in meeting our national priorities of preventing and responding to terrorist attacks.

The Office for Domestic Preparedness identified a need to examine and classify various types of vulnerability assessment methodologies, software and tools as they would pertain to different types of assets. This Vulnerability Assessment Methodology Report provides an analysis of various commercial and government vulnerability assessment methodologies which can be used by state and local governments to assess the risk associated within their areas of responsibility. The analysis provides a baseline comparative point from which to evaluate participating vulnerability assessment providers' services, products and capabilities.

The Department of Homeland Security looks forward to continuing to empower the first responder community - enabling them to make better-educated decisions about the equipment and technologies available to them.

CD-ROM versions of this document are available, in limited quantity, by sending requests to:

Centralized Scheduling and Information Desk (Publication Request)
Office for Domestic Preparedness
Department of Homeland Security
810 Seventh Street, N.W.
Washington, DC 20531

Table of Contents

EXECUTIVE SUMMARY

The Department of Homeland Security Office for Domestic Preparedness identified a need to examine and classify various types of vulnerability assessment methodologies, software, and tools that could be used by state and local governments to assess the risk associated with various assets within their areas of responsibility. A Sources Sought, OJP-Q-28, was released August 6, 2002 and published as FEDBIZOPS Notice #0249 requesting this information. This "Study of Vulnerability Assessments" Project is an analysis of various commercial and government vulnerability assessment methodologies.

Phase I of the current support to the Department of Homeland Security identified a group of methodologies. However, it did not test the usability of these methodologies or their effectiveness in a field environment. Such an operational test is essential to truly determine which methodologies are best used by state and local governments to allocate their scarce resources and best improve their overall security.

Forty-eight responses were received to the Sources Sought: thirty non-proprietary, eighteen proprietary. Most proprietary sources elected to redact proprietary markings. Four elected not to do so. Hence, forty-four private methodologies were considered in this study. It should be noted that most of the companies that responded to the Sources Sought notice provided marketing documents, not specific methodologies. In addition, the assessment team found sufficient information to make some level of assessment for twenty-four public (federal, state, and local government) methodologies.

Five subject matter experts (SMEs) from Booz Allen completed a final list of ten evaluation criteria to be used to assess and compare submissions to the Sources Sought (Table 1). Using this list of evaluation criteria and a forced choice, pairwise comparison methodology, called Expert Choice, these SMEs developed relative weights for each criterion.

This first group of SMEs, blind to the developed weights of each evaluation criteria, used software called IARDstick, and completed independent assessments of the forty-four private responses to the Sources Sought notice. A subgroup of SMEs assessed the twenty-four public methodologies identified by the study team. Based on the weights of the criteria and the degree to which each methodology satisfied that criteria, each methodology received a score, which was used to compare that methodology to all other submitted or obtained methodologies.

A second group of SMEs, representing fourteen of the participating companies, reviewed the evaluation criteria. This group concluded that the evaluation criteria were correct, comprehensive and useful for assessing each of the government and private sector methodologies under consideration. This second group of SMEs, again using

Expert Choice, replicated the criteria weightings derived by the first group of SMEs. There were no significant differences between the two groups.

CONCLUSIONS

First, the most robust methodologies do not solely focus on one sector of the economy.

Second, the quality of the assessor in all cases is very important. In other words, a mediocre methodology, well applied by a knowledgeable assessor will yield an acceptable and useful result and, thus, provide a basis for great improvements in security. The converse is also accurate. A good methodology applied by an unskilled assessor will not produce very useful results.

Third, while all methodologies determined some measure of risk, often implicitly, few actually calculated a numerical value for that risk. Clearly, the numerical values assigned were in nearly every case ordinal, at best.

Fourth, the training required to accurately use one of these methodologies varied greatly in time and cost. In the opinions of the SMEs, the quality and diligence of the assessor is as important or more important than the specific methodology used. A well-qualified and knowledgeable assessor minimizes the need for additional expensive training, is able to conduct the assessment more quickly, and will provide a more accurate, useful assessment. This will enable the user to more effectively assess vulnerability or risk.

Additional phases of this project would better determine the effectiveness of these various methodologies.

REPORT FOCUS AND APPLICATION

This document provides the results of this study that examined and classified various types of vulnerability assessment methodologies. A glossary of terms to standardize the multiple definitions of common terminology used in vulnerability assessment methodologies may be found at Appendix A. The report also includes a CD-ROM, which contains the report and the appendices in their entirety. The CD has two versions of IARDstick, the software tool developed and used in this study. The IARDstick tool icons are labeled “DHS Locked” and “DHS Unlocked.” The DHS Locked tool enables the reader to assess additional methodologies using the same metrics as used in this study. The DHS Unlocked version provides access to the IARDstick tool with the weights inserted, however, the criteria weights may be changed in this version. A Help Guide for the IARDstick tool is provided to allow locally determined criteria weights to be placed in the tool as developed by the reader. In doing so, it is important to remember not to compare assessments using the unlocked version against assessments using the

locked version because the baseline weighting criteria will be dissimilar. To utilize the IARDstick software, it must be copied onto the user's computer.

1.0 INTRODUCTION

The tragic events of September 11, 2001 profoundly changed the way that the United States views the potential for lethal terrorist attacks. According to intelligence gathering and public statements by known terrorists, there is a credible terrorist threat that the U.S. can again be a target. Years of repeated terrorist bombings around the world, the sarin gas attack on the Tokyo subway in 1995, and regular suicide bomber attacks on buses in Israel, gave grave concern to senior U.S. government decision makers that the United States may continue to be vulnerable.

The world environment has changed. Terrorism has become a global threat; no nation is immune. With an increased awareness and urgency, the United States must prepare to counter terrorist acts. After the attacks in New York and Washington, the Federal government had to quickly determine how vulnerable the country is to a terrorist attack and what to do about it. One of the highest priorities in government and the private sector is to prevent and prepare for future terrorist attacks using a variety of weapons.

Many organizations have conducted workplace risk, threat and vulnerability assessments in the past to keep their systems and businesses open and safe for the public. Although there are numerous commercial and government methodologies in use today, there is currently no single reference that defines what vulnerability assessment methodology (VAM) is most appropriate for specific types of assets in the community. Is it possible to use a single encompassing methodology to assess a stadium, government building, or an electric power plant? How are these various methodologies evaluated in terms of measures of effectiveness and other criteria such as cost, time involved, and complexity of the methodology?

The former Department of Justice, Office of Justice Programs, Office for Domestic Preparedness (ODP), now the Department of Homeland Security Office for Domestic Preparedness, identified a need to examine and classify various types of vulnerability assessment methodologies, software, and tools as they would pertain to different types of assets; e.g., office buildings, subways, stadiums, ports, electric power plants, etc. This "Study of Vulnerability Assessments" Project is an analysis of various commercial and government vulnerability assessment methodologies. It provides a clear mapping of each product's applicability toward individual asset types. Note that this study does not analyze counter-measures for reducing vulnerabilities (i.e., metal detectors at doors, barricades, air filters, etc.). Instead it focuses on the methodologies used to determine vulnerabilities and risks, which in turn, identify countermeasures that could be effective at reducing the risk by reducing the vulnerability.

The study's initial step was an OJP Sources Sought (OJP-Q-28, released August 6, 2002 and shown in Appendix A) that requested information concerning vulnerability assessment methods, software, and tools. Forty-eight responses were received, thirty of which were non-proprietary and eighteen that were marked proprietary. The responders were asked in writing if they desired to participate in the study. Of the forty-eight responses received, only four responders declined participation. It should be noted that most of the companies that responded provided marketing documents, not specific methodologies.

The study team of subject matter experts (SMEs) from Booz Allen Hamilton then developed a criteria matrix to assess the various aspects of each response and to measure the degree to which each response addresses these critical aspects of known, effective risk and vulnerability assessment methodologies. Each criterion was weighted using Expert Choice, a decision support tool. Then to validate and apply those weightings, another tool, the Infrastructure Assurance Readiness Decision stick or IARDstick, was used as a metrics-based mechanism to provide a consistent basis of comparative analysis for the submitted vulnerability assessment methodologies.

1.1 PURPOSE

The purpose of this study was to identify physical asset vulnerability assessment providers using a proven methodology, which incorporated the most current automated tools, software and technologies. In conducting this detailed study, the goals were to

- Develop criteria for analysis of various methodologies.
- Clearly map capabilities and identify any capability overlaps provided by the government and/or commercial vulnerability assessment methodologies, automated tools, software and emerging technologies.
- Describe advantages and disadvantages of using particular methodologies, automated tools, software and emerging technologies to assess different types of assets, i.e. stadiums, public buildings, factories, water systems.
- To the extent possible, within the time available, and without a corroborative study, provide evidence that methodologies, automated tools, software and emerging technologies can perform as advertised.

Subsequent phases of this study could provide an independent assessment of the above findings

- To document lessons learned via comparing and contrasting approaches used by the insurance industry to calculate risk and vulnerability with approaches

being taken to establish vulnerability and risk in defense of our national infrastructure against terrorists.
- To document the best process for selecting and validating VA tools.
- To document the costs and benefits associated with "target specific" versus more generic "industry specific" or "jurisdiction-wide" vulnerability assessment instruments.

This analysis provides a baseline comparative point from which to evaluate participating vulnerability assessment providers' services, products and capabilities.

1.2 SCOPE

The Office for Domestic Preparedness (ODP), Department of Justice (DOJ) charged Booz Allen Hamilton (BAH) to conduct a "Study of Vulnerability Assessment Methodologies, Automated Tools, Software and Emerging Technologies" for physical assets. As noted earlier, this study does not include evaluation of the countermeasures to reduce vulnerabilities that might be recommended as a result of using a given methodology. Companies using vulnerability assessment methodologies responded to a Sources Sought notice in FedBizOps and found at FBO.com. It should be noted that most of the companies that responded to the Sources Sought notice provided marketing documents, not specific methodologies. These responses were carefully catalogued and a library of the information submitted was created. Criteria for analysis of those methodologies was developed, weighted, and validated by subject matter experts. And then, submitted responses were evaluated against the criteria to ascertain the stated capabilities of the methodology used by each firm. While few of the respondents provided actual methodologies, some did indicate that they utilized well-known, existing methodologies, such as RAM-Wsm or CARVER.

1.3 DOCUMENT ORGANIZATION

This document shows the results of synthesizing information gathered; the science of risk assessment and vulnerability assessment; and an identified best process for selecting and validating vulnerability assessment tools.

The Executive Summary leads the report. It contains the overview and the report focus and application, which explain the contents of the report and the accompanying CD-ROM. Section 1 provides the introduction, purpose, scope, and organization. Section 2 discusses background, baseline information and a general discussion of risk assessments and the relationship of vulnerability assessments to the larger, and more beneficial category of risk assessments. It also provides a description of the designed model criteria for a vulnerability assessment. Section 3 defines the process used in the study and includes the general findings and discussion of the study. Section 4 is the

conclusion. Appendices A through D provided supporting documentation. Appendix A is a glossary of terms that sets forth definitions of common terminology used in vulnerability assessments. Several of the terms are shown with multiple definitions. In this phase, a survey was not conducted to determine which definition is or should be universally accepted. Additionally, a separate manual is provided to explain the usage of the IARDstick Methodology Assessment Tool.

2.0 BACKGROUND

The need to protect critical infrastructures and their interconnected systems as well as information, people, equipment, facilities and operations requires a comprehensive systematic evaluation of risk and careful, planned application of countermeasures to improve overall organizational security. There are many methods used in various industries to calculate risk. Hence, a general discussion of risk and risk assessment processes is essential to make a reasonable comparison between these different methodologies and determine their applicability to a given economic sector, mission, or organization.

2.1 UNDERSTANDING RISK

Terrorism has become a global threat. The terrorist bombings of the World Trade Center in New York City in 1993 and 2001, and the Federal Building in Oklahoma City in 1995 heightened concern about potential vulnerabilities to terrorist activities within the United States' borders. In 1998, attacks on the U.S. Embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, made it apparent that no one, anywhere, is completely safe from the effects of terrorism. Everyone, regardless of nationality or locality, must have effective safety measures and mechanisms that afford protection against potential terrorist activities.

In the past, the primary focus of the U.S. has been international terrorism. Although terrorists have long posed a threat to U.S. citizens and facilities, previous terrorist violence was generally limited in scope, primarily conducted overseas, and mostly directed at the destruction of property rather than

An effective Security Program Plan requires:

- Providing a coordinated approach that integrates all available resources to provide enhanced protection from potential terrorist activities.
- Identifying key assets that require protection and the potential threats and likely adversaries.
- Performing a vulnerability analysis to determine the effectiveness of existing and planned countermeasures for the key assets.
- Determining the degree of risk to each key asset.
- Providing prioritized countermeasure recommendations including their cost.
- Performing a cost benefit analysis for each countermeasure.
- Providing a roadmap of individual countermeasure actions as well as integrated collective countermeasure costs.

causing significant loss of life. As demonstrated by the bombings of the World Trade Center and the Murrah Federal Building, these tactics have changed. A primary objective of the terrorist today is to make a statement by killing and injuring as many innocent people as possible thereby causing embarrassment to the U.S. government. In addition to the resulting carnage from these terrible events, terrorism has become a media event. Terrorists will exploit the news media coverage to incite fear and gain attention for their cause. Further, even "small" terrorist events may potentially cause great economic disruption.

A terrorist group's selection of targets, weapons and tactics is primarily a function of the group's affiliation, level of training, organization, and sophistication. To achieve their goals, terrorists are likely to strike unprotected and highly visible targets. Terrorists often choose targets that offer little danger to them, have relatively easy access, and are located in the vicinity of large crowds of people that could be injured or killed as a result of the terrorist event. This target description is unfortunately also descriptive of our national infrastructure.

Terrorist groups are categorized according to their operational tradition. The categories include national, transnational, and international. National groups operated solely within the boundaries of a single nation. Within the U.S., these groups are referred to as domestic terrorist groups. Transnational groups operate across international borders. In the decade since the end of the cold war, transnational terrorism has become a major security concern for the U.S. International terrorist groups operate in two or more nations. They are usually assumed to have received their direction from some foreign government.

Although U.S. intelligence sources indicate conventional explosives and firearms remain the weapons of choice for the terrorist, there are also increasing concerns about the terrorist potential to use weapons of mass destruction (WMD) similar to the use of a nerve agent in the Tokyo subway in 1995. Today's terrorist is a more sophisticated entity than yesterday's. Partly due to technological advances, most terrorist groups are able to easily gather useful data as well as learn techniques to develop and produce modern weapons including WMD. Now the average terrorist group is highly organized, communicates effectively, is equipped with modern weapons and explosives, is thoroughly mobile, and has the capability to move these weapons and explosives rapidly across international borders. Vast funds available to some terrorist groups afford them armaments and technology rivaling some nation states.

Membership in terrorist groups brings together individuals who are willing to commit terrorist acts for various different reasons. Ideology may not be the only glue that holds many terrorist groups together. Some of these groups are augmented with professional criminals who are mainly opportunists; other members may be mentally disturbed. Regardless of their motivation, terrorists will look like ordinary citizens and they will come from all walks of life.

U.S. interests and citizens at home and abroad are targets for terrorism for many reasons, but primarily for ideological differences. America is a leading industrial power and capitalist state. This is more than enough reason to incite the animosity of some terrorist groups that are committed to different social systems. Other groups object to what they perceive to be the U.S. government's desire to dictate policy and courses of action over other governments. Another reason is U.S. citizens, mainly tourists, are almost everywhere. This makes targeting Americans relatively easy for the terrorist, and adds to the opportunities and increases the chances that Americans could be kidnapped, killed or injured.

Although there are statistically fewer terrorist events in the U.S. than in the past, concern over the potential for domestic terrorism in the U.S. is also on the rise. The relatively open U.S. political system allows minor groups to voice concerns legitimately through the political process. Sometimes the activities of these groups can lead to violence such as the bombings and shootings associated with the antiabortion movement. In addition, some groups of domestic separatists have recently targeted U.S. federal institutions and their employees for violence such the bombing of the Murrah Federal Building. These attacks demonstrate a willingness of these groups to attack symbols of the U.S. government. Radical and religious extremist organizations and individuals coupled with the growth and rise of radical militia elements in the 1990s within the U.S. also constitute a growing threat to public safety, law and order.

As a result of this evolving and unstable terrorist threat environment, there has been renewed interest, heightened domestic concern, and increased emphasis across the U.S. government. The FBI has stated that the Washington DC area is "the number one target in the world" for terrorist attacks. It is not "if but when." In view of this heightened concern, a number of Presidential Decision Directives (PDDs) have been issued emphasizing the terrorist threat, assigning responsibilities, directing planning, and enhancing training to protect the nation's critical infrastructure and respond to a terrorist crisis. Congress has already obligated substantial funds to combat terrorism with the understanding that the U.S. is not a sanctuary and the realization that some terrorist event will eventually occur. Despite this heightened awareness across the government and the private sector, the domestic U.S. infrastructure remains largely unprepared and in need of critical support. There continues to be concern within the U.S. over meeting the requirements established in PDDs and in previous security studies. The assessment of risk is as important as the quantification of risk. Subjective perception of risk is the basis for risk acceptance regardless of the objective or quantified level of risk.

In An Anatomy of Risk, William D. Rowe states that within the field of risk, there is a surprising diversity of definitions and as much diversity in the determination of an acceptable level of risk. Further, there is a singular lack of understanding of the means to assess risks.

For this report *risk* is simply the possibility of damage happening to an organization. Three important steps to performing a risk analysis include (1) identify risks; (2) determine impact of threats; and (3) balance impact of threats with safeguards.

Risk analysis helps determine risk exposure, and allows organizations to integrate financial objectives with security objectives.

There are three primary risk types that should be considered in determining risk exposure (1) mission or function risks; (2) asset risks; and (3) security risks.

Mission risk exposure is a determination of the vulnerabilities that exist and have the potential to prevent an organization from accomplishing its stated mission. Mission risk is sometimes referred to as function risk. Asset risk exposure is a determination of the vulnerabilities that exist and have the potential to harm an organization's physical or tangible assets. Security risk exposure is a determination of the vulnerabilities that exist and have the potential to cripple actual data, or people.

Threats subject an organization to risk. Therefore, when a threat is exhibited, a risk exposure variable needs to be considered in order to understand how to manage the risk. An agency threat management team should have processes and procedures in place for measuring the probability of loss and the severity of loss, in light of a threat. Determining risk exposure precedes decisions in how to manage the risk. Proper risk analysis helps organizations determine whether they should reduce, re-assign or transfer the risk, or accept the risk.

Thus, risk may be mathematically expressed as:

Risk [R] = Consequences [C] times Likelihood [L] or C x L

Likelihood can be further defined in terms of a specific vulnerability [V] that is exploited by a specific adversary or threat [T]. Each of these events is a probability. Hence, Likelihood is a conditional probability expressed as

[L] = p[T] x p[V]

In this case, the threat is any indication, circumstance, or event with the potential to cause loss of or damage to an asset. In its traditional definition, a threat is a product of intention and capability of an adversary, both manmade and natural, to undertake an action which would be detrimental to an asset.

A vulnerability is a weakness that can be exploited by an adversary to gain access to an asset. For example, vulnerabilities might include, but are not limited to, building characteristics, personal behaviors, properties of equipment, and security practices and procedures.

Thus, risk may be defined more fully as the product of consequences or impact [I] to the owner in case of loss or damage to a valued asset, and the likelihood that the asset may be damaged or destroyed by a particular adversary exploiting a specific vulnerability.

The equation is shown as

$$R = I \times p[T] \times p[V]$$

With this explanation, the next section addresses the model criteria developed to measure vulnerability assessments. This is a product created by subject matter experts to define a baseline vulnerability assessment methodology that is most appropriate for assets in the community.

2.2 MODEL CRITERIA FOR VULNERABILITY ASSESSMENTS

To equally evaluate all methodologies, criteria for this evaluation needed to be established. A group of SMEs developed the ten evaluation criteria shown in Table 1. These criteria were developed based on the essential elements of an effective risk evaluation. In other words, the SMEs determined they would include the indicated ten major areas if allowed to develop their own methodology. This is the baseline model criteria against which each submitted methodology was compared.

In addition, these evaluation criteria were weighted using a forced choice pairwise comparison system known as Expert Choice. While the initial assessment only assessed if each methodology considered the criteria when determining risk, a subsequent assessment indicated the relative importance or weight of each criteria and subcriteria in determining risk.

To assist U.S. government departments and agencies in determining their vulnerabilities and allocating their available resources to provide protection from terrorist activity, the Department of Homeland Security Office for Domestic Preparedness asked Booz Allen Hamilton to compare vulnerability assessment methodologies and to provide a '"consumer reports" type of assessment of available methodologies. In August 2002, ODP Special Projects released "Sources Sought for Vulnerability Assessments of Physical Assets for the Office of Domestic Preparedness." Forty-four companies responded by submitting information describing their capabilities for review, agreeing to allow Booz Allen to review their submissions. Finally, representatives of fourteen of these companies participated in a one-day, subject matter expert workshop to validate common, standard criteria for assessment of each methodology.

In the development of criteria, subject matter experts concluded that vulnerability assessments were only part of the true requirement, and that the methodologies should be assessed based on their usefulness for risk assessments. Simply stated, risk is the

potential for damage or loss of some valued entity needed in the performance of the organizational mission. It is composed of two factors, the consequence of the loss of the valued entity or asset, and the likelihood that this loss could or would actually occur.

The following table shows the ten criteria developed by the subject matter experts. They represent the ten most desirable characteristics of a risk assessment methodology.

Ten Risk Methodology Evaluation Criteria

- **Clearly Identify the Infrastructure Sector Being Assessed**
- **Specify the Type of Security Discipline Addressed, e.g. Physical, Information, Operations**
- **Collect Specific Data Pertaining to Each Asset**
- **Identify Critical/Key Assets to be Protected**
- **Determine the Mission Impact of the Loss or Damage of that Asset**
- **Conduct a Threat Analysis and Perform Assessment for Specific Assets**
- **Perform a Vulnerability Analysis and Assessment to Specific Threats**
- **Conduct Analytical Risk Assessment and Determine Priorities for each Asset**
- **Be Relatively Low Cost to Train and Conduct**
- **Make Specific, Concrete Recommendations Concerning Countermeasures**

Table 1

Risk is the likelihood that a specific undesirable event will occur given the right set of circumstances under some scenario. This assessment will be based on an integrated analysis of the data previously collected on critical/key assets, real threats, and identified vulnerabilities. The risk assessment process will begin with a baseline review of the existing risk under present conditions to include countermeasures already in place. The level of risk will be based on the value placed on the asset by its owner; the consequence, impact, or adverse effect of loss or damage to the asset; and the likelihood that a specific vulnerability will be exploited by a specific threat. Risk will be expressed as a function of the likelihood of a given threat exploiting a given vulnerability, the magnitude of the impact should a threat successfully exploit the vulnerability, and the criticality of the critical/key asset being attacked. If a potential threat is found that is likely to exploit an identified vulnerability, the asset will be subject to a certain level of risk.

The likelihood of successful exploitation will be determined based on the resources required to exploit the vulnerability, the threat's motivation to exploit the vulnerability,

and the planned or existing countermeasures in place to defeat the exploitation attempt. To determine the relative degree of risk, the probability or likelihood of occurrence of the undesirable event must be estimated. The probability and expected impact together will be considered in estimating the risk level. Impact can be expressed either qualitatively or quantitatively.

When vulnerabilities are high and the threat is evident, the risk of exploitation is greater. As a result, a higher priority for asset protection should be considered. When the vulnerability is low and the terrorist has little capability to exploit the vulnerability, now or in the future, the risk is less and the priority for new countermeasures for this asset will be lower. The areas of greatest risk will become the basis for deciding where to focus additional countermeasures and what kind of countermeasures to apply.

The acceptable level of risk will not be determined by a formula. Risk levels will vary with time, circumstances, and management attitude toward risk in the organizational environment. The asset managers or owners of the critical/key asset will ultimately decide what constitutes an acceptable level of risk. Judgments made regarding impact, threat, and vulnerability will help determine risk priorities.

In the first portion of this research, subject matter experts using the criteria listed above evaluated forty-four submissions from different companies. While the SMEs agreed that these ten criteria were important, they did not agree on the relative importance, or that an effective risk assessment methodology must perform all ten in every situation. Further, it is not clear that each of these methodologies is usable by state and local governments without some special training or equipment.

Thus the first phase of this effort completed a developmental test for these methodologies, narrowing the field to those that successfully accomplished some portion of all ten criteria. A natural follow-on to this phase is Phase II, where selected methodologies are tested in an operational environment. This test would be designed to answer the question, “Can you accomplish a reasonable assessment without fully developing all ten criteria?” Such an operational test would require a test bed to compare the results obtained by using various methodologies with a known standard.

2.3 SUMMARY

Phase I of the current support to the Department of Homeland Security identified a group of methodologies that could be used by state and local governments to assess the risk associated with various assets within their areas of responsibility. However, it did not test the usability of these methodologies or their effectiveness in a field environment. Such an operational test is essential to truly determine which methodologies are best used by state and local governments to allocate their scarce resources and best improve their overall security.

3.0 PROCESS

The "Study of Vulnerability Assessment Methodologies, Automated Tools, Software and Emerging Technologies" for physical assets used a three-phase approach, to include an analysis of various vulnerability assessment methodologies, automated tools, software and emerging vulnerability assessment technologies.

Phase I consisted of cataloguing, to the extent possible, vulnerability assessment methodologies available in the commercial. All the responses received in the ODP Special Projects "Sources Sought for Vulnerability Assessments of Physical Assets for the Office of Domestic Preparedness" were examined and evaluated against the model criteria to set a baseline for further analysis. The responses also established a library of vulnerability assessment methodologies.

This Phase was designed to

- Develop criteria for analysis of the various methodologies and rate each methodology on the developed criteria
- Analyze and facilitate responses concerning government owned or used vulnerability assessment methodologies, automated tools, software and emerging VA technologies and clearly map those capabilities and any overlaps of capabilities provided by the methodologies, automated tools, software and emerging technologies
- List advantages and disadvantages of using particular methodologies, automated tools, software and emerging technologies to assess different types of assets, i.e. stadiums, public buildings, factories, water systems
- Identify evidence that methodologies, automated tools, software and emerging technologies can perform as advertised, if any.

SPECIFIC DELIVERABLES:

- The criteria used to assess each methodology, software, or tool for applicability of assessing individual asset types
- A common lexicon or glossary of vulnerability assessment and risk assessment terms
- The results of synthesizing information gathered and the science of risk assessment and vulnerability assessment
- The best process for selecting and validating VA tools

Additional deliverables:

- An automated software tool on the enclosed CD-ROM to enable the reader to assess additional methodologies
- A Help Guide to assist the reader in utilizing the IARDstick tool

3.1 SUBJECT MATTER EXPERTS

In addition to the Booz Allen Hamilton team of subject matter experts who developed the model criteria for what an effective vulnerability assessment methodology should consider, an invitation was sent to the Sources Sought respondents to further enhance the study. Fourteen experts currently working in the field of risk assessments agreed to share their expertise, thus adding validity and credibility to the overall project.

They attended a daylong seminar on February 21, 2003 at a Booz Allen Hamilton facility. These vulnerability assessment providers were able to evaluate and comment on the criteria applied to the submitted methodologies. They used the Expert Choice pair-wise decision support system to validate the selected criteria. Seminar participants were impressed with the depth of thought and research put into the model methodology and lauded the process used to conduct the study.

The companies represented were

- Digital Sandbox, Inc.
- DynCorp Systems and Solutions LLC
- EDS Security and Privacy Professional Services
- Gage-Babcock & Associates, Inc.
- Idealsoft, Inc./ ASVACO
- Management Systems Designers, Inc.
- NCI Information Systems, Inc.
- Premier Technology Group, Inc.
- Protections Strategies, Inc.
- RISKWATCH, Inc.
- Standing Stone Consulting, Inc.
- TECTONIC Engineering & Surveying Consultants
- Titan
- UTD, Inc.

3.2 EXPERT CHOICE

Expert Choice (EC) is a decision support tool designed to help groups enhance the quality of their decisions. It is not a polling device. It brings structure to the decision-making process. In addition to eliciting ideas, feelings, emotions, and the judgments of

stakeholders, it represents those judgments as meaningful numbers; synthesizes the results; and analyzes the sensitivity of those judgments to changes.

Through the use of pairwise comparisons**,** the relative importance of each criterion is calculated. Participants compare two pieces of criteria and decide which one, in their view, is more important. Using remote controls, participants then assign a number (1-9) on the degree of importance. Once all pairwise comparisons are made, EC calculates the results and produces a ranking of criteria.

Validation of the mathematics behind the process is vital. The results are calculated based on the Analytic Hierarchy Process (AHP) – this process has been used by government organizations and private corporations in the United States and around the world, including, the Department of Defense, the Department of Veterans Affairs, the Department of State, Xerox, Merck, and General Electric.

The EC session is facilitated. Votes are analyzed and discussed in real time. Participants are free to state their opinions and change their minds – and votes – if they so desire. Regardless of whether votes change, participants are afforded the opportunity to hear reasons why others voted the way they did. Participants have a better understanding of each other's perspectives, knowledge base, and interpretations. Expert Choice helped to organize the thought process, facilitate discussion, calculate results, and improve the decision process.

3.3 IARDSTICK

The Infrastructure Assurance Readiness Decision stick (IARDstick) is a software tool developed by Booz Allen Hamilton. It is a proven methodology with a corresponding software application that enables organizations to assess readiness posture of any aspect of a government or private sector organization. The IARDstick methodology provides features that enable tailoring of the approach and implementation to meet any organization's specific mission requirements. IARDstick capitalizes on the existing proven framework of the Booz Allen Hamilton Information Technology Metrics Program. It was developed in close coordination with the Department of Defense Joint Staff and Military Services to provide a comprehensive set of field-tested, mission-based performance measures.

IARDstick provides the mechanism for the initial and continuous assessment of an organization's IA readiness posture. However, it is a flexible program that encourages long-term acceptance, consistency, and effectiveness.

It is important to note that IARDstick can be used to address any specific subject area. For example, for an organization whose primary responsibility is associated with cyber

security, IARDstick could be tailored to focus solely on cyber security-related metrics; similarly, IARDstick could be used to focus solely on Intrusion Detection Systems (IDS) or Certification and Accreditation (C&A). Although the individual metrics can be readily and easily tailored, the supporting business principles and model utility remain constant.

It is because of its flexibility and applicability, this tool was used as the comparison vehicle for the vulnerability assessment methodology project.

IARDstick provided a metrics-based model for a consistent basis of comparative analysis of the submitted vulnerability assessment methodologies. The model's quantitative results could also be used to indicate deficiencies within the specific methodology, thus serving as justification for distinguishing between competing methodologies.

A CD-ROM included with this report contains two versions of the IARDstick software tool. The IARDstick tool icons are labeled “DHS Locked” and “DHS Unlocked.” The DHS Locked tool enables the reader to assess additional methodologies using the same metrics as used in this study. The DHS Unlocked version provides access to the IARDstick tool with the weights inserted, however, the criteria weights may be changed in this version. To utilize this software, it must be copied on the user’s computer. Once copied on the user’s computer, right click on the appropriate icon. Then click on Properties. Next the user must un-check the “read only” Attributes block. The software tool is now ready for use. A Help Guide for the IARDstick tool is also provided to allow locally determined criteria weights to be placed in the tool as developed by the reader. In doing so, it is important to remember not to compare assessments using the unlocked version against assessments using the locked version because the baseline weighting criteria will be dissimilar.

3.4 DISCUSSION

Forty-eight responses were received to the Sources Sought: thirty non-proprietary, eighteen proprietary. Most proprietary sources elected to redact proprietary markings. Four elected not to do so. Hence, forty-four submissions were considered in this study. It should be noted that the preponderance of the documents received were marketing documents. Those 14 companies that provided subject matter experts to validate the vulnerability assessment priorities and weights were telephonically contacted and asked specifically about each of the measured criteria of the methodology used by their company.

The assessment team also found sufficient information to make some level of assessment for twenty-four public (federal, state, and local government) methodologies.

- On December 18, 2002, five SMEs from Booz Allen completed a final list of ten evaluation criteria to be used to assess and compare submissions to the Sources Sought (Table 1).
- On that same date, these SMEs, using the above list of evaluation criteria and a forced choice, pairwise comparison methodology, called Expert Choice, developed relative weights for each criterion. However, these weights were not revealed to the SMEs to prevent unintentional influence on their evaluations.
- In January 2003, the first group of SMEs, using a software called IARDstick, and blind to the developed weights of each evaluation criteria, completed independent assessments of the forty-four private responses to the Sources Sought. A subgroup of SMEs also assessed the twenty-four public methodologies identified by the study team. Based on the weights of the criteria and the degree to which each methodology satisfied that criteria, each methodology received a score, which was used to compare that methodology to all other submitted or obtained methodologies.
- In February 2003, a second group of fourteen SMEs from participating companies reviewed the evaluation criteria. This group concluded that the evaluation criteria were correct, comprehensive and useful for assessing each of the government and private sector methodologies under consideration. This second group of SMEs, again using Expert Choice, replicated the criteria weightings derived by the first group of SMEs. There were no significant differences between the two groups.
- Generally, sector specific methodologies provided an excellent result for the intended sector. However, utility of these methodologies for sectors other than that for which it was specifically designed, was cumbersome and in most cases would require extensive modification to be fully effective.

It was determined that there is a need for commonly accepted terminology when considering vulnerability assessments or risk assessments to lessen confusion. For example, *risk* is defined by the Critical Infrastructure Assurance Office of the Department of Homeland Security as “the probability that a particular critical infrastructure’s vulnerability being exploited by a particular threat weighted by the impact of that exploitation.” RAM-Wsm defines *risk* as “a measure of the potential damage to or loss of an asset based on the probability of an undesirable occurrence.” And, William D. Rowe, PhD, in An Anatomy of Risk defines it as, “the potential for realization of unwanted, negative consequences of an event.” Three separate respected authorities each define risk in a slightly different manner. In these definitions risk is characterized as a probability, a measure and as a potential. Each of the three definitions is accurate, however, each could be interpreted differently. For the skilled assessor, these variations are of minor concern, but for an individual without experience in conducting risk or vulnerability assessments, these differences could be a source of confusion.

Additionally, it was found that individuals and some companies use certain terms with different meanings interchangeably, such as *risk* and *vulnerability*. Some used the terms *Risk Assessment* and *Vulnerability Assessment* interchangeably. However, it should be noted that the vulnerability assessment is only one part of the overall risk assessment. The risk assessment, as was previously noted in Section 2.1 of this report, is determined by multiplying the consequences of an unwanted event by the likelihood of that event occurring. The likelihood is determined by multiplying the level of threat by the vulnerability or weakness of the asset to be protected. The criticality of the asset, the impact of the loss of that asset and the potential threats to the asset are all be essential to assessing the overall risk to an asset. These elements will also assist in the prioritization of assets, but they are not specifically germane to the determination of the vulnerability of the asset.

The glossary of terms (Appendix A) included with this report should be further standardized during Phase II, as the process is clarified.

It is important to understand that this report does not provide a listing of recommended companies, which provide vulnerability assessments. What was revealed from the process is that there appears to be a core methodology used. A baseline criteria was developed against which agencies may compare companies that offer vulnerability assessment, by using the DHS Locked version of the IARDstick tool. The DHS Unlocked version provides an opportunity to assess a company against the agency-weighted criteria prior to making a commitment for assessment.

4.0 CONCLUSIONS

The following represent the major findings and conclusions that result from this analysis.

First, the most robust methodologies do not solely focus on one sector of the economy. Instead, they seem to have a core methodology that is applicable without regard to the economic sector. If more specific results are desired, a sector specific module is added to the core methodology. Single sector methodologies, such as RAM-Wsm, are excellent for that particular infrastructure (water systems), however to use this type of methodology for other infrastructures generally requires extensive modification.

Second, the quality of the assessor in all cases is telling. In other words, a mediocre methodology, well applied by someone with great knowledge and experience will yield an acceptable result and, thus, provide a basis for great improvements in security. Conversely, a superb methodology, applied by those with little or no training and experience, will not produce very useful results. Checklists, while useful, do not replace the need for careful assessment by an experienced and well-trained assessor.

Third, while all methodologies determined some measure of risk, often implicitly, few actually calculated a numerical value for that risk. Clearly, the numerical values assigned were in nearly every case ordinal, at best. Thus, those methodologies that did calculate a risk value did so using mathematical techniques that were not supported by the scaling assumptions involved. In all mathematical calculations, the scales presented only order, not relative values. Hence, a reduction in risk by one unit-- for example, from 23 to 22 -- may or may not be comparable to a similar reduction in risk by one unit from 5 to 4.

Fourth, the training required to accurately use one of these methodologies varied greatly in time and cost. Some were designed for the assessor to read the handbook and use that information to complete the assessment. Others required time consuming and expensive training courses to learn the methodology. In the opinions of the SMEs, the quality and diligence of the assessor is as important or more important than the specific methodology used. A well-qualified and knowledgeable assessor minimizes the need for additional expensive training, is able to conduct the assessment more quickly, and will provide a more accurate, useful assessment. This will enable the user to more effectively assess vulnerability or risk.

Additional phases of this project would better determine the effectiveness of these various methodologies.

TERM	DEFINITION
Acceptable Risk	The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific system (CIAO)
Accessibility	The quality of being assessable; that which may be approached or entered (Webster's Unabridged Dictionary)
Accident	Possible result of a deviation (USCG)
Accountability	The principle that responsibilities for ownership and/or oversight of resources are explicitly assigned and that assignees are answerable to proper authorities for stewardship of resources under their control (CIAO)
Adversary	Any individual, group, organization or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. (ARM)
Analytical Risk Management (ARM)	The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost
Asset	Anything of value: people, information, equipment, facilities, activities/operations, which needs to be protected (e-envoy.gov.uk)
Assurance	The confidence that may be held in the security provided by a system, product or process (e-envoy)
Attack	A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it (CIAO)
Audit	The process of reviewing and evaluating compliance with applicable directives and regulations and/or the examination of records or accounts to check their accuracy (Security Ed. Glossary)
Availability	The ability to have access to mission essential infrastructure resource elements when required by the mission and core supporting processes (CIAO)

Benefit	Amount of risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities (ARM)
Capability	The ability of a suitably organized, trained, and equipped entity to address, penetrate, or alter systems and/or to disrupt, deny or destroy all or part of a critical infrastructure (CIAO) A measure of the degree to which a system is able to satisfy its performance objectives (*An Anatomy of Risk* by William E. Rowe, Ph.D.)
Consequence Management	Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by (the consequences of terrorism) [a disrupting event] (CIAO)
Contingency Plan	Plan maintained for emergency response, backup operations and post-disaster recovery for a system (or an entity) to ensure availability of critical resources and facilitate the continuity of operations in an emergency (CIAO)
Continuity of Core Business Function	Strategies to mitigate risks and alternative methods for ensuring the continuation of the entity's business functions, e.g. financial management, information technology, operations support, critical training and the primary reason(s) for being for the entity
Continuity of Operations	Those plans and/or processes designed to ensure a viable capability exists to continue essential functions across a wide range of potential emergencies. The focus of this type of planning is to ensure the survivability of critical department/agency/entity functions (FEMA)

Cost	Tangible items, such as money, equipment and operational expenses; and, intangibles such as lost productivity, morale, etc. A result of a specific action that constitutes a *decrease* in the production possibilities or welfare level of society (*An Anatomy of Risk* by William D. Rowe, Ph.D.)
Countermeasure	An action taken or physical entity principally used to reduce or eliminate one or more vulnerabilities (ARM)
Critical Asset	An asset that supports national security, national economic security, and/or crucial public health and safety activities (CIAO)
Critical Infrastructure	"Physical or cyber-based system essential to the minimum operations of the economy and government" (PDD-63 CIAO)
Critical Infrastructures	Those systems and assets-both physical and cyber-so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety
Decision Tree	A device used to portray alternative courses of action and relate them to alternative decisions showing all consequences of the decision. The tree represents alternative courses or series of actions related to a previous decision. (*An Anatomy of Risk* by William D. Rowe, Ph.D.)
Defeat	To overcome or vanquish; to beat; to prevent the success of; overpower; foil (Webster's Unabridged Dictionary)
Defend	To guard from attacked; to protect by opposition to resistance; to prevent from being injured or destroyed (Webster's Unabridged Dictionary)
Deny	To refuse access to (Webster's Unabridged Dictionary)
Detect	To discover; to find out (Webster's Unabridged Dictionary)
Deter	To discourage or keep (a person) from doing something through fear, anxiety, doubt, etc. (Webster's Unabridged Dictionary)

Disaster	A crisis event that surpasses the ability of an individual, community or society to control or recover from its consequences (NOAA)
Emergency	The most serious event and consists of any unwanted operational, civil, natural-phenomenon, or security occurrence which could endanger or adversely affect people, property, or the environment. (Security Education Glossary)
Emergency Management	The development, coordination and direction of planning, preparedness, and readiness assurance activities (Security Education Glossary)
Emergency Plan	A brief, clear and concise description of the overall emergency organization, designation of responsibilities, and descriptions of the procedures, including notifications, involved in coping with any or all aspects of a potential credible emergency (Security Education Glossary)
Emergency Preparedness	The training of personnel, acquisition and maintenance of resources, and exercising of the plans, procedures, personnel and resources essential for emergency response (Security Education Glossary)
Event	An occurrence, not yet assessed, that may affect the performance of a system (or an entity) (CIAO) Any real-time occurrence or significant deviation from planned or expected behavior that could endanger or adversely affect people, property, or the environment (Security Education Glossary)

Exposure (to risk)	The number, types, qualities, and monetary values of various types of property or infrastructure and life that may be subject to an undesirable or injurious hazard event (NOAA) The condition of being vulnerable to some degree to a particular outcome of an activity, if that outcome occurs (*An Anatomy of Risk* by William D. Rowe, Ph.D.)
Hazard	An event or physical condition that has the potential to cause fatalities, injuries, property damage, infrastructure damage, agricultural loss, damage to the environment, interruption of business, or other types of harm or loss (NOAA)
Impact	The amount of loss or damage that can be expected or may be expected from a successful attack of an asset (ARM)
Incident	An occurrence that has been assessed as having an adverse effect of the security of performance of a (critical infrastructure) (CIAO)
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole (CIAO)
Intrusion	Attacks or attempted attacks from outside the security perimeter of (an asset) (CIAO)
Key Asset	An organization, group of organizations, system, or group of systems, the loss of which would have widespread and dire strategic, economic or social impact
Methodology	An open system of procedures (*An Anatomy of Risk* by William D. Rowe, Ph.D.*)*

Natural Disaster	A physical capability with the ability to destroy or incapacitate critical infrastructures. Natural disasters differ from threats due to the absence of intent
Operations Security	The co-mingling of computer, technical counterintelligence security measures developed and implemented to augment traditional security programs (physical security, information or personnel security and communications security) as a means of eliminating or minimizing vulnerabilities that impact on technical programs (classification references omitted)(Security Education Glossary)
Organic Security	Security that is part of the organization itself rather than contracted services
Physical Protection System	Integration of people, procedures, and equipment for the protection of assets or facilities against, theft, sabotage, or other malevolent human attacks (RAM-Wsm)
Physical Security	Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks (CIAO)
Probability	The probability that the system will perform its required functions under given conditions for a specified operating time (*An Anatomy of Risk* by William D. Rowe, Ph.D.*)*
Recover	The likelihood of some event occurring A numerical property attached to an activity or event whereby the likelihood of its future occurrence is expressed or clarified (*An Anatomy of Risk* by William D. Rowe, Ph.D.*)*
Reliability	To get back; to regain; to get back (a position of readiness) (Webster's Unabridged Dictionary)
Restore	To bring back to a former or normal position (Webster's Unabridged Dictionary)

Risk	The likelihood that an event will occur which will cause the loss or diminished use of an asset – a function of asset value and the impact and likelihood of threat and vulnerabilities (e-envoy) The combination of two factors: 1) the value placed on an asset and consequence of an undesired on that asset; 2) the likelihood that a specific vulnerability will be exploited by a specific threat (ARM) The probability that a particular critical infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation (CIAO) *Measure* of the potential damage to or loss of an asset based on the probability of an undesirable occurrence (RAM-Wsm) The potential for realization of unwanted, negative consequences of an event (*An Anatomy of Risk* by William D. Rowe, Ph.D.*)*
Risk Acceptance	Willingness of an individual, group, or society to accept a specific level of risk to obtain some gain or benefit (*An Anatomy of Risk* by William D. Rowe, Ph.D.)
Risk Analysis	See Risk Assessment
Risk Assessment	*Process* of analyzing threats to and vulnerability of a facility, determining the potential for losses, and identifying cost effective corrective measures and residual risk (RAM-Wsm)
Risk Level	A combination of the two factors pertaining to impact of loss and probability of adverse event (ARM)
Risk Management	The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost (ARM)

Threat	Any indication, circumstance, or event that can cause the loss of, damage to, or the denial of an asset (ARM)
Threat Assessment	The process to identify threat categories and adversaries, assessing the intent of each adversary, the capability of each adversary, the frequency of past incidents and an estimation of the threat relative to each critical asset
Vulnerability	Any weakness which can be exploited by an adversary to gain access to an asset (ARM) An exploitable security weakness or deficiency at a facility (RAM-Wsm) The level of exposure of human life, property, and resources to damage from hazards (NOAA) A feature of a system, which, if exploited by an attacker, would enable the attacker to breach security (e-envoy) A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat (CIAO)
Vulnerability Assessment	Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation (CIAO) A systematic evaluation process in which qualitative and/or quantitative techniques are applied to arrive at an effectiveness level for a safeguards and security system to protect specific targets from specific adversaries and their acts. (Security Education Glossary)

ACRONYMS

CIAO – Critical Infrastructure Assurance Office

NOAA – National Oceanographic and Atmospheric Administration

PDD 63 – Presidential Decision Directive 63

RAM-Wsm – Risk Assessment Methodology – Water (Sandia Methodology)

USCG - U.S. Coast Guard

FBO DAILY ISSUE OF AUGUST 08, 2002 FBO #0249
SOURCES SOUGHT

B -- Contracting Officer

Notice Date

8/6/2002

Notice Type

Sources Sought

Contracting Office

Department of Justice, Office of Justice Program, OJP/Acquisition Management Division, 810 Seventh Street NW, Washington, DC, 20531

ZIP Code

20531

Solicitation Number

OJP-2002Q-028

Response Due

9/30/2002

Point of Contact

Janice Waller, Contracting Officer, Phone 202-307-1418, Fax 202-3070086, - Janice Waller, Contracting Officer, Phone 202-307-1418, Fax 202-3070086,

E-Mail Address

wallerj@ojp.usdoj.gov, wallerj@ojp.usdoj.gov

Description

This is a Sources Sought Notice for MARKET RESEARCH ONLY for the Office of Domestic Preparedness. NO SOLICITATION DOCUMENTS EXIST AT THIS TIME. The subject of this research is Vulnerability Assessments as they pertain to state, local and commercial physical assets. The purpose of this Sources Sought is to identify sources of physical asset Vulnerability Assessment providers, equipment, emerging technologies and software/ automated Vulnerability Assessment tools. Responses must be categorized as pertaining to the following categories: Vulnerability Assessment providers, equipment, emerging technologies and software/ automated Vulnerability Assessment tools. The term "vulnerability" is defined as: any weakness in an asset that can be exploited to gain access to, compromise, steal, reduce, deny use of, destroy, kill, maim, poison, infect or otherwise use

against the American people. The term "provider" refers to organizations that provide Vulnerability Assessments (or any part thereof) of physical assets. The term "equipment" refers to any specialized item used to assist individuals or teams in conducting Vulnerability Assessments. The term does not refer to countermeasure items that would be used to mitigate risk once a vulnerability has been exposed (i.e. entry detection systems or security personnel). The term "emerging technologies" refers to products that use technologies that are either under development or have recently been made available to the government or public. The term "software/ automated Vulnerability Assessment tools" refers to applications, databases and other cyber items that would be used to assist individuals or teams in conducting a Vulnerability Assessment, selecting the assessment methodology or determining effective types of countermeasures that could mitigate the risk of exposed vulnerabilities. This is a Sources Sought Notice for MARKET RESEARCH ONLY. NO SOLICITATION DOCUMENTS EXIST AT THIS TIME. The government has no plans on purchasing Vulnerability Assessment products or services at this time. Responses shall include your company's name, capabilities, product and service category (Vulnerability Assessment providers, equipment, emerging technologies or software/ automated Vulnerability Assessment tools) for each response product or service provided. Companies responding shall also provide a synopsis of their company experience in Vulnerability Assessments and related fields.

Place of Performance

Address: U.S. Department of Justice, Office of Justice Programs, 810 7th Street, NW, Washington, DC 20531

Zip Code: 20531

Country: USA

Record

SN00133158-W 20020808/020806213335 (fbodaily.com)

Source

FedBizOpps.gov Link to This Notice
(http://www2.eps.gov/spg/DOJ/LEAA5/LEAA5/OJP-2002Q-028/listing.html)
(may not be valid after Archive Date)

Number	Government Name	Mission/Sector	Security Category or Discipline	Data Collection	Asset Categories	Asset Loss Consquences	Threats	Vulnerabilities	Risk	Costs	CM Recommendations
1	ASDWA Security Vulnerability Self Assessment Guide										
2	The Buddy System										
3	Business Continuity Management										
4	California Highway Patrol Crime Prevention Plan										
5	Colorado Critical Infrastructure/Key Asset Assessment Methodology										
6	DOJ Assessment and Strategy Development Tool Kit										
7	Florida Domestic Security Risk Assessment Model										
8	Guidelines for Analyzing/Managing Security Vulnerabilities of Fixed Chemical Sites										
9	Method to Assess the Vulnerability of U.S. Chemical Facilites										
10	Military Standard 882-D										
11	Naval Criminal Investigative Service (NCIS) ThreatPlanner										
12	North Carolina Terrorism Vulnerability Self-Assessment										
13	Port Facility Vulnerability Assessment										
14	Probabilistic Risk Assessment Methodolgy of the Nuclear Regulatory Commission										
15	Risk Management for Non-Profit Organizations										
16	Sandia National Lab Community Vulnerability Assessment Methodology										
17	Sandia National Lab RADTRAN 5										
18	Sandia National Lab Vulnerability Assessment Methodology for Water Surety (RAM-W)										
19	Sandia National Lab VAM-CF										
20	SmartRISK										
21	USAF Operational Risk Management										
22	US Coast Guard Risk Assessment Project Management										
23	US Coast Guard Risk-based Decision Making										
24	Virginia Statewide Terrorism Target Assessment Survey										

Indicates "No" or "No Information Provided"

Indicates that the Methodology Does Address this Criteria

Association of State Drinking Water Administrators (ASDWA) Security Vulnerability Self Assessment Guide for Small Drinking Water Systems

This is a checklist generated self-assessment for physical water systems facilities.

Mission/Sector. This guide is specifically designed for small water systems.

Security Category/Discipline. The checklist speaks to physical, personnel and cyber security in general.

Data Collection.

Asset Categories. The checklist addresses people, information equipment and facilities in general terms.

Asset Loss Consequences. Disruption is a consideration.

Threats. The checklist is specifically attuned to tampering/threat of contamination, bio/chem/explosive

Vulnerability.

Risk.

Resource Costs.

Countermeasure Recommendations.

The Buddy System

This is survey-based risk management software built on a relational database, founded on Navy and Coast Guard methodology. The datasets contain pairings between related threats, vulnerabilities and countermeasures.

Mission/Sector. The software comes with ready-to-use datasets or the user may customize data. From the list of agencies that have used the product (Dept of Energy, Dept of Transportation, Navy/Coast Guard, State of TX, NY State Gas, PDVSA Oil Company), it is assumed that the applicable sectors may include Gas, Oil and Energy, Transportation, Water, non-government critical and inherently governmental functions.

Security Category/Discipline.

Data Collection. This is accomplished by survey.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk.

Resource Costs. A 2-day training course is included in the cost of the software.

Countermeasure Recommendations. The software provides recommendations in the report; no specifics available.

Business Continuity Management (BCM) Methodology

This methodology addresses identifying and placing a value on the information asset; identifying threats to disclosure, loss or disruption; assessing vulnerabilities (technical and non-technical system weaknesses); and calculating the risk by integrating the threat and vulnerability assessments.

Mission/Sector. This methodology was created especially for financial institutions.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences. This process speaks directly to loss or disruption in the confidentiality, integrity, or availability of financial information.

Threats.

Vulnerability.

Risk. Risk is calculated.

Resource Costs.

Countermeasure Recommendations.

California Highway Patrol Crime Prevention Plan

This plan provides guidelines for awareness, risk assessment and mitigation actions, crime prevention, property security and personal safety. It lists questions for self assessment, mostly directed toward physical security of law enforcement facilities.

Mission/Sector.

Security Category/Discipline. This plan addresses physical/personnel security.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk.

Resource Costs.

Countermeasure Recommendations.

State of Colorado Critical Infrastructure and Key Asset (CIKA) Assessment Methodology

This is a software package that allows the user to self-assess with a numerical 0-5 rating scale based on the following CIKA factors: visibility, value, accessibility, hazard, population, mass casualties, criticality, service disruption, primary function, and geographical impact. The total score provides the criticality/vulnerability rating for the identified critical infrastructure and key asset.

Mission/Sector. This software package is designed for critical infrastructure and key assets.

Security Category/Discipline.

Data Collection. Data is subjective self-assessment. There is a qualitative area provided to set rationale for selecting the quantitative 0-5 numeric rating for factors. A report is generated once input is completed.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk. Risk is estimated.

Resource Costs.

Countermeasure Recommendations.

DOJ Assessment and Strategy Development Took Kit

This is a program guideline developed by the Department of Justice, Office for State and Local Domestic Preparedness Support.

Mission/Sector. Designed to be applied to all mission/sectors to identify potential targets and conduct vulnerability assessments for baseline grant funding for State Domestic Preparedness Equipment.

Security Category/Discipline.

Data Collection. Data is subjective self-assessment.

Asset Categories. These guidelines consider people, facility, and value.

Asset Loss Consequences. Death/injury, damage/destruction to facility, and general economic disruption are addressed.

Threats. This program uses a revised DoD terrorist threat analysis methodology.

Vulnerability. The vulnerability assessment considers visibility, attractiveness, criticality, value, access, target threat of hazard, population capacity, collateral mass casualties, and places these on a 0-5 numeric scale. There is also a checklist assessment for Public Health, which is integrated to determine a risk profile. The capabilities and needs assessment could be construed as lead in for countermeasures determination.

Risk. Risk is estimated using a risk assessment matrix.

Resource Costs.

Countermeasure Recommendations.

Florida Domestic Security Risk Assessment Model

This model was designed to serve as a working instrument to be used by Florida's Regional Domestic Security Task Forces, public and private sector organizations charges with protecting Florida's citizens, facilities, and infrastructure from terrorist attack.

Mission/Sector. The scope of this model is facilities and other venues, which are likely terrorist targets.

Security Category/Discipline. This addresses physical security; no mention of personnel, cyber or operations security.

Data Collection. This model does not specifically address data collection other than site visit and interaction with personnel from the target site.

Asset Categories. Facilities are mentioned; other venues are subject to interpretation.

Asset Loss Consequences. This model takes into consideration death and injury, economic impact, environmental impact, impact on critical infrastructure and symbolic effect. There is a numeric 1-5 scale applied to consequence assessment analysis in the previously listed factors.

Threats. The likelihood is based on critical intelligence and/or attacks on targets of a similar nature.

Vulnerability. This model addresses availability, accessibility, organic security and target design/construction. There is a numeric 1-5 scale applied to vulnerability assessment analysis in the previously listed factors.

Risk. The methodology uses a numeric scale to estimate risk.

Resource Costs.

Countermeasure Recommendations. After an on-site review, if appropriate, recommendations for improvements in policy, procedures, and structure are provided.

Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites

These guidelines are provided by the Center for Chemical Process Safety, American Institute of Chemical Engineers.

Mission/Sector. This is specifically directed to fixed chemical sites.

Security Category/Discipline. These guidelines address physical, personnel, cyber and operations security in a roundabout way, although the emphasis is on physical.

Data Collection. While data collection is not specifically mentioned, the risk assessment is qualitative in nature, not quantitative.

Asset Categories. The categories addressed are people, chemicals, information, environment, equipment, facilities and activities/operations. It does speak to attractiveness.

Asset Loss Consequences. These guidelines speak to loss of containment, theft or misuse, contamination or spoilage, and degradation of assets or infrastructure and/or business function.

Threats. These guidelines were developed specifically in response to terrorist attacks. It includes internal/external threats.

Vulnerability. Current countermeasures are discussed with specific mention of deter, detect, and delay as an overall management strategy, as well as the layers of protection concept. Manpower, technology/equipment, procedures/policies, and training /education are incorporated into the countermeasures.

Risk. The analysis supports estimating risk via a methodical process.

Resource Costs.

Countermeasure Recommendations. The Security Vulnerability Analysis (SVA) makes recommendations that follow the process of deter, detect, delay, diminish, mitigate and possibly prevent. One assumes this involves manpower, technology/equipment, procedures/policies, and training/education countermeasures, although not specifically mentioned in the guidelines.

Method to Assess the Vulnerability of US Chemical Facilities

This is a prototype vulnerability assessment methodology (VAM) developed by Sandia National Laboratories and the National Institute of Justice. It compares relative security risks and allows for development of recommended measures to reduce risks.

Mission/Sector. This was developed especially for chemical facilities.

Security Category/Discipline. This lends itself to physical, cyber, and operations security.

Data Collection. Data gathered is a combination of quantitative and qualitative.

Asset Categories. The focus is on the facility, equipment and operations/activities.

Asset Loss Consequences. The methodology does consider disruption.

Threats. This methodology covers numerous sub-categories of threats as it pertains to detect, delay and response.

Vulnerability. Availability, accessibility, organic security, and target design/construction, as well as current countermeasures are taken into consideration.

Risk. Risk is estimated.

Resource Costs.

Countermeasure Recommendations. After analysis, recommendations are made for risk reduction/improvements in the areas of physical protection, consequence education, and process control protection.

MIL-STD-882D, Department of Defense (DoD) Standard Practice for System Safety

MIL-STD-882D provides for a standard practice normally identified as system safety. It was designed to manage environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities with a goal of zero mishaps.

Mission/Sector. This process was developed especially for DoD systems, subsystems, equipment, and facilities. However, it is applicable to a number of

Security Category/Discipline. This lends all of the sub-disciplines of security.

Data Collection. Data gathered is qualitative.

Asset Categories. The focus is on the facility, equipment and operations/activities.

Asset Loss Consequences. The methodology develops scenarios, and thereby does consider both destruction of the asset as well as disruption.

Threats. This methodology covers numerous sub-categories of hazards which equate to threats (natural vs man-made, but applicable as written) as they pertain to an asset.

Vulnerability. Estimates of mishap probabilities equate to calculations of vulnerabilities.

Risk. Risk is estimated based on the interaction of the loss consequences and the severity of the vulnerabilities that would allow such loss.

Resource Costs. No estimates of costs of time to learn or training costs are given.

Countermeasure Recommendations. After analysis, recommendations are made for risk reduction/improvements in the areas of physical protection, consequence education, and process control protection.

Naval Criminal Investigative Service (NCIS) ThreatPlanner

This is a software tool used by the Navy and Marine Corps to inventory and assess risk to their defense posture relative to terrorist and criminal threats, specifically attacks against personnel, ships and aircraft. It generates threat assessment information and disseminates it quickly to other potential users, other than for whom the threat assessment was conducted.

Mission/Sector. Limited to military.

Security Category/Discipline. The focus is on operations security.

Data Collection.

Asset Categories. People, equipment/facilities, and activities/operations are considered.

Asset Loss Consequences. This tool considers disruption.

Threats.

Vulnerability.

Risk. Risk is estimated.

Resource Costs. Initial cost $442K with a total of $7,614K over a 7-year period.

Countermeasure Recommendations.

NC Terrorism Vulnerability Self-Assessment

This is a general guideline worksheet for state agencies which allows the user to rate vulnerability on a scale of 1 to 20 (low to high) in the following areas: potential terrorist intentions, specific targeting, visibility, on-site hazards, population, mass casualty potential, security environment, criticality, high risk personnel (critical to continuity of business/government), communications, security/emergency response preparedness, with special emphasis for local health departments/hospitals concerning bio-terrorism response capability.

Mission/Sector. This process could be applied to any sector.

Security Category/Discipline.

Data Collection. Data is qualitative in nature in that assessment is subjective.

Asset Categories. This assessment addresses all asset categories in some manner.

Asset Loss Consequences.

Threats. The assessment loosely takes into account the various sub-categories of threat.

Vulnerability.

Risk.

Resource Costs.

Countermeasure Recommendations.

Port Facility Vulnerability Assessment (Prevention and Suppression of Acts of Terrorism against Shipping)

This is a concept of operations developed by a working group for the International Maritime Safety Committee, which sets guidelines/criteria for assessing port facilities. It describes the need to use a risk analysis tool for understanding, identifying and mitigating vulnerabilities through criticality, threat and vulnerability assessments.

Mission/Sector. This is specifically for port facilities.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk.

Resource Costs.

Countermeasure Recommendations.

Probabilistic Risk Assessment

This Human Reliability Assessment Training Course was designed to train Nuclear Regulatory Commission staff in the use of Probabilistic Risk Assessment techniques to apply to the process of regulating and inspecting nuclear power plants.

Mission/Sector. The process of PRA and Human Reliability Assessment (HRA) can be applied across mission/sectors.

Security Category/Discipline. The emphasis is on personnel security, i.e., human reliability.

Data Collection. The methodology claims to be qualitative in that it describes the human contribution to risk. Data sources include systems information and human action related information. Modeling and simulation are used. It is also quantitative in that the modeling portion is calculated.

Asset Categories. Human reliability is the main focus of this particular type of PRA.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk. The methodology calculates risk.

Resource Costs.

Countermeasure Recommendations.

Risk Management for Non-Profit Organizations

This process is part of a resource guide that describes an overarching view to managing risk within a specific type of agency. The 5-part process incorporates establishing the context, identifying the risk, evaluating and prioritizing the risk, strategies and responses, and monitoring/updating the program.

Mission/Sector. This process is designed for the non-profit sector.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk.

Resource Costs.

Countermeasure Recommendations.

Sandia National Lab Community Vulnerability Assessment Methodology (VAM)

This methodology was developed as a prototype for the Chemical Facility Vulnerability Assessment Project and lays the foundation for a computer-based vulnerability assessment tool. Sandia National Laboratories has a Dams Security Assessment Methodology, Water Supply and Treatment VAM, Vulnerability Analyses and Security Design Reviews for Correctional Facilities, as well as the VAM-CF.

Mission/Sector. This methodology is applicable to all mission/sector categories, in addition to Education, Recreation Venues (parks, museums, tourist attractions, etc) Emergency Facilities, Foreign represented Governments (Embassies, residences, businesses, etc), and special categories such as abortion clinics and religious facilities.

Security Category/Discipline. No specifics were mentioned, although the security categories might be assumed.

Data Collection. No specifics were mentioned about data collection.

Asset Categories. Human life, revenue, vital equipment and vital capabilities are considered as assets.

Asset Loss Consequences. Disruption is alluded to although not specifically mentioned.

Threats. This methodology addresses the range of subcategories within the criteria.

Vulnerability. This methodology addresses availability, accessibility, organic security and target design/construction.

Risk. Risk is a function of severity of consequences of the event, likelihood of adversary attack and effectiveness of the security system.

Resource Costs. Training was mentioned as one of the next steps.

Countermeasure Recommendations. Nothing specific was mentioned.

Sandia National Lab RADTRAN 5

This is a technical manual with descriptions of the calculational models and mathematical and numerical methods used in this specific computer code for transportation risk and consequence assessment. This manual is to be used in conjunction with the RADTRAN Guide.

Mission/Sector. This process was developed especially for analysis of the consequences and risks of radioactive-material transportation via highway, rail, water and air.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk. Risks are estimated with numerical models of exposure pathways, receptor populations, package behavior l accidents, and accident severity and probability. This suggests that it fits the definition of calculating risk, as well.

Resource Costs.

Countermeasure Recommendations.

Sandia National Lab Risk Assessment Methodology for Water Surety (RAM-W)

This is a security risk assessment for water utilities. Some of this notebook contains strategy. A variety of risk management techniques are used, such as fault tree and SCADA—Supervisory Control and Data Acquisition system.

Mission/Sector. Designed for the water sector.

Security Category/Discipline. Physical, cyber, operations, and personnel are considered.

Data Collection. Qualitative data is gathered.

Asset Categories. This methodology considers people, facilities, equipment, and processes.

Asset Loss Consequences. Loss of lives, number of illnesses, loss of critical customers, economic losses, and loss of public confidence are addressed. A matrix is used to determine consequence loss.

Threats. This methodology takes into consideration threat type, tactic mode, capabilities, threat level and likelihood as well as insider/outsider attributes.

Vulnerability. Existing countermeasures to detect, delay and respond are identified.

Risk. Risk is calculated.

Resource Costs.

Countermeasure Recommendations. This is a part of the risk reduction concept that includes detection, delay and response elements to include manpower, procedures and policies, technology/equipment, and training /education countermeasures.

Sandia National Lab VAM-CF

This methodology is a systematic procedure, a tool to aid in making consistent risk-based analyses.

Mission/Sector. This assessment methodology is specifically for chemical facilities and transport activities.

Security Category/Discipline. The emphasis is on physical security although cyber protection is mentioned.

Data Collection. Information is gathered via surveys and worksheets focusing on the detection, delay, response and safety/mitigation aspects of paths. Adversary sequence diagrams are the foundation for the analysis. A facility characterization matrix is used to identify critical areas for analysis.

Asset Categories. Facilities are screened and prioritized based on estimated population within the potentially impacted area.

Asset Loss Consequences. A table to determine the severity of the attack is used; levels are designated based on the number of people potentially impacted.

Threats. This methodology addresses physical security to include attacks by criminals and terrorists. It views type, tactics, and capabilities. There is a basic assumption that the knowledgeable insider is the probably the greatest threat.

Vulnerability. The methodology estimates the attack potential in light of existence, capability, history/intent, motivation, targeting, attractiveness and accessibility.

Risk. This methodology estimates and calculate risk.

Resource Costs.

Countermeasure Recommendations. The likelihood of adversary success is calculated and physical and cyber recommendations are provided.

SmartRISK

This is a software product used by EPA highlighting exposure models in spreadsheets for calculating risk.

Mission/Sector.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk. Risk is calculated.

Resource Costs.

Countermeasure Recommendations.

USAF Operational Risk Management (ORM)

This is a process used by the Air Force to detect, assess and control risk while enhancing performance and maximizing combat capabilities. It is applied to tasks, missions and activities. This 6-step process identifies the hazard(s), assesses the risk, analyzes the risk control measures, makes control decisions, implements risk controls, and supervises/reviews.

Mission/Sector.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk. Risk is calculated via a pre-designed risk assessment matrix.

Resource Costs. The process is self-explanatory; no mention of costs.

Countermeasure Recommendations. The process is designed to provide control of risk.

US Coast Guard Risk Assessment (RA) Project Management

This is a process used to select an approach. The guidelines define the scope of the risk assessment, identifies the stakeholders and RA team, sets the preparation phase and how to facilitate/document meetings and write an RA report, as well as validate the process and data and evaluate the recommendations. There is also a section that provides information to review a risk assessment completed by another entity.

Mission/Sector. This process does not specifically mention a sector, although one may assume transportation.

Security Category/Discipline.

Data Collection. This process simply states that data must be collected and organized before making the report.

Asset Categories.

Asset Loss Consequences. The process requires definition of public/personal injury, equipment/property/environmental damage, revenue loss and community relations.

Threats.

Vulnerability.

Risk. The process defines the limits of risk in terms of overall activity, operations, functions and components. It stipulates that the risk assessment itself should be validated via historical data and previously conducted risk assessments.

Resource Costs.

Countermeasure Recommendations. This process does not specifically address manpower, technology/equipment, procedures and policies or training and education countermeasures. It states that recommendations should be the most effective and efficient way of meeting the risk-related goals for the activity/system; be implemented in a timely manner; and provide a cost-benefit analysis.

US Coast Guard Risk-based Decision Making

This process is used specifically in the transportation sector managing port and waterway operations. This is more a concept of operations than a methodology.

Mission/Sector. Primarily, this involves a small portion of the transportation sector, specifically port and waterway operations.

Security Category/Discipline. The process can be applied to physical, personnel, cyber and operations security, although it is not specifically mentioned.

Data Collection. No mention of data collection. However, to identify, measure and evaluate risk, one can assume data is collected.

Asset Categories. The process is geared towards eliminating or controlling hazards.

Asset Loss Consequences. The emphasis is to reduce the risk to an acceptable level if elimination is not possible. Loss being financial, physical or something such as technical or schedule risk.

Threats. The process alludes to “that which will cause disruption.”

Vulnerability. Does not specifically mention vulnerabilities.

Risk. The process focuses on risk management factors: probability, consequence and sensitivity, and therefore estimates risk.

Resource Costs. The process states that proper training and procedures, as well as technology, will reduce the risk. No costs mentioned.

Countermeasure Recommendations. The process alludes to proper selection and full integration of measures with commitment to risk management as a necessity. If hazards cannot be eliminated, then reduce the risk to an acceptable limit.

Virginia Statewide Terrorism Target Assessment Survey

This is a potential terrorist target assessment document used by law enforcement for location or public event. It addresses the following criteria on a 0-5 point scale: visibility, criticality, value, access, threat of hazard, population involved, potential collateral mass casualties.

Mission/Sector.

Security Category/Discipline.

Data Collection.

Asset Categories.

Asset Loss Consequences.

Threats.

Vulnerability.

Risk.

Resource Costs.

Countermeasure Recommendations.