EPA 550-R97-003
December 1997

Security Study

An Analysis of the Terrorist Risk Associated with the Public Availability of Offsite Consequence Analysis Data under EPA's Risk Management Program Regulations

Table of Contents

List of Appendices

Introduction

Background

Clean Air Act §112(r) required EPA to publish regulations focusing on the prevention of chemical accidents. On June 20, 1996, EPA published the final rule for Risk Management Programs. An estimated 64,000 facilities are subject to this regulation based on the quantity of regulated substances they have on-site. These facilities will be required to implement a Risk Management Program and submit a summary of the program, the risk management plan (RMP), to a central location specified by EPA.

The RMP (which CAA section 112(r) requires must be available to the public, except in the case of confidential business information) consist of four elements:

- A hazard assessment that includes a history of accidental releases and an offsite consequence analysis (OCA) describing the potential impacts that an accidental release could have on the public and the environment around the facility;
- A prevention program that includes operating procedures, employee training, hazard evaluation, and other activities designed to improve safety at the facility and thus reduce the likelihood of an accident;
- An emergency response program that ensures that either facility employees or public responders are prepared to deal with any accidents that do occur and thus minimize the consequences; and
- A facility registration section and executive summary.

This report focuses on the OCA and the individual data elements that will be included in the RMP. The mandatory OCA data elements include the release modeling assumptions (e.g., quantity released, wind speed) as well as the potential consequences (the distance beyond which no serious adverse effects are anticipated and an estimate of the total population within this zone) for both worst-case (catastrophic) and alternative accidental releases from the facility. A complete list of the OCA (and related) data elements is included in Appendix A.

Electronic Submission Workgroup

The Accident Prevention Subcommittee of the CAA Advisory Committee created the Electronic Submission Workgroup in October 1996 to examine the technical and practical issues associated with creating a national electronic repository of risk management plans. The Workgroup was charged with recommending the best way(s) for members of the regulated community to submit their risk management plans and the best way(s) for EPA, State and local governments, and the public to have access to this information.

On May 9, 1997, the Workgroup presented to the Accident Prevention Subcommittee a Discussion Paper that outlined its preliminary recommendations and requested advice on five issues. Based on its analysis, the Workgroup offered recommendations for both the RMP Submission System (which the Workgroup named RMP*Submit) and the RMP Access System (named RMP*Info). This report is concerned principally with one issue: should the offsite consequence analysis (as part of the RMP) be made available to the public over the Internet.

The Workgroup struggled with how EPA should provide access to OCA data -- refer to Appendix B for a more detailed description of this discussion. Many felt that the Internet was the obvious choice, but others saw potential problems in putting RMPs on the Internet. Some Workgroup members believed that making the OCA data available on the Internet would increase the risk that terrorists, foreign or domestic, would target reporting facilities. Specifically, they were concerned that the data elements providing the distances over which people might be harmed and the number of people within such distances (for the worst-case release scenario) would be useful to those contemplating a terrorist action. The Workgroup did unanimously agree that EPA should provide full, unrestricted access via the Internet to most RMP information (registration, prevention program, emergency response program, and five-year accident history data). However, neither the Workgroup nor the Accident Prevention Subcommittee have made a recommendation as to whether there should be full, unlimited access to offsite consequence analysis (OCA) data via the Internet.

Because of the lack of consensus, this issue remained a major concern to the Workgroup. At the May 9, 1997, Accident Prevention Subcommittee meeting, several Subcommittee members advised EPA to conduct a security study to quantify the incremental change in risk of putting OCA information on the Internet and to identify potential security measures that can be taken to reduce risk. The scope of the proposed study was developed by the Workgroup in conjunction with the Subcommittee and is included as Appendix C.

RMP Databases

The process of collecting and disseminating RMP information will consist of two elements:

- Each of the regulated facilities will receive **RMP*Submit** diskettes, which contain pre-designed forms for all of the RMP data elements. The completed diskettes (along with paper submissions from facilities without access to computers) will be submitted to EPA.

- The data will be downloaded regularly to **RMP*Info**, the database that will provide the public with access to RMP information.

EPA has contracted for the development of RMP*Submit and RMP*Info through EPA's Mission Oriented Software Engineering Support (MOSES) contract.

Primarily, the RMP data will be made available in RMP*Info on the Internet, through EPA's EnviroFacts at www.epa.gov/envirofw/. EnviroFacts is a relational database that provides a single point of access to data from multiple data resources. It currently incorporates data from seven EPA program databases and Locational Reference Tables including the Comprehensive Environmental Response, Compensation and Liability Information System (CERCLIS) and the Toxic Release Inventory (TRI). Databases contained in EnviroFacts can be viewed through a set of structured queries or by downloading the data in an Oracle database. EPA plans to have RMP*Submit and RMP*Info fully operational by January 4, 1999, to allow sufficient time for industry to submit prior to the final RMP deadline of June 20, 1999.

Security Study

This report presents the findings of the security study, which as conducted for the Agency by Aegis Research Corporation, ICF Incorporated, and Science Applications International Corporation:

- Section 1 summarizes the benefits associated with the Risk Management Program and the public availability of the RMP that EPA identified in its *Economic Analysis in Support of the Final Rule on Risk Management Program Regulations for Chemical Accident Prevention*, to accompany the final rule.

- Section 2 describes the nature of the security threat associated with the public availability of the OCA data and provides a quantification of the existing level of risk (baseline) and the incremental risk of the Internet and other methods that EPA has considered for making the RMP (including the OCA data) publicly available.

- Section 3 provides a summary of potential approaches to minimizing the risk described in Section 2 through facility security and information technology.

At the December 17, 1997, Accident Prevention Subcommittee meeting, Aegis Research Corporation will provide a more detailed presentation of the analysis, including the Adversary Strategy, outlined in Section 2.

Section 1: Benefits

EPA published *Economic Analysis in Support of the Final Rule on Risk Management Program Regulations for Chemical Accident Prevention* to accompany its final rule. That document quantified the primary benefits expected from the rule, including reductions in the damages to human health, property, and the environment from fires, explosions, and toxic releases at facilities covered by the rule. This section summarizes that analysis, with particular attention to the non-quantified benefits associated with the public availability of the RMP.

Implementation of the Prevention Program

EPA believes that the benefits expected from the RMP regulations arise primarily from avoiding chemical accidents and the associated damages to human health, property, and the environment. The types of damages considered in EPA's analysis were human health threats, including deaths and injuries; environmental damages, including threats to wildlife, soil, and water; and economic damages such as lost production, property damages, and litigation. EPA's prevention program requirements -- activities such as employee training, equipment maintenance, hazard review, operating procedures, incident investigation, and compliance audits -- are very similar to those mandated by OSHA under its Process Safety Management Standard. Based on the analysis in *The Cost and Benefits of Process Safety Management, Industry Survey Results*, EPA expects that compliance with the prevention program component of the risk management program will result in a significant reduction in chemical accidents and the associated damages at facilities subject to the RMP regulations. Specific estimates of the initial and annualized benefits arising from avoided damages are provided in the *Economic Analysis.*

Public Availability of the Risk Management Plan

EPA expects that the availability of the RMP information will provide a number of benefits beyond the reduction in accidents that will result from the implementation of the prevention program. These benefits -- assumed to derive primarily from access to the data elements in the registration, prevention program, and offsite consequence analysis -- will accrue to both the public and industry.

First, the public will benefit from RMP information, particularly the OCA data, because this information will allow the public to make more informed decisions on a number of issues. EPA research shows that approximately 85 million people live within a five-mile radius of a regulated source. This is equivalent to approximately 35 million households, or a third of the nation's total household population. This population is expected to benefit directly from the information provided by the offsite consequence analysis. Land use planners will be able to use OCA data when making decisions about siting of new industrial facilities and siting other buildings near existing industrial facilities. Emergency response agencies will have more complete information to use when they make decisions about devoting resources to establish special procedures and training for fire fighting and other emergency response personnel to respond to an accident, and maintaining additional emergency and medical equipment in case of an accident. The result will be more efficient, targeted use of resources.

RMP information will also provide the community with a better basis for conducting dialogues on prevention activities. Not only will RMPs provide previously unavailable on prevention practices of local facilities, but RMP*Info will allow the community to compare practices at their facilities with those of facilities of the same size and industrial sector. These comparisons will make it possible for the community to determine where local facility practices are similar to or better than the industry norm and where they may fall short.

EPA's experience with EPCRA section 313, the Toxic Release Inventory (TRI), has shown that making data easily available to the public has a powerful influence on facility practices, absent any regulatory requirements to change practices. Many companies that are required to file annual emission inventories under TRI have voluntarily adopted measures to reduce emissions out of a desire to be seen as a good neighbor. EPA expects that publication of the RMP data will have a similar impact. Facilities are likely to take steps beyond those required in the rule so that they can lessen the distances to endpoints, reduce the number of reported accidents, or reasonably demonstrate that they have reduced the likelihood of serious releases.

The availability of TRI information also has led to more frequent meetings between citizen groups and industry. This increased contact has led to plant tours, citizen inspections, the establishment of community advisory boards to monitor industrial activities, and the creation of "Good Neighbor Agreements" with specific facilities. Public interest groups use the data to educate the public about toxic chemical emissions and potential risk. A bibliography prepared by the Working Group on Community Right-to-Know listed over 100 state and local reports and more than 30 national TRI reports compiled by public interest groups. In California's Silicon Valley, for example, citizens used TRI data to pressure the state's largest emitter of ozone-depleting CFCs, IBM, into eliminating CFCs altogether. In Akron, Ohio, TRI information was used to pressure BF Goodrich into publicly announcing a 70 percent reduction goal in its emissions of air toxics. The Clean Water Action/Clean Water Fund used TRI data on the Houston Ship Channel in a report arguing that the channel be included in the Texas Water Commission's list of Toxic Impaired Waters.

Finally, experience in states with existing accident prevention programs has demonstrated that risk information has led to improved decision-making at covered facilities. Facilities can identify and target higher risk activities and share information about technological improvements. The New Jersey accident prevention rule has served as an impetus for industries to adopt innovative new technologies in their production processes. The result is more efficient production processes for the sources with decreased risks in associated accidents. The state also has shared information on state-of-the-art technologies. In addition, the State of California has noted that industries covered under its accident prevention rule have identified areas of waste in their production processes and been able to realize cost savings by improving operations.

Section 2: Risk Analysis

As described in the Introduction, the Electronic Submission Workgroup could not reach consensus on the means of making the RMP (specifically its OCA component) available to the public. This section focuses on this primary concern by describing the potential risk associated with a terrorist attack against a facility required to submit an RMP under EPA's Risk Management Program. It provides background information that outlines the nature of the potential terrorist threat and then examines the incremental risk associated with the public availability of OCA data on the Internet and the relative risk associated with alternative means of dissemination of the RMP.

Targeting RMP Facilities

The World Trade Center bombing in 1993 and the Oklahoma City Federal Building bombing in 1995 have made concerns about terrorist activities in the United States (whether from a domestic or foreign source) a reality. The federal budget currently provides hundreds of millions of dollars for prevention and response to terrorism in this country. In years past, much of this effort focused on airports. However, these two recent events (and others) have highlighted the potential susceptibility of "non-traditional" targets.

On July 15, 1996, Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) to examine the protection of eight critical infrastructures: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, water supply systems, emergency services (including police, medical, fire and rescue), and continuity of government and government operations. Two of those categories, gas and oil storage and transportation and water supply systems, overlap in part with the focus of this study. The classified findings of the PCCIP were presented to the White House on October 21, 1997. Although the PCCIP was concerned primarily with electronic warfare (the "cyber threat"), its input has been sought in the development of this analysis.

As directed by the Workgroup, this study examines the terrorist threat to the 64,000 regulated facilities and the surrounding public as a direct result of the availability of OCA data on the Internet. The possible consequences of an accidental release involving the toxic and flammable substances at these facilities led to these regulations; these same consequences make such facilities potentially attractive targets for terrorists – in such cases, the facility itself becomes a weapon. Although such actions have not occurred in the international arena where terrorist attacks are more prevalent, two specific incidents provide a basis for this assertion:

- On February 4, 1991, six pipe bombs were found on chemical tanks near the Norfolk Naval Base at the Allied Terminals, Inc., facility on the Elizabeth River. Fortunately, the timers on the bombs failed, and explosive ordnance personnel were able to remove and neutralize the devices without incident.

- Earlier this year, three men and one woman allegedly planned to blow up a gas refinery in Bridgeport, Texas, releasing what they thought would be a lethal cloud of hydrogen sulfide gas and perhaps killing police officers who would come to investigate a telephone bomb threat. During the chaos, they hoped to rob an armored car in the small town of Chico of $2 million and use the money to finance other terrorist actions. Due to information provided by an informant who was part of the group, they were arrested quietly before the bombs were set.

It is important to recognize that the RMP regulations apply to only a small percentage of the hundreds of thousands of facilities regulated by EPA and other federal, state, and local agencies for their use of toxic, flammable, or otherwise hazardous chemicals. For example, this analysis does not examine the risk associated with the transportation of regulated substances and other hazardous chemicals by truck, pipeline, barge, and train. Similarly, it should be recognized that facilities with hazardous chemicals represent only a small fraction of the potential universe of targets for a terrorist action. As has been demonstrated by the sarin release in the Tokyo subway and the bombs at the Atlanta Olympics, and in New York City and Oklahoma City, any public gathering places, including recreational facilities, transportation systems, and commercial buildings, can serve as the target of a terrorist attack. Thus, a listing of facilities submitting RMPs does not represent either a comprehensive listing of the potential universe of terrorist targets or even a comprehensive listing of targets where hazardous chemicals are present.

Use of the Internet

Intelligence experts have estimated that as much as 80 percent of our country's intelligence collection needs can be satisfied from open (unrestricted) sources, primarily the Internet, thus enabling the intelligence community to concentrate its efforts on the remaining 20 percent. The usefulness of Internet open source collection is likely to be even higher for foreign intelligence services collecting data on the United States. In addition, huge on-line databases, such as those developed by EPA and other government agencies, greatly diminish the amount of processing and analysis that must be done to make the information useful.

Information of "targeting" quality is already available to terrorist organizations on the Internet and from other sources that can be easily accessed, most for the cost of an envelope and a stamp under the Freedom of Information Act. The question remains, are foreign nations in general and those that sponsor terrorism availing themselves of that information? Because intelligence collection and operational plans are among the most closely guarded secrets of any nation, it is impossible to know the answer to that question with absolute certainty. However, with an estimated 120 countries already having or developing the capability to exploit the Internet for warlike purposes, the probability that they are using on-line databases as intelligence sources must be assumed.

Understanding the Baseline

The findings presented in the following pages represent the efforts of Aegis Research Corporation, in consultation with ICF Incorporated, to evaluate the risk of several scenarios under which the data in the offsite consequence analysis would be made available to the public under the mandate of Clean Air Act section 112(r). For the purposes of examining the risk, this study focuses on the post-June 21, 1999, time frame (after the initial submission of RMPs) and assumes that there will be no significant modifications to the RMP regulations in the intervening months. Other key assumptions are as follows:

- EPA will implement a national RMP database (RMP*Info), accessible over the Internet within the EnviroFacts system. RMP*Info will contain the executive summary, registration, and the summaries of the prevention program and emergency response program for the covered processes at RMP facilities; that is, all elements of the RMP except the OCA data.

- Users will not be able to sort or examine the RMP database itself; instead, directed searches based on a limited number of key data elements can be performed to view information on facilities of interest – for example, a list of all facilities in Houston, Texas. The search fields will consist primarily of data in the registration and would not include individual data elements from the offsite consequence analysis, prevention program, or emergency response program.

- Due to the size of the database (which would make it difficult, if not impossible, to download from the Internet in any case), EPA will produce a CD-ROM version of RMP*Info for use by states, local entities, and other stakeholders.

- Other right-to-know programs (e.g., EPCRA), federal databases (e.g., TRI), and computer systems (e.g., CAMEO) will continue to operate as they do currently.

Finally, this analysis does not attempt to evaluate the overall "success" or "failure" of an actual attack, but rather whether an attack is more likely because information vital to the planning process has become available (or more accessible) to the terrorist. The success or failure of an attempted strike would depend on numerous factors beyond the scope of this study, including facility-specific conditions, the competency of the terrorist(s), and the substances involved.

Findings: Incremental Risk

Following the direction of the Workgroup, the incremental risk was defined as the increased likelihood of a terrorist targeting an RMP facility due to the availability of additional information to support the planning process. To determine how useful certain information would be to a potential terrorist, our first task was to take the perspective of a terrorist. To do so, we reviewed the intelligence requirements and operations planning/targeting criteria used by the U.S. Special Operations Command, a military force whose assignments often involve the destruction of enemy infrastructure. We adapted this approach to develop an Adversary Strategy, which consists of three components:

- The key knowledge elements (e.g., the security measures in place at a facility) for a terrorist planning a strike against an RMP facility;
- A listing of individual data sources (e.g., the OCA) that can to some degree provide each of these knowledge elements; and
- An evaluation (scoring) of both the comprehensiveness of the data provided and its utility for each individual data source for each knowledge element.

The Adversary Strategy provides a structure for comparing relative reductions in the likelihood of completing the task through the elimination of selected sources of knowledge. For example, eliminating access to data on the number of persons living within the distance to the endpoint for a worst-case release might lower the attractiveness of a facility as a target. This allows the measurement of the relative risk associated with that particular piece of information (and the data sources that provide that information). In this way, the incremental increase in the risk of a terrorist attack associated with the availability, over the Internet, of the OCA data as part of the RMP, could be evaluated.

Specifically, we first identified a series of ten knowledge elements – the information that the terrorist needs to select a particular RMP facility as the target. Next, we identified a list of the potential sources for each piece of information, considering sources including observation, insider knowledge, and data available to the public on the Internet or though a FOIA request. Finally, we reviewed and graded each source (on a scale of one to ten, with ten being "most useful") based on a subjective analysis of the level of effort involved to use the source and the comprehensiveness of the information provided.

To calculate the likelihood that a terrorist can complete the target identification process, the highest valued source for each element was identified. Then, following the approach in a proprietary model developed by Aegis to support such evaluations, these values were multiplied together to reflect the overall effectiveness of the data sources in contributing to the planning process. (Note: Because the RMP serves as a data source for only some of the elements of the Strategy, the remaining elements were treated as constants for this analysis. For example, determining facility security measures is very important to the planning process, but these data are not available except through insider knowledge or observation of a particular facility.)

First, a value for the baseline level of risk upon implementation of RMP*Info was determined, reflecting the availability of the RMP (but not the OCA data) over the Internet, as well as the other sources for similar data that were identified. This value was then compared to the product of the scores for the highest valued source for each element when the OCA data are available with the RMP over the Internet.

Conclusion

This comparison indicated that the risk (although still very small) was slightly more than two times higher with unrestricted availability of the RMP with OCA data on the Internet. This increase reflects several factors, including the nature of the OCA data elements and the enhanced accessibility of data on the Internet to an international audience. Taken together, the primary utility of the unrestricted RMP and OCA data to a terrorist emerges from the capability to scan across the entire country for the "best" targets.

Findings: Relative Risk

In the second stage of the analysis, we developed a model to compare five alternative means of disseminating the RMP with the OCA data:

- In a publicly accessible database on the Internet – RMP*Info;
- On one or more CD-ROMs;
- Through a system of Bulletin Boards;
- Upon request (in hardcopy); and
- At a system of EPA-funded state Reading Rooms.

This model was based on Expert Choice^{TM}, a software program that facilitates decision making under conditions of uncertainty. We considered four primary criteria:

(1) Ease of access by potential users to the data source ("medium"), including the physical location of the data and the need to expend additional resources;

(2) Anonymity of the potential user of the medium;

(3) Number of facilities whose data can be accessed through the medium at a given time, and

(4) Extent to which the medium increases public awareness (including that of fringe or terrorist groups) of the availability of the data.

We then weighted each of the four criteria based upon its relative importance to a terrorist in the process of acquiring the data.

Conclusion

We used this model to evaluate each of the mechanisms for disseminating the data. In the initial analysis, we assumed that the entire RMP (including the OCA) was available on the Internet and could be downloaded or sorted at the user's discretion. The results are presented in Figure 10. In this case, the Internet ranked much higher (i.e., represented a greater security risk due to its value to a potential terrorist as measured by the four criteria) relative to the other alternatives. Bulletin Board and CD-ROM dissemination ranked similarly at a lower level, while Paper was a distant fourth with Reading Room representing the least risk. The main reason is the Anonymity factor; terrorists must remain anonymous to carry out their operations.

In the second analysis (based on the current operational parameters of other databases in EnviroFacts), we assumed that RMP*Info could not be downloaded wholesale from the Internet and users would be provided with a limited search capability based upon the registration data. We also assumed that the maximum geographical area that could be searched at one time would be either a county or local emergency planning district. This level of access to information is analogous to that provided by a feature article in a local newspaper or a publication by a local environmental group describing "zones of vulnerability." These results are presented in Figure 11. Under these conditions, the utility of the Internet to a terrorist would be comparable to Bulletin Board and CD-ROM; Paper and Reading Room remain in their same relative positions.

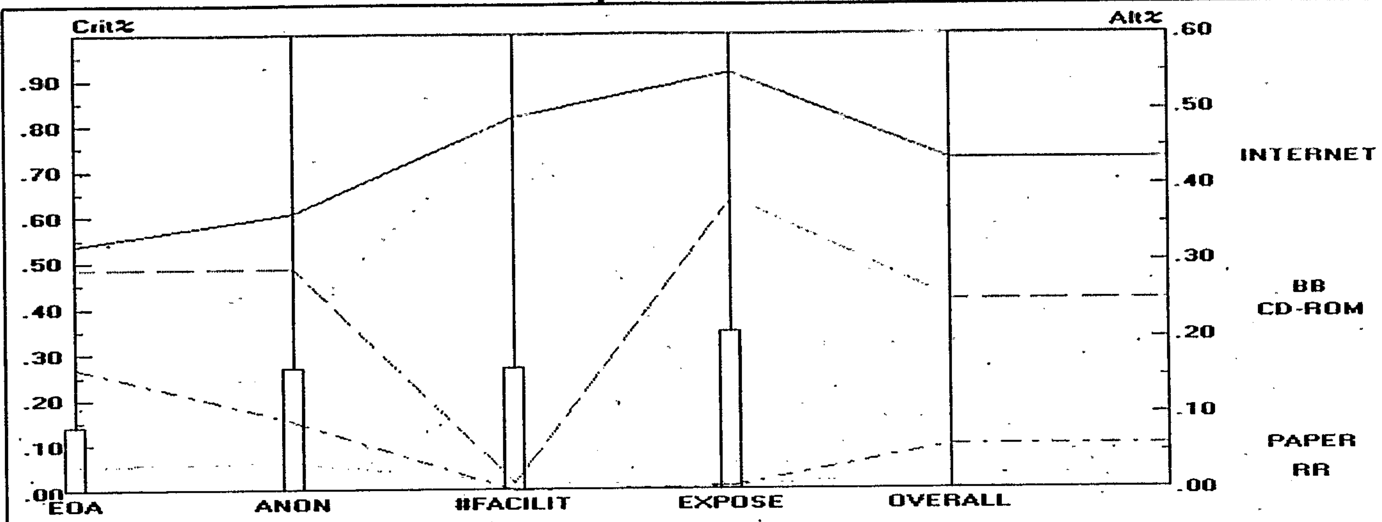
Conclusion

One way to achieve a resolution of this issue is to formulate a cost-benefit comparison. In this case, as described in the previous chapter, EPA believes that dissemination of the RMP (including OCA data) to the widest possible audience will lead to efforts (on the part of the facility and its neighbors) to reduce the risk of a chemical incident impacting the surrounding community. This can be displayed graphically with a downward-sloping curve representing an inverse correlation between information and risk. At the same time, some members of the chemical industry have voiced concerns with EPA's plans to put the OCA data on the Internet, citing the potential for an increased risk of a terrorist attack on their facilities as the cause. Under this line of reasoning, the optimum course of action would be to limit the information available to the extent possible. This, in turn, can be displayed graphically with an upward-sloping curve representing a direct correlation between information and risk.

As shown in Figure 12, the optimum solution is to make enough information available to the public to bring us to where the downward-sloping curve for the Risk of Chemical Accident intersects the upward-sweeping curve for the Risk of Terrorist Attack. (Please note: This graphic is presented for conceptual purposes only; the slope of the two curves and their point of intersection as depicted in Figure 12 are not intended to accurately reflect current conditions.) If we are "inside the box," we will have succeeded in reaching a solution that balances the benefits to be achieved with the potential risk to be incurred. The analysis presented in this section is intended to allow the Accident Prevention Subcommittee and EPA to make this determination.

Comparison of Alternate Means of Dissemination

Performance Sensitivity w.r.t. GOAL for nodes below GOAL



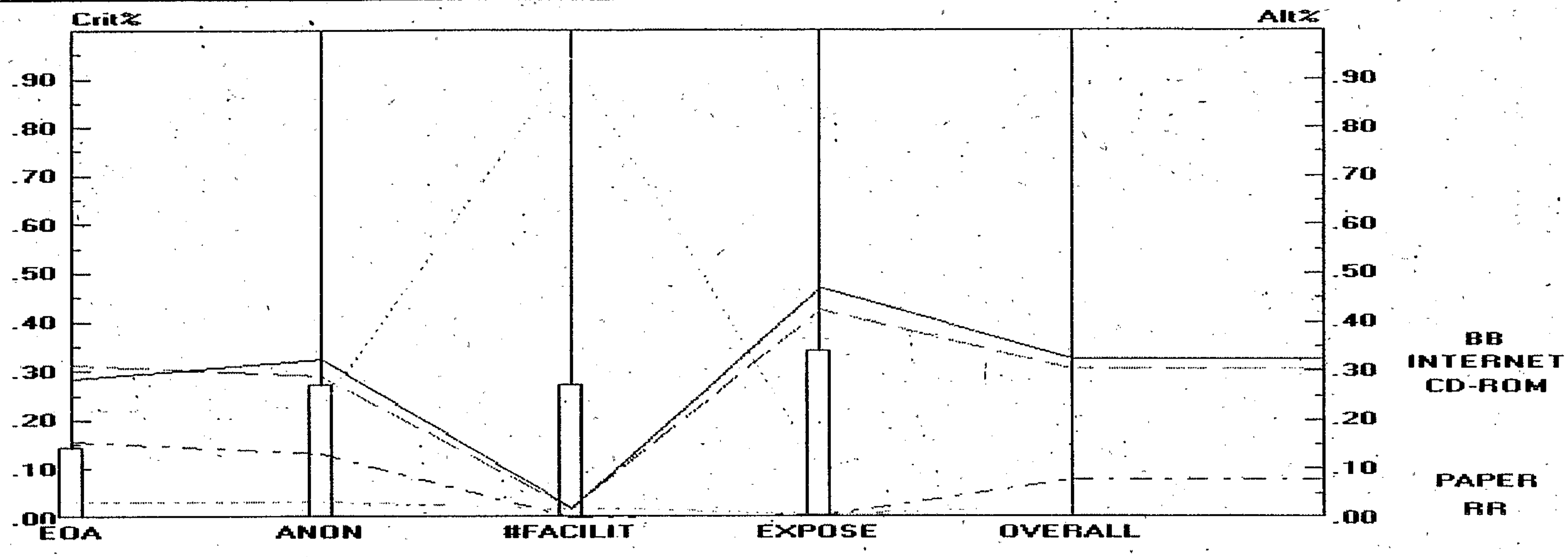
Abbreviation	Definition
EOA	Ease of access to the medium.
ANON	Anonymity - to avoid discovery and post-event capture.
#FACILIT	Number of facilities - equates to number of targets.
EXPOSE	Measurement of increased probability of attracting fringe groups.

INTERNET	Full RMP and OCA data on and downloadable from Internet.
BB	Bulletin Board - assuming that each BB will have data on 1 state.
CD-ROM	Same as Internet, but on CD-ROM (up to 11 CDs).
PAPER	Paper - Request the paper RMP/OCA from a facility or EPA.
RR	Reading Room - at a public facility
one per state	

Figure 10

Internet Mitigation Measures

Performance Sensitivity w.r.t. GOAL for nodes below GOAL

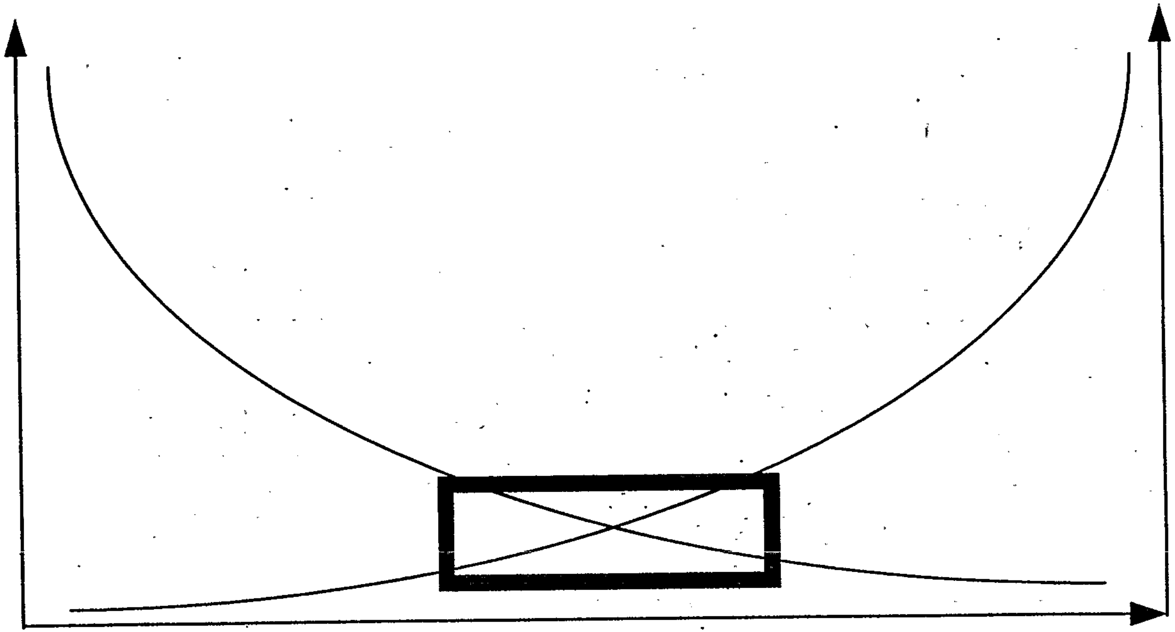


Abbreviation	Definition
EOA	Ease of access to the medium.
ANON	Anonymity - to avoid discovery and post-event capture
#FACILIT	Number of facilities - equates to list of potential targets.
EXPOSE	Measurement of increased probability of attracting fringe groups.

BB	Bulletin Board - assuming that each BB will have data on 1 state.
INTERNET	Full RMP and OCA data on Internet - controlled query only.
CD-ROM	Same as Internet, but on CD-ROM (up to 11 CDs).
PAPER	Paper - Request the paper RMP/OCA from a facility or EPA.
RR	Reading Room - at a public facility
one per state	

Figure 11

Are We "Inside the Box"?



Risk of Chemical Accident

Risk of Terrorist Attack

Availability of Information

Figure 12

Section 3: Risk Minimization

This section will address two complementary approaches to minimizing the risks identified in the preceding section:

- Information technology measures that can be implemented as part of the design of RMP*Info, and
- Facility security measures that reflect the hazard posed by the presence of toxic and flammable substances.

Information Technology

As described in the Introduction, at a minimum, RMP information (with the exception of the OCA) will be stored in a publicly available database (RMP*Info), accessible through the EnviroFacts system. EnviroFacts provides a single point of access to data from seven EPA program databases and Locational Reference Tables, including the Comprehensive Environmental Response, Compensation and Liability Information System (CERCLIS) and the Toxic Release Inventory (TRI). Under current plans, there are two options for accessing the databases contained in EnviroFacts:

(1) Due to its multi-gigabyte size (and normal data transmission speeds), it is unlikely to be feasible to allow users to download the entire RMP database. As a result, EPA is developing a capability to allow users to select information based on functional areas, which can then be downloaded. Such files could then be imported into another software product on the user's PC where it may be searched, sorted, and tailored to the user's needs. However, because EnviroFacts imposes a 15 minute connection time limit, it would require a lengthy series of such operations to acquire the whole database.

(2) Users can also conduct any of a set of pre-designed, structured queries on specific fields within the database and then view the RMP associated with the facilities that meet the search criteria. EPA has proposed searches for RMP*Info based on facility name, facility ID number, facility location, NAICS code, and chemical name. Thus, the user can search for facilities in a specific community or with processes in a specific NAICS code and then view the data for each such facility.

EnviroFacts requires the entry of a user ID and password to download its associated databases (but not for conducting the on-line queries), although a functional user ID and password are provided on its home page. Although this is the most cost-effective way of making the data available to the largest number of people, it means that there are no general security measures already in place for RMP*Info, and specifically for any data that are determined to be sensitive in any way. As described below, there are several types of mechanisms that could be put in place to protect OCA data generally or specific OCA data elements.

At the most basic level, EPA could implement a registration system specifically for users of RMP*Info to exercise some control over who uses the database. Practically, this would most likely apply to the database as a whole rather than for the OCA data elements individually. Such a system would require the user to provide identifying information such as name, address, phone number, etc., and then provides a password. The personal nature of the information provided through such a login process is protected by Oracle SQL*Net® and Secure Network Services™, which can encrypt password information as well as client-server, server-server, and server-gateway datastreams. Unfortunately, although simple, this type of registration system is not foolproof. For example, to preserve his or her anonymity, a terrorist, or any other individual, could simply enter false information into the registration form.

The challenge of avoiding false registration may be overcome by adopting an approach similar to that followed for Freedom of Information Act requests. In this case, the interested party would submit a formal, written, and signed request to EPA for access to the OCA information. Upon receipt, a user ID and password would be assigned and delivered to the user.

Neither of these systems, however, provide a basis for evaluating potentially illicit use of the data; they only serve as a speed bump to discourage the casual Internet surfer. A more complex step would be to combine the registration system with an Oracle tracking system in which each query in RMP*Info will be executed through a stored procedure (or program) in the Oracle database. A user ID and password dialogue box could be displayed each time a user tries to query sensitive information. Which users access what information could then be tracked by examining the log files in Oracle using the AUDIT command. If a problem ever arises involving a facility for which RMP*Info has an entry, it would be possible to identify all persons who had accessed that particular piece of information. To be effective as a deterrent, this process would need to be made clear to all users of RMP*Info up front.

At the same time, additional measures could be implemented to limit the overall usefulness of the database to a potential terrorist. First, in contrast to the other databases in EnviroFacts, EPA could determine to not activate any download option for the OCA, such as that described in option (1). In this case, individuals wanting a copy of the entire database to examine at their leisure would need to request the CD-ROM version from EPA. In this case, users would only be able to query RMP*Info in the structured, pre-determined fashion that EPA developed. In addition, EPA could further restrict the query function to prevent searches based on the information in the OCA judged to be most sensitive; the sensitive information would be viewable, but could not serve as a sorting criterion. In combination with the expected distribution of national reports on specific practices and industries, this approach would likely satisfy all members of the anticipated audience for the database, but would prevent a potential terrorist from sorting facilities nationwide to identify targets based on specific criteria.

Finally, it is important to note that, regardless of the actions taken by EPA to provide a measure of security for elements of the OCA that are judged to be particularly sensitive, the public retains a legal right under the statute to view this data. Freedom of Information Act and E-FOIA requirements make it possible for any citizen to request the RMP information, including the OCA, for all facilities across the country. As a result, EPA would be unable to prevent anyone from compiling all of the RMP data (whether from RMP*Info, CD-ROMs, or any other means of dissemination that EPA selected) and posting it on the Internet themselves. In fact, certain public interest groups have already indicated that they may do so.

Facility Security

The variety of facilities subject to the RMP regulations make it difficult to provide any generalizations regarding the "state-of-practice" or the "state-of-the-art" for security measures at regulated facilities. Instead, this section will simply review strategies and practices that have been observed with respect to security programs in several key areas: entry of facility employees, entry of facility visitors, exit of visitors and employees, unwanted entry, and acts of sabotage by employees and others.

Every company subject to the RMP regulations, formally or informally, has its own system for ensuring its security. To be effective, such systems are based on the real or perceived threat to the facility: a small facility in a rural location will have a different security strategy than that of a large manufacturing complex in a densely populated area. The first step in creating such a system is identifying vulnerable areas, potential threats to the facility, and the security measures already in place at the site. It must then be determined whether the existing security measures adequately respond to the specific risks faced by the facility. This is closely tied to the next step, that of developing a process for management approval of and implementing any necessary changes in personnel, equipment, and procedures. Finally, a security program necessitates an ongoing effort to determine whether the site-specific risk has changed as a result of internal and external events. This effort is supported by communication both within the industry (e.g., trade association) and with public officials such as the local police department.

The process of employee entry into a facility depends on several factors. In a large manufacturing facility, considerations of employee accountability (e.g., in the event of an emergency), may result in implementation of a badge system with entry through a control point such as a guard gate or an electric turn-style gate. Employees may also be issued badges with magnetic strips so their entry and exit can be tracked. Personal vehicles may be parked in an employee parking lot; however, it is possible for an employee to drive a personal vehicle into the site of a facility without having the contents of the vehicle subject to investigation. Other facilities rely on employee time cards or a security guard to track employee arrival.

For visitors, entry to a facility is generally restricted by full-time security personnel who staff the entrance gate(s). Visitors may be required to provide identification and state the nature of their visit, and may also be registered and provided with a badge or other identifying equipment (e.g., colored hard hat) to designate their status. Depending on the nature of their operations, some facilities require a brief safety and security presentation to be issued prior to issuance of a visitor badge. If their destination is in the manufacturing or process area, visitors may be accompanied by a representative of the facility; if not, they may or may not be allowed to proceed unaccompanied. Visitors may also be restricted from driving their vehicles on facility grounds, thus eliminating uncontrolled traffic in process areas; guards may check the vehicle contents in cases where the vehicle will be driven on site. Guards are trained to identify suspicious persons or situations and have the authority to refuse entry on the basis of their own judgement. In cases where a visitor is permitted to drive onto plant property, they may either proceed directly to the administrative office or other destination, or they may need to check in with a receptionist and follow the procedures described above upon arrival.

The procedures for exiting a facility often demonstrate that most security objectives are based on property protection. Searches for company property hidden in vehicles, bags, and briefcases can occur upon exit. In addition, employees and visitors may be required to sign-out or turn in their badge as they leave the facility.

The first line of defense against unauthorized entry is based on perimeter defense and visible deterrence. Regardless of size, facilities may have perimeter fencing to prevent individuals from entering the grounds. However, the level of perimeter monitoring and protection varies from facility to facility. Some facilities have sophisticated security systems: video cameras, beam perimeter motion detectors, and regular walking or driving checks by security personnel. Remote cameras may be monitored from a central security point and can be remotely controlled and positioned to view a large area. In cases where there are no systems to support the primary deterrents, entry can be gained by almost any determined individual and many times without being noticed, particularly at night or during non-operating hours.

Traditional security threats, including acts of sabotage by employees and bomb threats, have led to specific operating practices at facilities likely to be subject to such threats. Some security experts claim that the greatest potential for sabotage may be from employees. To address this concern, facilities use the existing supervisory structure and train their supervisors to be aware of suspicious or suspect behavior in their staff. If such behavior is detected, companies may have a system in place that allows the supervisor to report and begin an investigatory process or act to defuse the situation. Although not a universal practice, internal procedures may have been established to deal with bomb threats and similar incidents. Personnel handling incoming phone calls may be trained in asking appropriate questions, taking notes, and calling the appropriate authorities. In addition, the facility may be equipped with call recorders to tape such threatening phone calls.

Given the wide array of facilities regulated under the RMP regulations, not all of these measures are necessary or appropriate to provide security. However, facilities may be able to mitigate their vulnerability to sabotage and vandalism by implementing security measures that are appropriate for their type of operation.

Appendix A: RMP Data Elements of Concern

1. REGISTRATION

1.1 Source identification

a. Name
b. Street
c. City
d. County
e. State
f. Zip
g. Latitude
h. Longitude

1.2 Source Dun and Bradstreet number

1.3
a. Name of corporate parent company (if applicable)
b. Dun and Bradstreet number of corporate parent company (if applicable)

1.4 Owner/operator
a. Name
b. Phone
c. Mailing address

1.5 Name and title of person responsible for part 68 implementation

1.6 Emergency contact
a. Name
b. Title
c. Phone
d. 24-hour phone

1.7 For each covered process:
a. 1. Chemical name 2. CAS number 3. Quantity 4. SIC code 5. Program level

1.8 EPA Identifier

1.9 Number of full-time employees

2. TOXICS: WORST CASE

2.1 Chemical name

2.2 Physical state
a. ___ Gas
b. ___ Liquid

2.3 Results based on
a. ___ Reference table
b. ___ Modeling
c. Model used ______________________________

2.4 Scenario
a. ___ Explosion
b. ___ Fire
c. ___ Toxic gas release
d. ___ Liquid spill and vaporization

2.5 Quantity released ________ lbs

2.6 Release rate ______ lbs/min.

2.7 Release duration (if modeled) ______ min.

2.11 Distance to endpoint _____ miles

2.12 Residential population within distance (number) ___________

2.13 Public receptors (check all that apply)
a. ___ Schools
b. ___ Residences
c. ___ Hospitals
d. ___ Prisons
e. ___ Public recreational areas or arenas
f. ___ Major commercial, office, or industrial areas

2.14 Environmental receptors within distance (check all that apply)
a. ___ National or state parks, forests, or monuments
b. ___ Officially designated wildlife sanctuaries, preserves, or refuges
c. ___ Federal wilderness areas

2.15 Passive mitigation considered (check all that apply)
a. ___ Dikes
b. ___ Enclosures
c. ___ Berms
d. ___ Drains
e. ___ Sumps
f. ___ Other (specify)

3. TOXICS: ALTERNATIVE RELEASES

4. FLAMMABLES WORST CASE

4.1 Chemical

4.2 Results based on (check one)
a. ___ Reference table
b. ___ Modeling
c. Model used ________________________________

4.3 Scenario (check one)
a. ___ Vapor cloud explosion
b. ___ Fireball

4.4 Quantity released _________ lbs

4.5 Endpoint used __________

4.6 Distance to endpoint _____ miles

4.7 Residential population within distance (number) ____________

4.8 Public receptors (check all that apply)
a. ___ Schools
b. ___ Residences
c. ___ Hospitals
d. ___ Prisons
e. ___ Public recreational areas or arenas
f. ___ Major commercial, office, or industrial areas

4.9 Environmental receptors within distance (check all that apply)
a. ___ National or state parks, forests, or monuments
b. ___ Officially designated wildlife sanctuaries, preserves, or refuges
c. ___ Federal wilderness areas

4.10 Passive mitigation considered (check all that apply)

a. ___ Dikes
b. ___ Fire walls
c. ___ Blast walls
d. ___ Enclosures
e. ___ Other (specify)

5. FLAMMABLES ALTERNATIVE RELEASES

6. FIVE-YEAR ACCIDENT HISTORY

7. PREVENTION PROGRAM PROGRAM 3

7.4 PHA

d. Major hazards identified (check all that apply)
1. ______ Toxic release
2. ______ Fire
3. ______ Explosion
4. ______ Runaway reaction
5. ______ Polymerization
6. ______ Overpressurization
7. ______ Corrosion
8. ______ Overfilling
9. ______ Contamination
10. ______ Equipment failure
11. ______ Loss of cooling, heating, electricity, instrument air
12. ______ Earthquake
13. ______ Floods (flood plain)
14. ______ Tornado
15. ______ Hurricanes
16. ______ Other

e. Process controls in use (check all that apply)
1. ______ Vents
2. ______ Relief valves
3. ______ Check valves
4. ______ Scrubbers
5. ______ Flares
6. ______ Manual shutoffs
7. ______ Automatic shutoffs
8. ______ Interlocks
9. ______ Alarms and procedures
10. ______ Keyed bypass
11. ______ Emergency air supply
12. ______ Emergency power

13. _____ Backup pump
14. _____ Grounding equipment
15. _____ Inhibitor addition
16. _____ Rupture disks
17. _____ Excess flow device
18. _____ Quench system
19. _____ Purge system
20. _____ Other

f. Mitigation systems in use (check all that apply)
1. _____ Sprinkler system
2. _____ Dikes
3. _____ Fire walls
4. _____ Blast walls
5. _____ Deluge system
6. _____ Water curtain
7. _____ Enclosure
8. _____ Neutralization
9. _____ Other

g. Monitoring/detection systems in use (check all the apply)
1. _____ Process area detectors
2. _____ Perimeter monitors
3. _____ Other

8. PREVENTION PROGRAM PROGRAM 2

(same data elements as 7, but for hazard review)

9. EMERGENCY RESPONSE

Appendix B: Summary of Electronic Submission Workgroup Discussion

For Restricted Access

Some Workgroup members believe that the OCA information should be fully available to the LEPC and community in which a facility is located; however, access by groups and individuals geographically distant from the community where the facility is located should be controlled in some way. These Workgroup members are concerned that providing unlimited access to release scenario data will increase the instances of amateur terrorism and false alarms. The Workgroup focused its attention on amateur terrorists because members agree that professional terrorists are savvy enough to access this type of data already. Some Workgroup members fear that posting release scenario data on the Internet will increase the likelihood of false alarms that will waste the resources of first responders. Members who favor controlled access to OCA information contend that the intent of legislators was to reduce risk by making RMP information available to the local community, not to the entire world. These members argue that widespread and virtually unlimited access to a database of worst-case and alternative release scenario information is inappropriate. Such information, if accessible via the Internet, could be obtained with minimal effort and total anonymity. In the hands of an individual or a group bent on making a statement through acts of sabotage or terrorism, this information could be used to intentionally inflict serious harm on the people of a community as well as on the environment. These members note that, in view of terrorist acts in the United States in recent years, industry and members of the public sector are concerned about security. They believe that putting the OCA information on the Internet unnecessarily increases the risk of terrorism and sabotage that could harm the public as well as the targeted facility.

Recognizing the division on this issue, the subgroup met with two members of the FBI's Infrastructure Protection Task Force (IPTF). The IPTF representatives shared some anecdotes from their experience and expressed concern that providing OCA information on the Internet would make it easier for an ill-willed person to find and use. When asked to compare potential benefits associated with making RMP information available (thereby leading to accident prevention activities by industry and the community) with potential risks associated with possible misuse of the information by potential terrorists, the IPTF members said that they could not make such an assessment. They expressed the opinion that the information needed to answer that question does not exist. The IPTF did not provide any compelling argument on one side or the other of this issue, but did indicate a professional concern.

For Unrestricted Access

A second group of Workgroup members believe that there should be unlimited Internet access to all RMP data. Their argument is simple: the RMP is community right-to-know information and should be made available to the public. They cite the language in the law, which specifies that EPA shall make RMP data "available to the public." From their point of view the "hazard" comes from the chemicals that are present in the community, not from the information about the chemicals being publicized. In fact, they believe a successful RMP program, including full disclosure of OCA data, will reduce the inherent hazards in the community.

They note that there are many valid and important uses for RMP information by people who live well beyond the immediate community where a facility is located. A community might want to compare one of their facilities to another similar facility in another State to see how their facility compares in terms of vulnerability zones and prevention practices. Researchers will use the RMP information to develop comparative studies on chemical hazards and effective accident prevention programs. Public interest groups anticipate that the data will be critical to their work in reducing accident risks throughout the country.

Members who favor full, unlimited access to RMP data argue that the threat of potential terrorism does not outweigh the public's right to full access of RMPs. They also question whether restricting information (as opposed to reducing the actual hazards) provides any real barrier to terrorism. They argue potential terrorists could calculate the vulnerable zone around a facility and estimate how many people are at risk without RMP*Info by combining existing EPCRA reports with EPA guidance on vulnerability analysis and software mapping programs. Larger facilities are already highly visible from the road and, in some cases, containers are clearly labeled. In addition, circles of vulnerability are more frequently being published in newspapers, and may be put on the Internet through newspapers going on-line. Even with the RMP, some argue that it wouldn't be very useful to an amateur terrorist because the RMP will only provide the address of the facility and the name and quantity of the hazardous substance, but not the specific location of the substance on site.

Other Data Access Options

The Workgroup has not determined a viable alternative to the Internet and, therefore, has worked under the assumption the Internet will be the dissemination method to make RMPs available to the public. At the same time, the Workgroup recognized that not all interested parties will be able to access RMP data on the Internet. The Workgroup has considered other options, including CD-ROM, bulletin board systems, state reading rooms, and access without facility name and address for those outside the community.

None of these options offers a comparable way to allow inexpensive, widespread access to current RMP data in one place. Further, the Workgroup agrees that even if EPA does not post RMP data on the Internet, it is highly likely that, because RMP data is subject to the Freedom of Information Act, a public interest group or other organization will eventually post RMP data on the Internet.

Appendix C: Security Analysis "Scope"

The study should:

1) Quantify the incremental change in risk of putting OCA information on the Internet, including qualitative judgements of an estimate/prediction of the extent of the risk. If it is found that there is adequate data to produce a terrorist threat, explicitly show what data would be used and how.

2) If a significant risk is found in #1, then advise EPA if it is possible to protect public from misuse of the information if it is on the Internet, and if so how. Provide a range of protection measures and their corresponding costs.

3) Quantify the risks associated with making the information available in other ways, including, but not limited to:
   (A) CD-ROM distribution to the public through an EPA hotline;
   (B) Requesting paper copies of the OCA from the LEPC;
   (C) Bulletin Board System;
   (D) Reading Rooms in each State and Washington DC; and
   (E) Access without facility name and address for those outside the community.

The study should also address the following questions:

a) How do public domain air dispersion models (such as ALOHA) and modeling guidance (such as the CAA OCA guidance) that are already publicly available factor into the risk? In other words, could a potential terrorist easily figure out the OCA information based on the chemical quantity or other basic information that is outside the OCA?

b) Given that chemical information is already available on the Internet and through other sources, such as EPA's Toxic Release Inventory (TRI), Toxic Substances Control Act (TSCA), Clean Water Act (CWA), Resource Conservation and Recovery Act (RCRA), the Emergency Planning and Community Right to Know Act (EPCRA) does RMP information on the Internet increase the potential threat to the public?

c) What information can be easily inferred from living or working in the community or driving by a facility (such as, a propane distributor listed in the yellow pages who has visible on-site tank)?

d) What are standard operating procedures for facilities to protect against sabotage? Are their additional steps a facility can take for protection?

e) Given the requirements on EPA to release information under FOIA and E-FOIA, and the high probability of someone else posting the information on the Internet if EPA does not, how do the risks compare for EPA posting and someone else posting the information? What are the best ways to control this risk?

f) What would be the increment of increased or decreased "risk" of terrorism when comparing making information available locally vs. nationally electronically? What factors account for this increase or decrease in risk?

g) How will the availability of media (such as NY Times articles publishing the OCA circle), environmental studies (like "Accidents Do Happen"), and government reports ("Hazard Screening of Anhydrous Ammonia in Nebraska, June 1995) differ from national database access?

h) How would this info be useful to a FOREIGN "terrorist" vs. local "terrorists" who would theoretically have access to the information?