**SAND REPORT**
SAND2002-0877
Unlimited Release
Printed April 2002

# A Scalable Systems Approach for Critical Infrastructure Security

Arnold B. Baker, Robert J. Eagan, Patricia K. Falcone, Joe M. Harris, Gilbert V. Herrera,W. Curtis Hines, Robert L. Hutchinson, Ajoy K. Moonka, Mark L. Swinson, Erik K. Webb, Tommy D. Woodall, and Gregory D. Wyss

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.



Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2002-0877
Unlimited Release
Printed April 2002

# A Scalable Systems Approach for Critical Infrastructure Security

Authors

Arnold B. Baker
Office of the Chief Economist

Robert J. Eagan
Energy, Information & Infrastructure Surety Division

Patricia K. Falcone
Systems Studies Department

Joe M. Harris
Deputy of Program Development Department

Gilbert V. Herrera
Deputy of Operations Department

W. Curtis Hines
Systems Analysis Group

Robert L. Hutchinson
Networked Systems Survivability & Assurance Dept.

Ajoy K. Moonka
Security Systems and Technology Center

Mark L. Swinson
Government Programs Department

Erik K. Webb
Geohydrology Department

Tommy D. Woodall
Strategic Development Department

Gregory D. Wyss
Risk, Reliability and Modeling Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0724

## Abstract

Critical infrastructures underpin the domestic security, health, safety and economic well being of the United States. They are large, widely dispersed, mostly privately owned systems operated under a mixture of federal, state and local government departments, laws and regulations. While there currently are enormous pressures to secure all aspects of all critical infrastructures immediately, budget realities limit available options.

The purpose of this study is to provide a clear framework for systematically analyzing and prioritizing resources to most effectively secure US critical infrastructures from terrorist threats. It is a scalable framework (based on the interplay of consequences, threats and vulnerabilities) that can be applied at the highest national level, the component level of an individual infrastructure, or anywhere in between. This study also provides a set of key findings and a recommended approach for framework application. In addition, this study develops three laptop

computer-based tools to assist with framework implementation—a Risk Assessment Credibility Tool, a Notional Risk Prioritization Tool, and a County Prioritization tool.

This study's tools and insights are based on Sandia National Laboratories' many years of experience in risk, consequence, threat and vulnerability assessments, both in defense- and critical infrastructure-related areas.

## Table of Contents



## List of Figures



## List of Tables

Intentionally Left Blank

# A Scalable Systems Approach for Critical Infrastructure Security

## INTRODUCTION

Critical infrastructures underpin the domestic security, health, safety and economic well being of the United States. These key physical and cyber systems include energy production, transmission and distribution, food and water, transportation, telecommunications and information systems. These systems grew up independently, in a world of relative trust. They were designed to minimize occasional failures from aging and degradation, adverse weather conditions, natural disasters and accidental operator error. Over time these systems have become increasingly complex and interdependent, increasing the potential for these occasional failures that the systems were designed to minimize. In general these systems were not designed to withstand terrorist attacks or be secure from deliberate use as lethal weapons, as was experienced in the September 11, 2001, terrorist attacks on the United States.

Mounting an effective domestic response to future terrorist infrastructure attacks is a difficult and complex challenge. Critical infrastructures are large, widely dispersed, mostly privately owned and operated under a mixture of federal, state and local government departments, laws and regulations. While there are enormous pressures to secure everything now, and many competing requests for federal funding solutions, budget realities limit available options.

The purpose of this study is to provide a clear framework for systematically analyzing and prioritizing resources to most effectively secure US critical infrastructures from terrorist threats. It is a scalable framework – meaning that it can be applied at the highest national level; at a single federal, state or local agency level; to a private sector system; or for a component of an individual infrastructure. This framework is based on the interplay of consequences, threats and vulnerabilities and includes approaches for how to think about each of these key components. This study also provides a set of key findings and a recommended approach for framework application. In addition, the study develops three laptop computer-based tools to help with framework implementation—a Risk Assessment Credibility Tool, a Notional Risk Prioritization Tool, and a County Prioritization tool.

This study's tools and insights are based on Sandia National Laboratories' many years of experience in risk, consequence, threat and vulnerability assessments, both in defense- and critical infrastructure-related areas. Listings of study team background briefings and illustrative Sandia critical infrastructure risk related tools are provided in Appendix B. Study team participants are shown in Appendix A.

Intentionally Left Blank

# HOMELAND SECURITY FRAMEWORK

## Consequences, Threats And Vulnerabilities

As depicted in Figure 1, the risk, the expected cost from or expected loss due to an adversary attack on a given infrastructure, is determined by the intersection of consequences of the attack, the threats or likelihood of the attack and vulnerabilities to the attack.

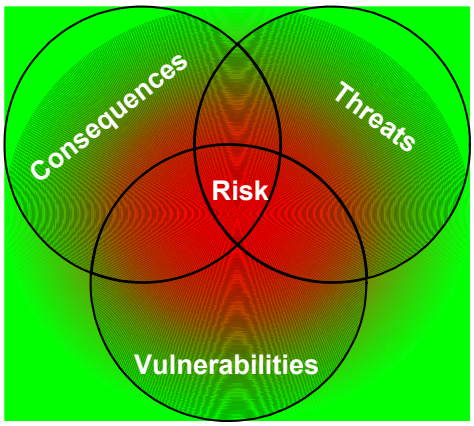


***Figure 1. Risk, Consequences, Threats and Vulnerabilities***

More specifically,

$$R = C \times T \times V,$$

where:

**R** = Risk associated with an adversary attack and/or system/asset failure

**C** = Consequence(s), the negative outcomes associated with degradation or failure of the system or asset(s). Consequences of an attack can be measured by loss of life, economic impact, loss of public confidence or other metrics

**T** = Threat, the probability or likelihood that a given attack scenario with the potential to disrupt systems or assets and cause undesirable consequences will occur. Threats are characterized by their means and likelihood of occurrence

**V** = Vulnerability, a weakness in the system or asset, or supporting systems or assets (e.g., security systems, etc.) to the threat (**T**) that would cause degradation or failure.

Each of these components will now be discussed in turn.

## Consequences

Consequences – and the perceived potential to inflict consequences – are the major weapons with which the terrorists fight to accomplish their agenda. Consequences can occur in many different dimensions, including death and injury, economic loss, loss of public confidence in government, personal inconvenience, etc., with many possible subcategories of each. These consequences can result either when a system fails to fulfill its intended function (such as when fires cannot be extinguished because a water supply system fails) or when an adversary inflicts harm by using a system's resources in an unintended way (such as when hijacked planes are used to kill civilians and destroy structures, as happened on September 11, 2001). Consequences can be caused either directly, as the immediate results of an event or attack, or indirectly, as the physical, logistical and psychological effects of the attack ripple across the nation. The actual and perceived consequences can be amplified for events that occur in areas with a high population density (allowing increased death and injury) and for events that cause widespread and/or protracted effects (e.g., a major outage of the nation's electric power grid).

A major and intended consequence of such attacks is to generate fear in the population. For an attack to generate fear, people must believe that they might fall victim to a similar attack that could cause severe personal consequences. The sense of fear is heightened when people feel they are helpless to prevent, detect, evade or recover from the attack or its consequences. Anthrax-containing letters, for example, place *my* life at risk because I cannot prevent someone from sending one to me and I cannot detect the spores before I am exposed. Diagnosis of anthrax is uncertain, so I cannot be certain of being accurately diagnosed and effectively treated after I am exposed to anthrax. And if I contract anthrax and do not receive treatment, I am likely to die. Thus the preferred scenario for a terrorist involves causing major direct and indirect consequences in such a way that the general population feels threatened by similar acts against which they are helpless.

## Threats

A threat is anything that can disrupt the mission of the system. Threats are characterized by their means and likelihood of occurrence. A system may face several threats to its mission. The many varieties of adversaries fall into three classes: insiders, outsiders and outsiders working in collusion with insiders.

The US mind-set is to think in terms of highly reliable and highly effective weapon systems that have well controlled, localized impacts, generally operating under the assumption that the attackers wanted to stay alive. But in recent years, terrorists have tended to seek out low-cost, broad-impact events, in which the attackers are willing to sacrifice their own lives to achieve broad impact.

Threat assessment also includes a number of other factors. For example, attack effectiveness combines both stealth and capability. The degree of stealth in threats falls as the number of members of the attack team rises. Yet the capability of the threat group is also likely to rise as the number of team members increases, at least until a certain point. (This may be less true with cyber threats or other "actions-at-a-distance").

Attackers also have become increasingly innovative and effective in their threats. Figure 2 illustrates that prior attacks here and abroad tended to be either highly effective or highly innovative. However, the attacks of September 11 showed elements of both innovations in attack scope, planning, and mechanisms as well as effective operational execution.

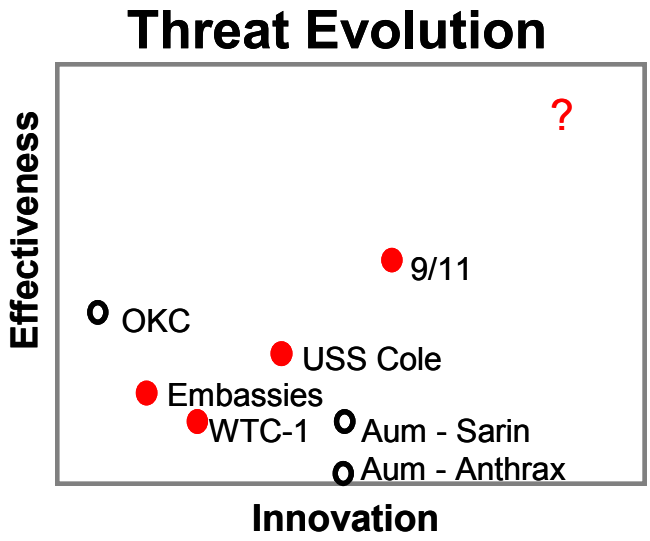


***Figure 2. Selected Examples of the Integration of Threat Innovations and Operationa1 Execution***

The September 11, 2001 attackers went beyond the previously witnessed guns and bombs approach and devised attack mechanisms that were deviously innovative – in effect leveraging a few box-cutters into a few guided missiles. The operational execution, while not perfect, was highly effective – coordinating multiple near-simultaneous strikes without providing a detectable attack signature until the operation was well underway.

## Vulnerabilities

Vulnerabilities are the characteristics of a system that cause it to suffer degradation or failure as a result of having been subjected to a threat or attack. A threat or attack can be caused by direct action, e.g., bombing an electrical power transformer switching station to stress a power grid, or by indirect actions, such as attacking a dependent infrastructure, e.g., bombing a natural gas pipeline that would cause a gas-fired power generation plant to shut down, thereby stressing a power grid. Each example represents a vulnerability of the power grid.

Vulnerability of an infrastructure element is a function of its intrinsic design, protection systems (physical or other) and changes over time. The intrinsic design of an infrastructure element defines the strengths and weaknesses associated with a specific attack, and these strengths and weaknesses can be assessed through an analysis of the element and its design parameters. Protection systems are designed to protect the infrastructure element against a range of threats. Protection systems are typically characterized by their ability to detect the occurrence of a threat, delay the threat from exploiting system vulnerabilities and respond to the threat with

protective forces or other countermeasures. Changes over time, such as physical aging, obsolescence or complacency, can affect the vulnerability of an infrastructure element.

Attacks may reveal or even exploit unexpected vulnerabilities within infrastructures and protection systems that are deeply buried and only become visible under extreme conditions or unusual coincidences. Protection systems also can create unexpected vulnerabilities if they provide misinformation to responders and decision-makers, such as suggesting all systems are normal when an attack actually is occurring, or mistakenly identifying an incorrect attack location.

### Qualitative and Quantitative Methods for Infrastructure Risk Assessment

Quantitative methods are systematic, repeatable and based upon objective measures. Thus these methods have high statistical validity. However, they require significant knowledge of the response of an infrastructure element to physical phenomena. The vastness and complexity of US infrastructure systems, their interdependency and the lack of integrated infrastructure databases and modeling tools limit the applicability of quantitative approaches at this time. Qualitative methods rely upon the use of expert teams using expert judgment and consensus to determine vulnerabilities. Such teams are assisted by tools and methods to improve consistency and scientific soundness. Special teams can be used to address infrastructure interdependencies.

For results to be meaningful, it is critical that the methods and models employed be validated. This applies equally to both quantitative and qualitative approaches.

Initial consequence, threat and vulnerability characterizations will be predominantly based upon qualitative methods. Over time, as infrastructure databases, modeling tools and our general understanding of infrastructures and their interdependencies improve, such characterizations will increasingly use quantitative methods, though the nature of this work is such that complete reliance on quantitative methods is unlikely.

## Integrated Framework

To analyze the complex web of US critical infrastructures, a consistent and systematic security assessment approach must be applied to each of the critical infrastructures and the interdependencies among them. We outline such a methodology in this study, which we will refer to as the Framework.

This Framework is based on closely related and detailed risk assessment methodologies that Sandia has developed and applied to a wide range of facilities over the last 25 years. Such facilities include:

DOE/NNSA Nuclear Weapon Complex Sites/Facilities

- DOE/NNSA Transportation Safeguards System
- DOD Bases/Facilities
- FSU Nuclear Weapons Facilities/Sites

- Federal Dams
- Water Infrastructure
- High Voltage Transmission
- Municipal Buildings
- Chemical Facilities
- National Airports
- Nuclear Power Plants
- Sectors of Civilian Transportation
- Strategic Petroleum Reserve
- US Mint Facilities and Depository
- Prisons/Jails
- Schools
- Bio-Terrorism/Defense of Cities

The Framework methodology provides the procedure for completing a risk assessment that evaluates the level of risk associated with the threat, consequences and vulnerabilities of a critical infrastructure as a system. The Framework also helps direct and implement security upgrades or other plans for risk reduction, as appropriate for the characteristics of the subject system, in a cost-effective manner. Thus the Framework defines the problem, generates suggestions for its mitigation, and provides a consistent system for resource-allocation decision priorities. Over time, the Framework also can be used for periodic, longer-term performance monitoring as the subject system and its risks evolve.

As noted above, the core of this Framework is

**RISK = Consequences * Threat * Vulnerabilities**
**(R = C x T x V)**

where:

**R** = Risk associated with an adversary attack and/or system/asset failure

**C** = Consequence(s), the negative outcomes associated with degradation or failure of the system or asset(s). Consequences of an attack can be measured by loss of life, economic impact, loss of public confidence or other metrics

**T** = Threat, the probability or likelihood that a given attack scenario with the potential to disrupt systems or assets and cause undesirable consequences will occur. Threats are characterized by their means and likelihood of occurrence

**V** = Vulnerability, a weakness in the system or asset, or supporting systems or assets (e.g., security systems, etc.) to the threat (**T**) that would cause degradation or failure.

Other specialized terms important for an understanding of the Framework include:

Assets - Tangible and intangible assets whose loss or disruption would be of high consequence.

System - Features that are deployed to meet the protection goals in an organized, interdependent whole. Includes the larger system of interconnected asset units and protection features.

Remediation Alternatives - Changes that reduce risks (mitigate consequence or reduce likelihood of attack). These could include, but are not limited to, public policy, security measures, system redundancy, process improvements, regulations, etc.

The process of applying the Framework is depicted in Figure 3. The process begins with asset characterization. Once that is complete, consequences, threats and vulnerabilities are evaluated for those assets, though there is no precise order for these evaluations. The key steps in the process are briefly described in a generalized way below. A more detailed technical description is provided in "A Risk Assessment Methodology for Physical Security", in Appendix C. (See also Mary Lynn Garcia (Sandia National Laboratories), The Design and Evaluation of Physical Protection Systems, Butterworth-Heineman, 2001.)

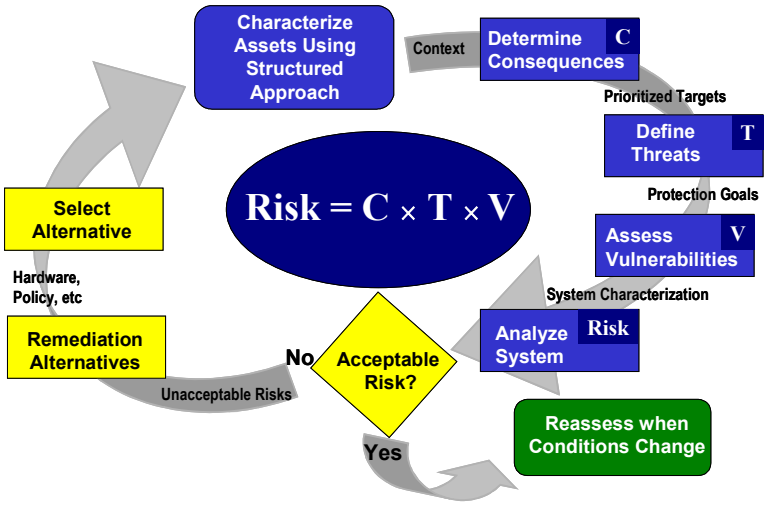


***Figure 3. Process for Determining Security Risk***

Characterize Assets - Critical assets are those assets essential to meeting the mission objectives of the system. The information required to identify and characterize the critical assets can be obtained from existing published information, observation, expert judgment, experience and interviews. There are also a number of formal tools available for identifying critical assets, including fault trees, expert teams, logic diagrams and event trees. Layout sketches that show critical assets will be very useful in the subsequent steps of this process.

Determine Consequences - Consequences are the negative outcomes associated with degradation or failure of a system or its assets. This step determines the negative outcomes as measured by an appropriate set of metrics such as economic losses, lives lost, loss of public confidence, injuries, public fear, etc. Consequences from individual assets as well as from

interdependencies among two or more assets should be included. Both expert judgment and some systematic tools for determining consequences are available.

Define Threats - A threat is anything that can disrupt the mission of the system. This phase of the assessment defines threats with the potential to disrupt assets/systems and cause undesirable consequences. Threats are characterized by their means and likelihood of occurrence. A system may face several threats to its mission. The many varieties of adversaries fall into three classes: insiders, outsiders and outsiders working in collusion with insiders.

Threat definition includes an identification and description of the types of adversaries (malevolent persons or groups) that may try to prevent the system or facility from performing its mission. Information is collected and evaluated to determine which adversaries pose a threat to the system. For each type of adversary, a likelihood of attack is developed so that threats can be weighted. Threat definition does not consider how a threat can be deterred, detected, or defeated. These issues are treated in later steps of this process.

Assess Vulnerabilities - This step defines weakness (degradation, failure potential, etc.) in the asset, dependent assets, interdependent assets, or supporting systems (e.g., security systems, etc.). Vulnerability also can be a weakness or gap in the asset's physical security protection system, whose effectiveness may deteriorate over time, due to aging equipment, outdated procedures, or complacency, for example. A wide range of tools is available to assess system vulnerabilities. For instance, Sandia National Laboratories has developed Adversary Sequence Diagrams as well as several software packages (ASSESS, SAVI, EASI, etc.).

Analyze System Risk - This step combines the consequence determinations, threat definitions and vulnerability assessments to permit evaluation, ranking and prioritization of relative risks within and across infrastructures. Those risks deemed acceptable for specific infrastructures should be reassessed when conditions change.

Table 1 shows a stylized template for considering integrated risk analysis.

***Table 1. A Stylized Risk Analysis Template***

| | CONSEQUENCE METRICS | | | THREAT | | RISK | | |
|---|---|---|---|---|---|---|---|---|
| INFRASTRUCTURE | Lives | $ Cost | Public Confidence | SCENARIO | VULNERABILITY | Lives | $ Cost | Pub. Conf. |
| Oil/Gas Production | | | | | | | | |
| Pipelines | | | | | | | | |
| Electric Power | | | | | | | | |
| Transmission/Dist | | | | | | | | |
| Rail | | | | | | | | |
| Highway | | | | | | | | |
| Water Transport | | | | | | | | |
| Air Transport | | | | | | | | |
| Water (Human Use) | | | | | | | | |
| Food | | | | | | | | |
| Telecoms | | | | | | | | |
| Info Systems | | | | | | | | |
| Nuclear Materials | | | | | | | | |
| Key Domestic Events | | | | | | | | |
| Terrorist Attack Materials | | | | | | | | |

Remediation Alternatives - Those risks not acceptable are then further reviewed for remediation alternatives – changes that reduce consequences, threats or vulnerabilities. Such changes include, but are not limited to public policy, security measures, system redundancy, process improvements, regulations, etc.

## Interdependencies

Interdependencies are a key part of critical infrastructure risk analysis. As shown in Figure 4, each critical infrastructure works to insure its own integrity. Because critical infrastructures depend on each other, assuring the integrity of the larger system is complex. For example, electricity is needed for oil and natural gas production and distribution systems, communication systems, water systems and banking and finance, etc. Communications are also needed for electric power, transportation, etc. Individual manufacturing and service industries also depend on these critical infrastructures as well as each other. For example, the automobile manufacturing industry depends on plastics as well as steel. The plastics industry depends on the oil and natural gas industry, in addition to electricity, communications, and so on. Steel depends upon electric power and other energy sources, as well as its own set of other critical inputs, including coking coal.

Each infrastructure also has "buffers" to insulate itself from temporal variations in other infrastructures, and to protect other infrastructures from its own. Examples include stand-by capacity (hot, warm, cold) in electrical networks, and bulk petroleum inventories. Because of economic factors, reserve capacity is declining in many infrastructures as Just-In-Time management practices spread. This relatively recent and widespread change makes systematic analysis both challenging and necessary.

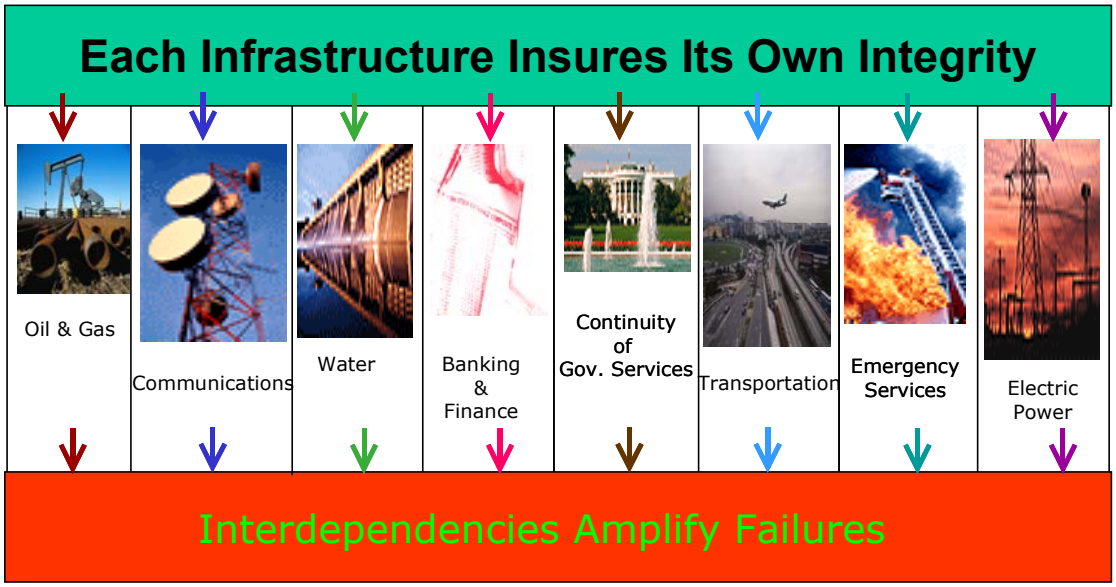


***Figure 4. Illustrative Critical Infrastructure Interdependencies***

Economists have developed a series of macroeconomic models to examine relationships between and among industries. These macroeconomic input-output models link the outputs of each industry to the inputs of other industries, as well as link the industries to key variables in the macro economy, such as gross domestic product, price levels and interest rates. Currently in the US we are aware of four such models that can operate at a national scale—Implan, Inforum (University of Maryland), REMI (Regional Economic Models Inc.), and DRI/WEFA. Both REMI and Implan can operate at various regional levels of detail and aggregate across regions to a national level—features that are important in tracing detailed regional interdependencies for specific infrastructures.

These models are useful for examining the relative economic impact of one infrastructure or industry upon another. For example, they can trace through the direct impact of higher oil prices on industries that use oil, as well as the indirect impact of higher cost intermediate goods (such as petrochemicals, steel, etc.), on industries that use them to provide products for final consumer demand. Their current state of development, however, is not sufficient to readily examine the consequences of a shutdown of specific portions of a specific infrastructure. If a portion of a power grid were shut down so that electricity was not available to certain industry customers, these models are not detailed enough to know whether alternative sources of electricity (such as self-generation, distributed electricity or alternative grid electricity) would be available to those customers. Hence these models currently cannot show whether the impact of such an act would simply raise the cost of goods produced for those electricity customers or would result in a significant shutdown of production for specific facilities. Such a facility shutdown could in turn shut down production for other industries that rely on the intermediate goods from the shutdown facility.

Further refinements of these models, including better integration with detailed energy and other critical infrastructure models, specific industry facilities data and industry expert knowledge, could provide longer-term tools for integrated infrastructure risk assessment.

Sandia National Laboratories is actively involved in assessing and modeling a number of these independencies in California and elsewhere and has helped policy makers to understand the need for a National Infrastructure Analysis and Simulation Center (NISAC). NISAC, a joint partnership with Los Alamos National Laboratory, is currently being established.

The Framework described above actively considers interdependencies at each step of the process. This is depicted in Figure 5 on the next page.

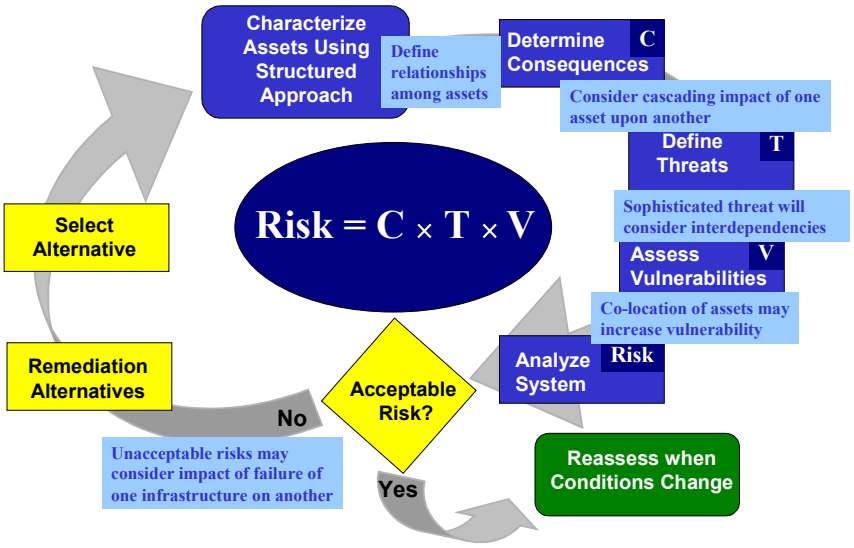


*Figure 5. Considering Interdependencies Within the Framework*

Interdependencies as well as consequences also can be examined by considering the co-location of different infrastructures and assets. One way of doing this is by integrating relevant geographic information system (GIS) databases. Many such databases have been developed by government and industry sources and are commercially available.

Figure 6 provides three illustrations of GIS analyses—the location of dams by type; consideration of airport, major road and rail transport; and electricity transmission and population density. The digital nature of GIS allows for both high level and very detailed geographical infrastructure and asset examination. However, variations in data quality, and incompatibilities in data base structure and semantics remain. .

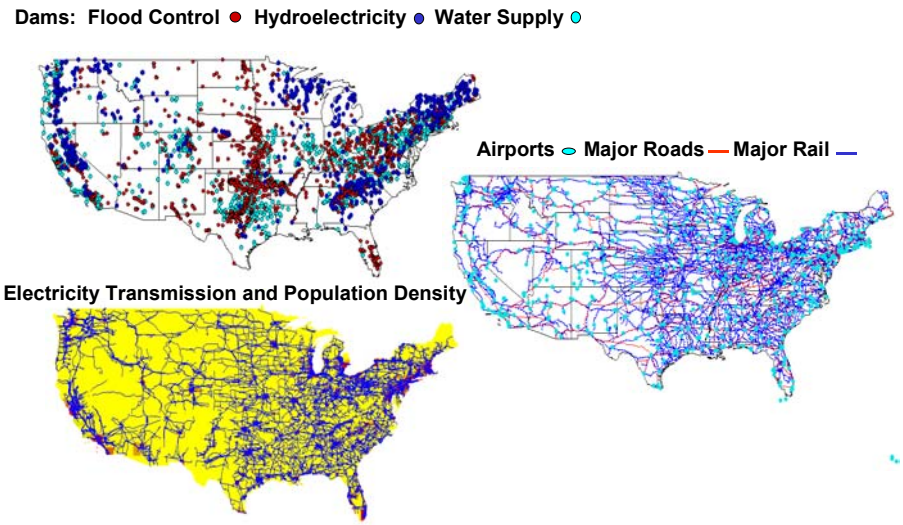


*Figure 6. Illustrations of GIS Tools for Infrastructure Analysis*

## Risk and Insurance

The private sector offers insurance--life, liability, property and casualty insurance, among other products-- on a "for profit" basis. Insurance companies typically redistribute their insurance risk for their policies by writing contracts with large, re-insurance companies, such as Lloyds of London or Swiss Re. Insurance companies use historical data and statistical methods to determine how to price their insurance products profitably. In several areas, most notably crop insurance or flood insurance, the risk is deemed so great that that private insurers typically do not offer policies, and instead, the federal government becomes the insurer of the last resort.

In the US, prior to September 11, the history of US terrorist acts was limited enough that most insurance policy holders and insurance companies had not focused on terrorist insurance. Since September 11, both insurers and re-insurers indicated they would require very high terrorist insurance premiums, if they offered terrorist insurance at all. After January 1, 2002 when the contracts of many re-insurers came up for renewal, most or them refused to cover primary terrorist risk. Thus, terrorist insurance in the US ultimately could work similarly to crop and flood insurance, with the US government becoming the insurer of the last resort. This has already happened in several European countries that have had considerably more experience with terrorists (e.g., Britain, Spain and France).

In the US, this issue is particularly important because direct insurance policies are written and regulated at the state level. Thus, insurance companies need state permission to exclude terrorist risk from their policies. As of mid-January, 2002, some 40 states have approved optional terrorist risk exclusions from general liability and other business related policies. Several states (New York, Alaska, California), however, have refused to offer such exclusions; concerned that this could set a precedent for other exclusions. (For additional information, see The Economist, January 10, 2000).

Intentionally Left Blank

# FINDINGS

This study set out to provide a clear, scalable framework for systematically analyzing and prioritizing resources to more effectively secure US critical infrastructures from terrorist threats. The framework (Framework) was built upon tools and approaches developed at Sandia National Laboratories over the last 25 years and applied to many specific infrastructures and components.

The Framework involves consideration of assets to be secured, the consequences that flow from those assets not being secured, the threats to those assets and the vulnerability of those assets to threats. The systematic assessment and combination of these inputs within and across critical infrastructures can provide consistent risk measures (characterization of expected losses or expected costs) from potential adversary activities. These risk measures can then be relatively ranked and prioritized for improving their security. The process for such risk reduction involves cost-effective consideration of reducing consequences, threats and vulnerabilities. Reducing risk should involve the full spectrum of tools available to industry and policy makers, including legal and regulatory reform, improved operating procedures, information protection and sharing and research and development into needed hardware, software, database and model development and decision-support tools.

We believe that such a Framework, if consistently applied from the top down, can help significantly improve critical infrastructure protection prioritization in the US both in the near and longer term.

We believe this to be true because in the course of this study we found that threat effectiveness and innovation among US adversaries appears to be increasing, raising the threat threshold and requiring evolving concepts of threat reduction. At the same time, the complexity of US infrastructure ownership and responsibility makes system security prioritization extremely difficult. This ownership and responsibility spans all levels of both the public and private sectors, although the vast majority of US critical infrastructure is privately owned. While critical infrastructure owners are also responsible for infrastructure design, operation and security, they currently receive relatively limited access to threat information that would affect the security of their specific infrastructures. The siting and operation of their infrastructures also are affected by a jurisdictional patchwork of federal, state and local laws and regulations, most of which have not been evaluated for their impact on security from terrorist threat.

We also found that government agencies and the private sector lack common terminology and common standards for infrastructure security assessments. As a result, present attempts to prioritize infrastructure security at best would be based on inconsistent risk estimates, which would lead to reduced infrastructure security at higher public and private costs.

Much of US infrastructure is privately owned. Private owners very much want to keep their infrastructure information proprietary for competitive reasons, for fear that their highest risks could become publicly known (thus raising the likelihood of adversary action) and even out of concern that the government might use such data against them. However, because of infrastructure interdependencies, infrastructure owners and the nation are likely not considering

the full risk. In fact, with so much proprietary information, they are not able to do so. Over time, some way must be found to balance the needs for private sector information security with the public need for infrastructure protection.

Significant additional knowledge deficiencies also exist. For example, terrorist threats cannot yet be characterized as probabilities. Currently the best we can do is to attempt to bound them by using intelligence estimates and some mathematical tools, such as fuzzy logic and complexity theory.

While there are many infrastructure-related databases, including GIS databases, they are not coordinated, integrated or consistent. It is even unclear how many such US infrastructure-relevant databases currently exist. Some of these are perhaps too public and readily available. A number of databases previously available on government web sites have recently been removed. As noted above, many other databases are perhaps too privately held for the best national interest.

While critical infrastructure interdependencies are very real and growing in importance, their true nature and significance for risk to attack are poorly understood. Available economic models and data sets cannot effectively characterize relative economic consequences of infrastructure interruptions.

There is no simple approach to national level critical infrastructure security prioritization. The infrastructures are too numerous, complex and interdependent. Today such a process would need to be highly qualitative, although guided as much as possible by hard data and scientific support tools. Over time the process should become more consistent as it becomes more quantitative, although the issues are so complex that it is doubtful it ever could become purely quantitative. Regardless of which approaches are employed, the models and tools used must be validated if the results are to be meaningful.

While the Sandia National Laboratories Framework described in this study may not be perfect, we believe it can provide a good starting point for bringing consistency to the US infrastructure security prioritization process. We also believe that regardless of what system is applied now to improve process consistency, new technologies and systems clearly will be needed to improve infrastructure security and its investment prioritization over time.

# RECOMMENDATIONS

We recommend that the Sandia National Laboratories Framework and related processes be considered for general application to the Homeland Security prioritization process in three phases.

## Initial Stand-Up

First and foremost, we recommend that the involved agencies agree on an integrated approach and terminology for infrastructure security prioritization and socialize, if not institutionalize, this process among key federal agencies.

We also recommend that the involved agencies establish national level expert teams to characterize assets and assess consequences, threats and vulnerabilities and determine the relative risk for key infrastructures and their components. State or local lead offices responsible for homeland security also could utilize such an approach. Once these priorities have been established, we further recommend that specific agency leads determine and implement the most cost-effective remediation approach (and budgetary requirements) for reducing unacceptable risk for key infrastructures.

The National Academies of Science and Engineering could organize these teams for the national level, and that the detailed results, conclusions and data used and developed should be protected from the public domain. These teams should draw upon the best information, analyses and studies available. The teams should be linked with the Homeland Security Policy Coordinating Committees and other related government and industry organizations as appropriate. The individual teams should be relatively small, supported with subject-matter and infrastructure experts from the private sector, government, national laboratories and universities and should draw on the knowledge and expertise of representative industry groups as far as possible to avoid issues of competitive information. The groups should use validated decision-analysis tools for decision support and available classified and unclassified infrastructure-related databases.

The recommended sequence for these teams is as follows:

**Stage 1: Set the Rules**
An initial team (A) will agree on the rules – that is, the boundaries, definitions and other terms of reference for the entire process. These will apply to key national assets, consequences, vulnerabilities and threats and the infrastructures to be assessed. This process will ensure consistency for each of the subsequent teams and for the process output.

**Stage 2: Determine Threat Scenarios**
The second team (B) will determine the threat characterization and threat scenarios to be considered by the other teams consistent with the rules established by team A.

**Stage 3: Assess Infrastructures**

In stage 3 of the process, parallel teams (Cs) will operate, one team for each infrastructure to be assessed. For example, if the infrastructures to be assessed were those listed in Table 1 above, there would be 15 parallel teams, though this number could be larger or smaller as determined by team A above.

Each of these parallel teams will evaluate and prioritize security elements in their respective infrastructure, including identify key interdependencies, using the asset, consequence and vulnerability frames of reference and the threat scenarios established by team A.

**Stage 4: Assess Interdependencies**

In Stage 4, a single team (D), consisting primarily of one representative each from the parallel infrastructure teams, would use the Stage 1 rules and outputs from Stage 3 to assess interdependency risks for the set of infrastructures under consideration.

**Stage 5: Integration**

The Stage 5 team (E) will integrate the output from Stage 3 (infrastructures) and Stage 4 (interdependencies) into a final infrastructure security prioritization and also will integrate any major knowledge-based deficiencies and lessons learned from the other teams. Results of the integration team would be presented for senior-level government executive review, discussion and appropriate action.

**Stage 6: Risk Remediation Decisions**

This government executive review will make final decisions on infrastructure priorities. It will select government agency leads (which may be current leads) to identify and implement (with budgetary requirements) the most cost-effective approach for remediation of the highest risk infrastructures and their components, as well as for key knowledge-based deficiencies and implementation of key lessons learned.

**Stage 7: Risk Remediation Implementation**

Responsible government agency leads will implement remediation in parallel, cooperating with each other on crosscutting remediation programs. As soon as practicable, each agency lead will determine budgetary needs and provide these to the Office of Homeland Security for review, integration and transmittal to OMB and the Congress.

The overall recommended process with potential time lines for each stage is shown in Table 2 below.

*Table 2. Recommended Process*

| 1<br>30 Days | 2<br>30 Days | 3<br>30-60 Days | 4<br>30 Days | 5<br>30 Days | 6<br>30 Days | 7<br>6-12 months + |
|---|---|---|---|---|---|---|
| **Team A** | **Team B** | **Teams $C_1$, $C_2$, $C_3$. . .** | **Team D** | **Team E** | **Govt. Exec Review** | **Agency Leads** |
| **Set the Rules &-Definitions** | **Determine Threat Scenarios** | **Assess Infrastructures in Parallel** | **Assess Inter-dependencies** | **Integration** | **Risk Remediation Decisions** | **Risk Remediation Implemen-tation** |
| For Key Assets Consequences Vulnerability Threats | | Use Team A Frames of Reference and Team B Threat Scenarios Evaluate and Prioritize Security Elements Identify Key Inter-dependencies | Includes Representative from Each Infrastructure Team | | | Agency Leads Implement in Parallel |

## Broader Rollout

Based on the results from the Initial Stand-Up, we recommend that best practices be identified and standards for threat, vulnerability and consequence assessments be established.

In addition, we recommend that approaches for integrating relevant public and private data relevant to infrastructure security be developed and implemented. These approaches must adequately protect critical information from adversaries and adequately protect proprietary information and consider implications relative to the Freedom of Information Act.

We also recommend that protocols be established for disseminating security assessment output to the public, including addressing which elements of information will be made available to infrastructure owners and operators as security design parameters.

Further we recommend the agreed-upon infrastructure security terminology, approach and implementation be extended to the regional, state and local level and to the private sector.

## Longer Term

Over the longer term, we recommend that concerned organizations develop a five- to ten-year strategic plan with input from this Framework process and available team output. To synchronize with federal budgetary cycles, this plan would be initially developed with best available information and adjusted over time as output from the Framework process and expert teams becomes available.

This plan would consider a range of risk scenarios and establish high-level infrastructure security objectives and priorities. It would define budget requirements, performance metrics and owners of specific goals. It also would consider regulatory and legislative issues.

As input to that strategic plan, we also would recommend that a five- to ten-year roadmap for supporting technologies and data requirements be developed in key areas such as consequence, threat and vulnerability assessments; database integration and maintenance; strategic modeling, simulation and analysis tools; and operating tools and protection mechanisms, including sensor and software systems.

# SANDIA NATIONAL LABORATORIES TOOL KIT

As a part of this study, three additional laptop computer based tools were developed to help with infrastructure security prioritization: "Risk Assessment Credibility Tool", "Notional Risk Assessment Tool" and "County Prioritization Tool". Each of these is discussed in turn.

## Risk Assessment Credibility Tool

The Risk Assessment Credibility Tool provides a hierarchy of questions that can be used to evaluate the degree of rigor and completeness of security assessments presented to the Office of Homeland Security or other federal or state government bodies. Ideally, security assessments and their associated requests for funding would be developed and presented to responsible government agency heads using methods that have internal integrity, are repeatable, are similarly structured and use metrics that can be compared for prioritization. However, given all of the assessments currently underway in many different organizations, this is unlikely to be the case. Thus the Sandia study team developed this Risk Assessment Credibility Tool.

The tool consists of a query structure that approximates the security assessment framework described above and addresses the following steps:

- Characterizing Assets and Determining Consequences
- Defining Threats and Defining Safeguards
- Proposing and Prioritizing Actions

Additionally, the query structure provides questions to evaluate the methodology of the assessment.

The query structure is organized in a multi-tiered hierarchy. Lower-tiered questions are used to elicit detailed answers. The detailed answers should provide information necessary to answer the next-higher-tier questions. The query structure can be accessed in either a bottom up or top down fashion, depending on the user's goals. For example, someone with responsibility for policy might ask questions from the top two tiers, while technical analysts might ask questions from the lower tiers. The lowest-tier questions are not comprehensive but indicate the kind of information needed at this level of detail. Further development would be needed for application at this level of detail to individual infrastructures.

There are four questions in the highest tier that pertain to the assessment of potential security consequences:

- How was this assessment performed? (Process)
- How much confidence is there that potential negative impacts and the key components of the infrastructure are adequately defined? (Assets and Consequences)
- How much confidence is there that potential threats to and vulnerabilities of the infrastructure are adequately defined? (Threats and Vulnerabilities)
- How confident are we that the proposed solutions will strengthen weaknesses in the infrastructure security? (Actions)

In total we have developed approximately 140 questions (see Appendix D). Obviously, this structure in outline format is difficult to use. Therefore we have provided a web-based tool that drills down through the structure four levels. While the tool is designed to be a descriptive tool allowing evaluation of others' work, we would strongly encourage it to be used prescriptively, as a component of defining what is required of new security assessments. Finally, we have not provided a way to rank answers to the questions we pose. This would be a logical and useful next step.

## Notional Risk Prioritization Tool

This tool, based on the stylized risk analysis template previously shown (Figure 4), is in the form of a Powersim laptop computer model. The model allows the user to insert his own values for the Consequences (Lives at Risk, Economic Cost, and Loss of Public Confidence), Threats and Vulnerabilities for the infrastructures/systems shown in Figure 4 above. Each parameter has a slider with a range between 1 (low) and 9 (high) for each infrastructure/system, and initially sets all values to "5" (medium). This tool allows for real time infrastructure/system risk ranking by individual consequence, and also allows the user to weight each consequence to develop a single risk metric, if so desired.

## County Prioritization Tool

In addition to top-down, national infrastructure prioritization, it also is important to consider regional infrastructure prioritization. Geographic areas with higher population density, for example, are ones in which a given terrorist event potentially could directly affect more people. Similarly, geographic areas with higher density of economic activity are ones in which a given terrorist event (without considering infrastructure interdependencies) could create higher potential economic losses. Such types of information are publicly available.

The Sandia team created a laptop County Prioritization Tool in Microsoft Access to allow ready analysis and ranking of US counties by a number of such density measures. Through such a ranking, priorities could be developed for examining critical infrastructures that are in or feed into the areas of greater population, economic or other important density measures. Such an examination for a high priority county could be a joint undertaking of the federal, state and local governments, and the private sector that serve that county.

The County Prioritization Tool was developed by combining open source information from the 1997 U.S. Economic Census and Environmental Systems Research Institute's US data set (Economic Census Report Series 1977 CD-EC97-1, ESRI Data and Maps: CD 2 United States) for all 3,100 plus US counties. The common link between the two data sets, the state and county name, permitted the combination of geographic and economic data. The tool allows ranking from highest density to lowest, and vice versa, and also provides data for each county and a quick graphical ranking as well. Four different densities are calculated in the model (per square mile): population, economic (GDP contribution), manufacturing (sales), and information systems (receipts).

# APPENDIX A

## Study Team Participants

## Study Team

- Arnie Baker, 6010, Principal Investigator
- Rick Craft, 16000
- Bob Eagan, 6000, Project Manager
- Pat Falcone, 8114
- Joe Harris, 14020
- Gil Herrera, 1310
- Curtis Hines, 9810
- Bob Hutchinson, 6516
- Clyde Layne, 9815
- Ajoy Moonka, 5801
- Mark Swinson, 15203
- Erik Webb, 6115
- Tommy Woodall, 6502
- Greg Wyss, 6410

- Cindy Acosta, 6001
- Teresa Mills, 6001
- Karen Padilla, 6001
- Lorraine Segovia, 6000

## Contributors

- Betty Biringer, 5845
- Theresa Brown, 6515
- Ruth Duggan, 6512
- John Ganter, 6534
- Dave Harris, 6516
- Len Malczynski, 6010
- John Milloy, 5845
- Dennis Miyoshi, 5800
- Jennifer Nelson, 6518
- Sharon O'Connor, 5862
- William Paulus, 5845
- Kevin Stamber, 6515
- Gordon Smith, 5861
- Juan Torres, 6517
- Ivan Waddoups, 5845
- John Wirsbinski, 5845
- William Young, 6516

Intentionally Left Blank

# APPENDIX B

This appendix contains an illustrative list of Sandia critical infrastructure risk-related tools. It also contains a list of internal Sandia briefings to the Study Team during the course of the study.

## Illustrative Sandia Critical Infrastructure Risk-Related Tools

| MODEL TITLE | DESCRIPTION | POINT OF CONTACT |
|---|---|---|
| Markov Latent Effects Tool | Safety assessment of air transportation operations. | Arlin Cooper<br>Airworthiness Assurance Department, 6252<br>505-845-9168 |
| Risk Assessment Method – Property Analysis and Ranking Tool (RAMPART) | Risk screening tool developed for GSA to assess risks from natural hazards, crime, and terrorism to federal buildings. | Regina Hunter<br>International Environmental Analysis Department, 6804<br>505-844-5837 |
| 4C Power Analysis Suite | Tools to find most critical nodes in the bulk power grid. | David Robinson<br>Risk & Reliability Analysis Department, 6413<br>505-844-5883 |
| RAM-D$^{SM}$ (Risk Assessment Methodology for Dams$^{SM}$ | A manual security risk assessment methodology for dams; training and no-fee license available. | Rudy Matalucci<br>Civilian Surety Programs Department, 5862<br>505-844-8804 |
| RAM-T$^{SM}$ (Risk Assessment Methodology for Power Transmission$^{SM}$) | A manual security risk assessment methodology for high-voltage electrical transmission. | Betty Biringer<br>Systems Analysis/Development Department, 5845<br>505-844-3985 |
| RAM-W (Risk Assessment Methodology for Water Supply Systems) | A manual security risk assessment methodology for water utilities. | Jeff Danneels<br>Civilian Surety Programs Department, 5862<br>505-284-3897 |
| Other risk assessment methodologies | Additional *Official Use Only* security risk assessment methodologies have been developed for federal and municipal government agencies. | Ivan Waddoups<br>Systems Analysis/Development Department, 5845<br>505-844-1649 |
| Prison Escape Risk Assessment Methodology | A manual tool with some simple computer augmentation that guides analysis and risk of prison escape. | Chris Robertson<br>Systems Analysis/Development Department, 5845<br>505-844-4776 |

| MODEL TITLE | DESCRIPTION | POINT OF CONTACT |
|---|---|---|
| *The Appropriate and Effective Use of Security Technologies in U.S. Schools* | A web handbook for school officials that offers practical guidance on security concepts and operational issues, video surveillance, weapons-detection devices, entry codes, and duress alarms. It can be found at<br><br>http://www.ncjrs.org/school/home.html | Mary Green<br>Public Safety Technologies Department, 5861<br>505-856-7969 |
| VAM (Vulnerability Assessment Methodology) | A systematic, risk-based tool to evaluate the security of chemical facilities against malevolent threats. | Cal Jaeger<br>Systems Analysis/Development Department<br>505-844-4986 |
| SAVI (Systematic Analysis of Vulnerability to Intrusion) | A software package for evaluating the effectiveness of physical security systems against outsider threats. | Mark Snell<br>Systems Analysis/Development Department<br>505-844-9283 |
| EASI (Estimate of Adversary Sequence Interruption) | A simple-to-use method of evaluating physical protection system performance along a specific path. | Mark Snell<br>Systems Analysis/Development Department<br>505-844-9283 |
| ASSESS (Analytic System and Software for Evaluating Safeguards and Security) | An integrated software package for evaluating physical protection system effectiveness against theft of SNM by a spectrum of adversaries. | Mark Snell<br>Systems Analysis/Development Department<br>505-844-9283 |
| BROM (Business Risk/Opportunity Model) | A manual process that characterizes risks and opportunities to support informed decisions. | John Wirsbinski<br>Systems Analysis/Development Department<br>505-284-3422 |
| Master Timeline Model | Tool for calculating consequences of a biological attack with and without relevant countermeasures. | Todd West<br>System Studies Department, 8114<br>925-294-3145 |

| MODEL TITLE | DESCRIPTION | POINT OF CONTACT |
|---|---|---|
| InSIST | Indications and Warning System and Information Sharing Tool. | Lillian Snyder<br>National Infrastructure Simulation and Analysis Center, 6518<br>505-284-3378 |
| Infrastructure Interdependencies Flow Model | The flow of sector commodities (trading, markets, and other economic aspects). | Theresa Brown<br>Critical Infrastructure Surety Department, 6515<br>505-844-5247 |
| Complex Adaptive System Simulation | Agent-Based economic modeling and simulation of complex systems. | Diane Barton<br>Critical Infrastructure Surety Department, 6515<br>505-844-5504 |

## Internal Sandia Briefings to the Study Team

- Analysis of Infrastructure Systems Using Agent-Based Microsimulation Presented by *Presented by Dianne C. Barton*
- Infrastructure Interdependency Macro-Economic Dynamic Simulation Modeling *Presented by Theresa J. Brown*
- Water Infrastructure Security *Presented by Jeffrey J. Danneels*
- Security Engineering *Presented by Dennis S. Miyoshi*
- US Energy and Greenhouse Gas Model *Presented by Arnold B. Baker*
- Defense Science Board Task Force: Unconventional Nuclear Warfare (UNW) Defense *Presented by Leonard W. Connell*
- Overview on Chem-Bio *Presented by John Vitko, Jr.*
- Risk-Informed Proliferation Analysis *Presented by Gregory D. Wyss*
- An Extensible Framework for Risk & Reliability Assessment *Presented by Richard L. Craft*

- Information Design Assurance Red Team
  *Presented by Ruth A. Duggan*

- Echelons of Damage Result from WMD Attacks
- Defense of cities Against Biological Weapons Attack
- US Population in Metro Areas-City Data
  *Presented by Patricia K. Falcone*

- 9-11-01—The Second Day of Infamy
  *Presented by John Taylor*

# APPENDIX C

## A Risk Assessment Methodology For Physical Security*

**Betty Biringer**
**Systems Analysis and Development Department, 5845**
**Sandia National Laboratories, MS 0759**
**Albuquerque, New Mexico 87185**
**(505) 844-3985**
**(505) 844-0011 FAX**
**E-mail: bebirin@sandia.gov**

Violence, vandalism, and terrorism are prevalent in the world today. Managers and decision-makers must have a reliable way of estimating risk to help them decide how much security is needed at their facility. A risk assessment methodology has been refined by Sandia National Laboratories to assess risk at various types of facilities including US Mints and federal dams. The methodology is based on the traditional risk equation:

**Risk = $P_A$ * (1 - $P_E$) * C,**
**$P_A$ is the likelihood of adversary attack,**
**$P_E$ is security system effectiveness,**
**1 - $P_E$ is adversary success, and**
**C is consequence of loss to the attack.**

**The process begins with a characterization of the facility including identification of the undesired events and the respective critical assets. Guidance for defining a design basis threat is included, as well as for using the definition of the threat to estimate the likelihood of adversary attack at a specific facility. Relative values of consequence are estimated. Methods are also included for estimating the effectiveness of the security system against the adversary attack. Finally, risk is calculated. In the event that the value of risk is deemed to be unacceptable (too high), the methodology addresses a process for identifying and evaluating security system upgrades in order to reduce risk.**

KEY WORDS: **Risk assessment, security effectiveness, physical security, consequence, vulnerability analysis, likelihood of attack**

**Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.**

* **Presented to Globex 2000, July 2000, Las Vegas, NV**

## Analysis Methodology

An analysis methodology has been used to assess the vulnerability of physical protection systems for facilities. Figure 1 describes the order and sequence of the seven basic steps of the methodology.

## 1. Facility Characterization

An initial step in security system analysis is to characterize the facility operating states and conditions. This step requires developing a thorough description of the facility itself (the location of the site boundary, building locations, floor plans, and access points). A description of the processes within the facility is also required, as well as identification of any existing physical protection features. This information can be obtained from several sources, including facility design blueprints, process descriptions, safety analysis reports, environmental impact statements, and site surveys.

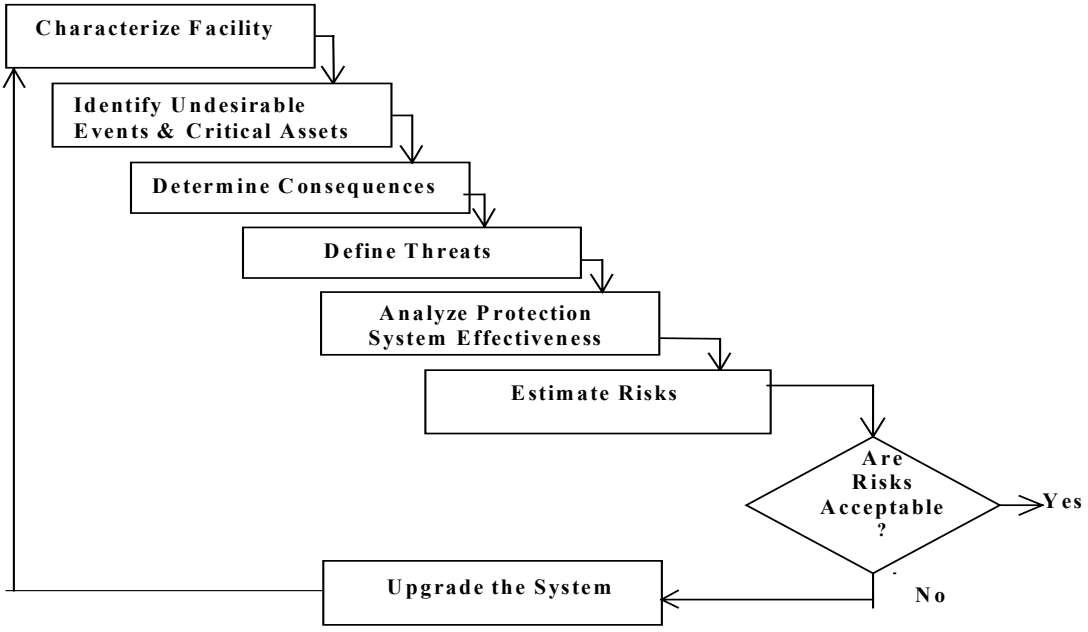


*Figure 1. Analysis Methodology*

## 2. Undesired Events/Critical Assets Identification

**Undesired Events-** The undesired events must be established. Undesired events result in undesired consequences. Undesired events are site-specific and have adverse impacts on public health and safety, the environment, assets, mission, and publicity.
**Critical Assets-** The adversary could cause each undesired event to occur in several ways. A structured approach is needed to identify critical components for prevention of the undesired events. A logic model, like a fault tree, can be used to identify the critical components. The

critical components and their locations become the critical assets to protect. Figure 2 is the top-level portion of a generic fault tree for facilities.

## 3. Consequence Determination

The next step is to categorize undesired events or loss of critical assets. The proposed categories of consequences are similar to those used by the Department of Defense per Military Standard 882C. The consequence values and categories are described in Table 1. The goal is to estimate the relative consequence value associated with each undesired event.

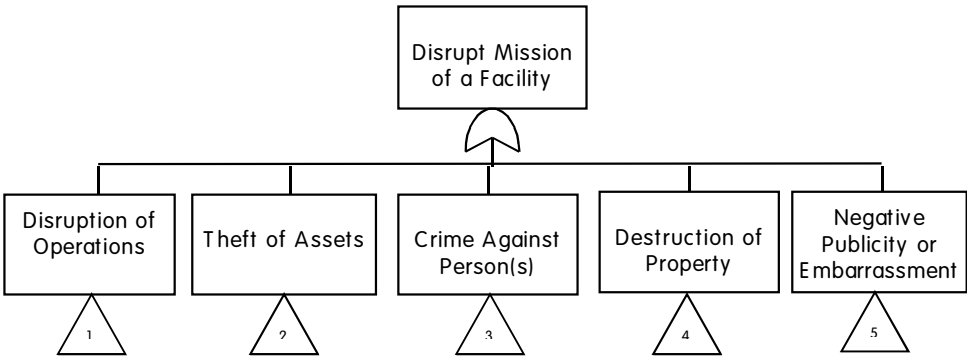


*Figure 2. Top Level Generic Fault Tree*

*Table 1. Consequence Categories and Associated Values*

| Consequence Category | Consequence Value |
|---|---|
| **Catastrophic-results in death(s), total mission loss, or severe environmental damage** | **Very high** |
| **Critical-results in severe injury/illness, major mission loss, or major environmental damage** | **High** |
| **Marginal-results in minor injury/illness, minor mission loss, or minor environmental damage** | **Medium** |
| **Negligible-results in less than minor injury/illness, less than minor mission loss, or less than minor environmental damage** | **Low** |

## 4. Threat Definition

**Threat-** Before a vulnerability analysis can be completed, a description of the threat is required. This description includes the type of adversary, tactics, and capabilities (number in the group, weapons, equipment, and transportation mode). Also, information is needed about the threat to estimate the likelihood that they might attempt the undesired events. The specific type of threat to a facility is referred to as the design basis threat (DBT). The DBT is often reduced to several paragraphs that describe the number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit.

The types of organizations that may be contacted during the development of a DBT description include local, state, and federal law enforcement (to include searching source material) and

related intelligence agencies. Local authorities should be able to provide reports on the type of criminal activities that are occurring and analytical projections of future activities. A review of literature may be conducted to include past incident reports associated with the site, local periodicals, professional journals, and other related material.

**Likelihood of Attack-** After the threat spectrum has been described, the information can be used together with statistics of past events and site-specific perception to categorize threats in terms of likelihood that each type of threat would attempt an undesired event. The DoD standard definitions [1] were modified in order to be used to categorize the threats. The modified DoD definition is based on the following characteristics:

*Existence*- the threat is assessed to be present or able to gain access to the area.

*Capability*- the threat is assessed to have, or has demonstrated, the level of capability to conduct the attack.

*Intention*- recent demonstrated activity or stated or assessed intent to conduct such activity exists.

*History*- demonstrated activity exists over time.

*Targeting*- current credible information indicates that the threat is preparing for a specific attack.

These definitions have been used to describe threat security levels. These levels are used to estimate the likelihood that the threat would undertake the undesired events. Figure 3 defines a process to estimate the likelihood of attack based on characteristics.

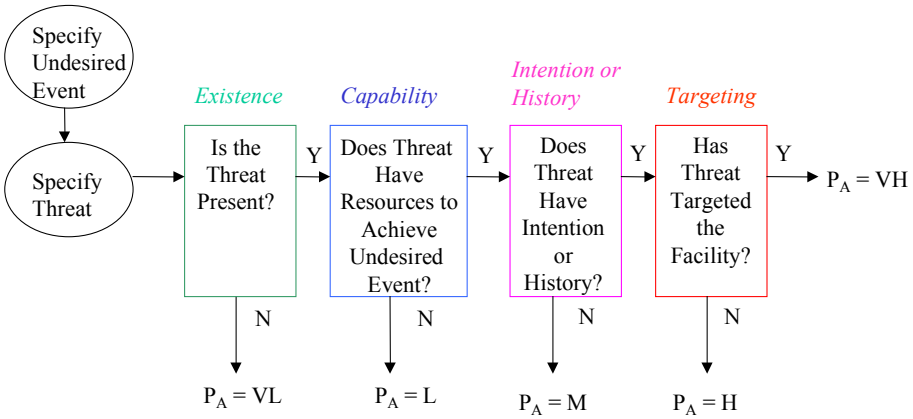


*Figure 3. Estimating Likelihood of Attack, $P_A$*

## 5. Protection System Effectiveness Analysis

Figure 4 describes the design and analysis process outline that can be used when estimating physical protection system effectiveness. The physical protection features must be described in detail before the security system effectiveness can be evaluated. An effective security system must be able to detect the adversary early and delay the adversary long enough for the security response force to arrive and neutralize the adversary before the mission is accomplished. In particular, an effective security system provides effective detection, delay, and response. These security system functions (detection, delay, and response) must be integrated to ensure that the adversary threat is neutralized before the mission is accomplished.

**DETECTION**, the first required function of a security system, is the discovery of adversary action and includes sensing covert or overt actions. In order to discover an adversary action, the following events must occur:

sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm
information from the sensor and assessment subsystems is reported and displayed
someone assesses information and determines the alarm to be valid or invalid. (If determined to be a nuisance alarm (defined below), detection has not occurred.)

Methods of detection include a wide range of technologies and personnel. Entry control, a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband, is included in the detection function of physical protection. Entry control, in that it includes locks, may also be considered a delay factor (after detection) in some cases. Searching for metal (possible weapons or tools) and explosives (possible bombs or breaching charges) is required for high-security
areas. This may be accomplished using metal detectors, x-ray (for packages), and explosive detectors.

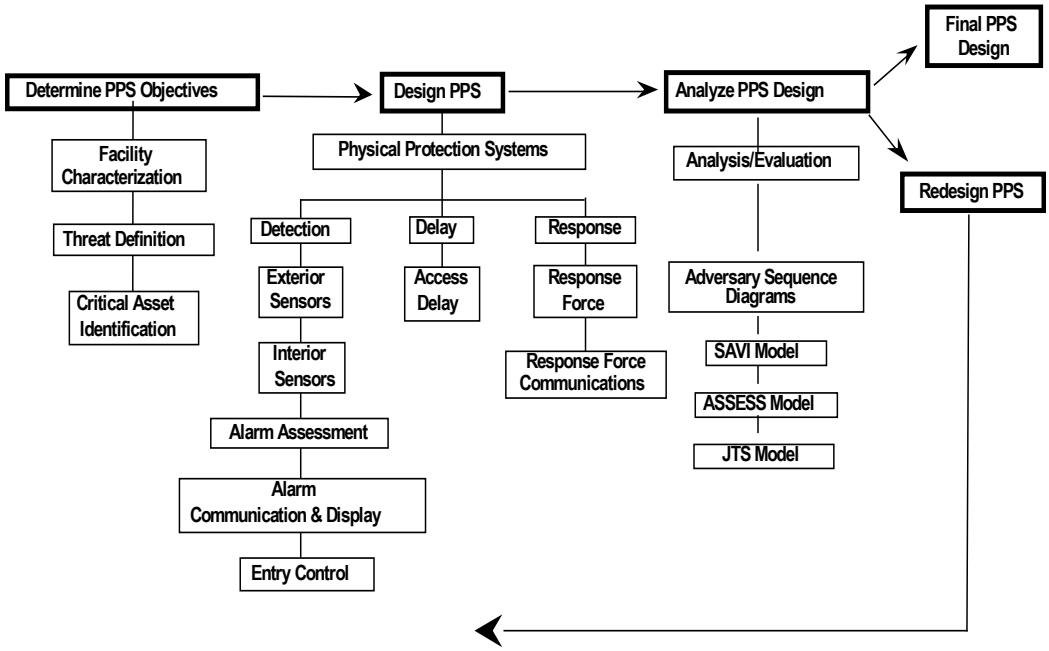


*Figure 4. Design and Evaluation Process Outline (DEPO)*

Security police or other personnel also can accomplish detection. Security police or other personnel can contribute to detection if they are trained in security concerns and have a means to alert the security force in the event of a problem. An effective assessment system provides two types of information associated with detection: (1) information about whether the alarm is a valid alarm or a nuisance alarm, and (2) details about the cause of the alarm, i.e., what, who, where, and how many. The effectiveness of the detection function is measured by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

**DELAY** is the second required function of a security system. It impedes adversary progress. Delay can be accomplished by fixed or active barriers, (e.g., doors, vaults, locks) or by sensor-activated barriers, e.g., dispensed liquids, foams. The security police force can be considered an element of delay if personnel are in fixed and well-protected positions. The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element.

**RESPONSE**, the third requirement of security systems, comprises actions taken by the security police force (police force or law enforcement officers) to prevent adversarial success. Response consists of interruption and neutralization. The measure of response effectiveness is the time between receipt of a communication of adversarial actions and the interruption and neutralization of the action. Interruption is defined as the response force arriving at the appropriate location to stop the adversary's progress. It includes the communication to the response force of accurate information about adversarial actions and the deployment of the response force. Neutralization is the act of stopping the adversary before the goal is accomplished. The effectiveness measures for neutralization are security police force equipment, training, tactics, and cover capabilities.

**Protection System Effectiveness-** Analysis and evaluation of the security system begin with a review and thorough understanding of the protection objectives and security environment. Analysis can be performed by simply checking for required features of a security system, such as intrusion detection, entry control, access delay, response communications, and a response force. However, a security system based on required features cannot be expected to lead to a high-performance system unless those features, when used together, are sufficient to ensure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a security system.

The Adversary Sequence Diagram (ASD) is a graphical representation of physical protection system elements along paths that adversaries can follow to accomplish their objective. For a specific physical protection system and threat, the most vulnerable path can be determined. This path with the least physical protection system effectiveness establishes the effectiveness of the total physical protection system. An ASD is developed for a single critical asset associated with an undesired event. Computer codes such as Systematic Analysis of Vulnerability to Intrusion (SAVI) and Analytic System and Software for Evaluating Safeguards and Security (ASSESS) can be used to determine the most vulnerable path. The neutralization module of ASSESS or Joint Tactical Simulation (JTS) can be used to estimate response force effectiveness.

## 6. Risk Estimation

RISK- **Risk is quantified by the following equation:**

$$R = P_A * (1-P_E) * C$$

Where: R = **risk associated with adversary attack**
$P_A$ = **likelihood of the attack**
$P_E$ = **probability security system is effective against the attack**
$(1 – P_E)$ = **probability that the adversary attack is successful (also the probability that security system is not effective against the attack)**
C = **consequence of the loss from the attack.**

## 7. Upgrades and Impacts

**System Upgrades-** If the estimated risk for the threat spectrum is judged to be unacceptable, upgrades to the system may be considered. The first step is to review all assumptions that were made that affect risk. All assumptions concerning undesired events, target identification, consequence definition, threat description, estimation of likelihood of attack, and safeguards functions should be carefully reevaluated. Upgrades to the system might include retrofits, additional safeguard features, or additional safety mitigation features. The upgraded system can then be analyzed to calculate any changes in risk due to change in likelihood of attack, system effectiveness, or consequence values. If the estimated risk for the upgraded system is judged to be acceptable, the upgrade is completed. If the risk is still unacceptable, the upgrade process of assumption review and system improvement should be repeated until the risk is judged to be acceptable.

**Upgrade Impact-** Once the system upgrade has been determined, it is important to evaluate the impacts of the system upgrade on the mission of the facility and the cost. If system upgrades put a heavy burden on normal operation, a trade-off would have to be considered between risk and operations. Budget can be the driver in implementing security upgrades. A trade-off between risk and total cost may have to be considered. When balance is achieved in the level of risk and upgrade impact on cost, mission, and schedule, the upgraded system is ready for implementation. At this point, the design/analysis process is complete.

## Methodology Summary

An analysis methodology for assessing the vulnerability of physical protection systems for facilities has been described. Vulnerability analyses for U.S. Mints and federal dams have been completed using the methodology. The methodology can be used to evaluate other important U.S. infrastructure components.

Henry H. Shelton, Joint Pub 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism, March 17, 1998.

Intentionally Left Blank

# APPENDIX D

## Risk Assessment Credibility Tool

(Also available in a web browser drill-down format for laptop computers)

Are the proposed activities and funding needs supported by a defensible security assessment?

**How was this assessment performed? (Process)**

1. What is the overall philosophy of the assessment?
   a. What component of the threat, consequence or asset is the primary focus?
   b. What kind of assessment was performed (e.g., vulnerability, risk, surety)?
   c. Is this a top-down (system level view), bottom-up (detailed component view rolled up to a system view), or hybrid approach?

2. What is the general framework for the assessment?
   a. Is the assessment process compliant with industry standard or generally accepted practice?
   b. What are the major components of the assessment (e.g., Characterize Assets, Determine Consequences, Define Threats, Define Safeguards, Analyze System, Evaluate Risk / Prioritize)
   c. Who performed this assessment?
      1) Do they primarily have experience in safety or in security risks?
      2) Are system managers involved in the assessment?
      3) Are users / operators of the system involved in the assessment?
   d. Is the system modeled?
   e. What automated / computer tools were utilized?
   f. How are the results presented and compared with other options / available results? (Decision Trees, rank lists, etc.)
   g. How much time was required to complete the assessment (man/months)?
   h. How often will the assessment need to be repeated? (months, years, eternity)
   i. What mechanisms can be or were used to verifying the accuracy, reproducibility and reasonableness of the analysis results?

3. Were prior assessments performed?
   a. When were they performed?
   b. Did they follow the process described above?
   c. Who performed these assessments?
   d. Did the current assessment use the results of previous assessments?
   e. How do the current results compare with the previous results? Why are they similar or different?
   f. How effective have the actions from these assessments been?

4. What is the description of the current assessment or proposed assessment?

a. When was/will the assessment be performed?
b. Who lead and who participated in the assessments?
    1) What were the roles for customer and analysts?
    2) Did outside experts participate? What were their roles?
    3) What were the interaction guidelines?
c. Did the assessment follow the general description listed above?
d. If the proposal is not based on a previous formal assessment, how is it justified?
e. How well do you understand the infrastructure system?
    1) Is there a cohesive but concise description of the overall infrastructure?
    2) Is there a list and description of major components and subsystems (e.g., SCADA systems), their functions and inter-relationships?
f. What other systems are directly dependent on this infrastructure?
g. On what other systems is this infrastructure dependent?
h. Are the analytic tools clearly identified?
i. Are the data/opinions underlying the assessment identified?
    1) What data were required to do the analysis?
    2) Has a justification of the data/opinions been included?
        (i) What is the source and pedigree of data used?
    3) Are there other sources of data available but not used?
    4) Are there other sources of data that exist but are unavailable?
j. Are the remedies proposed appropriate to the level of analysis detail?
k. How was the assessment ground truthed, calibrated, reviewed, red teamed?
    1) Are outside or independent experts involved?
l. What kind of uncertainty analysis has been performed?

**How much confidence is there that potential negative impacts and the key components of the infrastructure are adequately defined? (Assets and Consequences)**

1. Is the infrastructure or sub-system clearly defined?
   a. What is included?
   b. What is excluded?

2. Are the most important missions of the infrastructure or sub-system clear?
   a. What are the functions of the infrastructure?
   b. What failures could occur?

3. Are direct and indirect impacts of failure to achieve the mission or misuse of this infrastructure understood?
   a. What direct impacts are expected?
      1) What impacts are truly critical to the security of the United States?
      2) Are there differences in the short-term and long-term impacts?
      3) What protection mechanisms and approaches are currently in place?
      4) Can simultaneous failure of two or more infrastructures or systems cause a dramatically greater consequence?
   b. Is the location of consequences relevant?
      1) Who is impacted within facilities?
      2) Who is impacted in immediate geographic area?
      3) Who or what is impacted remotely?
   c. Does the duration of the consequence make the impact worse?
      1) How long can projected losses or consequences be accommodated?
      2) Are the consequences permanent?
      3) Do the consequences have a time delay?
      4) Do the consequences dissipate with time or do they grow worse?
   d. What dependent systems are compromised by a failure of this system?
      1) In what way are they compromised?
      2) Are the dependent systems robust / do they have redundancy?
   e. In what ways could this infrastructure or system be used as a weapon?
      1) Does the infrastructure provide access to secured facilities?
      2) Is the infrastructure in close proximity to large populations?
      3) Is the infrastructure inherently dangerous (i.e., explosive, corrosive)
      4) What components could be used to attack other infrastructures?
         (i) Could emission of hazardous materials occur?
         (ii) Could emission occur from the facility itself?
         (iii) Could theft of material and deliberate release occur?
      5) What skill level, training and resources are needed to use the system in this way?
      6) Is there evidence of this type of scenario in the past?

4. Are the measures of consequence understandable and consistent with metrics used for national prioritization?
   a. Are there qualitative or quantitative estimates of the consequences?
      1) What metrics are appropriate for this consequence?

2) How are consequences estimated?

b. How are importance levels determined/defined for each consequence?
   1) What is a "high" or "low" value for this consequence, and why?
      (i) e.g., Ex: deaths, illness or injury, economic impact, functional loss, behavioral change, public confidence, environmental consequences
   2) Is there a maximum tolerable level for this consequence?
      (i) Is there a minimum level of system performance that is essential?
      (ii) Is there some "catastrophic" level for this consequence that cannot be tolerated – regardless of likelihood?
   3) Is there a minimum level below, which this consequence doesn't matter?
c. Are there relative importance weights among the various metrics?

5. Are mitigating factors including the robustness of the infrastructure and current security measures adequately understood and included in the assessment?
   a. What security measures are currently in place?
   b. Who is responsible for these security measures?
   c. Have they been tested in any way?
   d. How does the infrastructure system prevented, mitigated, or remedied the consequences listed above for this direct infrastructure?
      1) Are there redundant systems to prevent or mitigate these direct impacts (either within or outside of this infrastructure/system)?
      2) Can the consequence be remediated? How quickly?
      3) How does one part of the infrastructure communicate problems to the rest of the infrastructures? How quickly?

**How much confidence is there that potential threats to and vulnerabilities of the infrastructure are adequately defined? (Threats and Vulnerabilities)**

1. Are components of the infrastructure that could cause any of the above-mentioned consequences (targets) clearly defined?
   a. What are the major components of the system?
   b. What targets (physical and cyber) are critical to these missions and concerns?

2. Are the currently identified system vulnerabilities clearly articulated?
   a. Are there physical vulnerabilities?
   b. Are there cyber vulnerabilities?
   c. Are there Personnel "social engineering" vulnerabilities?
   d. Are there Life Cycle vulnerabilities (e.g., planting something in the system long before it needs to be exploited for the attack)?
   e. Are there dependencies on other infrastructures that could cripple this infrastructure?
   f. Which vulnerabilities could be exploited to subvert these targets and/or produce the consequences described?

3. Are scenarios (sequence of actions or attacks) that might produce said consequence clearly understood and factored into selection of key vulnerabilities?
   a. What are the essential steps in the scenario?
   b. What is the time line for the scenario?
      1) How much time is required to complete the scenario?
      2) What is the time line of direct consequences as a result of the events in the scenario?
         (i) Time of onset, duration, and magnitude
         (ii) What elements are analyzed and what assumptions are made?
         (iii) What are the indirect consequences?
   c. What assumptions are made regarding emergency response to mitigate the stated consequences (make sure reasonable emergency response *already* factored into consequence estimates)?
   d. What is the likelihood of this scenario being detected in time to be interrupted?
   e. What is the likelihood this scenario can be completed if not interrupted?
   f. Can one forensically determine who is responsible for this to enable prosecution or retribution?

4. What are the most likely variations to this scenario?
   a. Scenarios that produce different consequence levels?
   b. Scenarios based on different adversary/threat characteristics?

5. How complete is the list of scenarios?
   a. Do the scenarios span the types of consequences described previously?
   b. Do the scenarios span the types of threats that might be encountered
      1) Do they consider: physical, cyber, and combinations thereof, various capabilities and levels of proficiency, threats both with and without insider participation, sudden and slow-acting scenarios

2) Do the scenarios consider interactions with other systems/infrastructures, and how "external" failures might push this system/infrastructure into a compromised condition?

6. Are adversary characteristics (people, financing and skills) required to exploit these vulnerabilities clearly articulated?

   a. How many people?
   b. What motivation would be necessary? (Ready to die?)
   c. What skills?
   d. What financing?
   e. What additional materials, tools and weapons would be required and which are available?
   f. What training and organization?
   g. Does it require insiders?
   h. What level of coordination and communication would be necessary?

**How confident are we that the proposed solutions will strengthen weaknesses in the infrastructure security? (Actions)**

1. Is there a clearly articulated roadmap (philosophy and systems view) to guide selection and implementation of more specific strategies and corrective actions to address the infrastructure security weaknesses?
   a. Is the approach piecemeal or systematic/system-wide?
   b. Did the analyst consider proposing actions that would affect each aspect of the scenario/consequence space?
      1) Is vulnerability removal/reduction (hardening) against each of the sources considered? (increasing the "degree of difficulty" for the attacker)
      2) Is increased surveillance (pre-incident alarms & surveillance) or improved forensics (post-incident) included?
      3) Is improved interdiction capabilities (improve likelihood that the scenario can be interrupted without consequences being realized) part of the solution?
         (i) Does the remedy allow a longer time to accomplish interdiction – i.e., increasing the time between detection and earliest time consequence-realizing steps could occur?
         (ii) Does the remedy improve response capabilities (interdictors stationed closer to target, etc.)?
      4) Were consequence prevention/reduction (e.g., removing the *source* of the consequence) considered?
      5) Was consequence mitigation (post-event emergency preparedness/operations) considered?
   c. If no actions are proposed for a particular aspect, why not?
      1) Were there no viable solutions found (too costly, minimal benefit, etc.)?
      2) Are there no viable solutions within the system/infrastructure owner's control or jurisdiction?

2. Are specific strategies, actions or sets of actions and their purpose clearly stated?
   a. What strategies and specific actions are proposed?
      1) What are the mitigation / prevention strategies?
      2) How do the proposed remedies deal with the identified vulnerabilities?
         (i) Have the proposed upgrades been analyzed?
         (ii) How were they analyzed or assessed?
         (iii) How much improvement is expected from the proposed upgrades?
         (iv) Will the actions provide protection against those scenarios that provide the adversary the *greatest* asymmetric advantage?
      3) What results can be obtained in which timeframe (changes in performance measures)?
         (i) What can be accomplished in the short term (1-3 months)?
         (ii) What can be accomplished over a longer-term?
         (iii) Which are the fastest, simplest and most cost effective methods?
      4) What uncertainties in technology, cost, schedule, etc exist?
   b. Is this course of action feasible?
      1) What is the current state of technology?

2) Is it administratively feasible?
3) Are there legal restrictions?
4) How functional / practical are these solutions?
5) What impact do these solutions have on primary functions and normal operations?
6) What will it cost?
7) Over what schedule can it be implemented?
8) What is the time of implementation?
9) Does this meet assumed deadlines?

c. What are the specific dependencies related to these actions?
   1) How does the effectiveness of the proposed action vary depending on whether other proposed actions do or do not move forward?
   2) Does this proposed action *assume* characteristics of other systems or infrastructures that have not yet been thoroughly verified?
   3) How would various answers to those assumptions affect the effectiveness of the proposed action?

d. Why are specific proposed actions assigned a high priority?
   1) To what degree do they avert the negative consequences listed above?
   2) Does this proposed action deal with averting a "catastrophic consequence" – one that is so severe that it cannot be tolerated under any circumstances?
   3) Does it provide a "uniform" level of protection? Or, does it leave significant "holes" at lower threat capability levels that really should be fixed first?
   4) Is this the right "mix" of actions?
   5) Why does this action need to be undertaken at all?
      (i) Are the consequences better or worse with the proposed action then the "no action" situation (where all scenarios remain un-addressed)?

3. Are the advantages of the proposed action clear?
   a. Which scenarios are addressed by this proposed action?
   b. How are these scenarios affected?
      1) Is the ability to observe the threat increased?
      2) Is the probability of detection increased?
      3) Is the degree of difficulty increased? (e.g., by adding additional required steps by the threat to achieve a disruption)
      4) Is the success likelihood reduced?
      5) Is the time scale of the scenario increased? (effects, detection, interruption probabilities)
      6) Are the consequences likely to be reduced?
         (i) Is a consequence made more difficult to achieve by removing a vulnerability or source (e.g., replacing gaseous Cl with solid Cl; fortifying the area where Cl gas is stored; improved Cl scrubbing capacity)?
         (ii) Are post-event responses improved to mitigate effects and reduce consequences?
      7) Are attacker requirements necessary to accomplish scenario greater? (better financing, materials, or skills required to exploit a vulnerability)

4. Are the disadvantages of the proposed action, if any, clear?

a. Which scenarios are not addressed by the proposed action?
b. Does the proposed action open up any new threat scenarios that were not previously viable?
    1) Are there completely new scenarios?
    2) What modifications occur to existing scenarios – especially changes that are "unfavorable?" (e.g., makes scenarios easier to conceal, more likely to succeed, easier to accomplish, etc.)?
c. What threat characteristics will be required to successfully carry out each of the scenarios after the proposed action?
d. What are the consequences resulting from each of the scenarios after the proposed action is taken?
e. What security gaps remain after the proposed action?

Intentionally Left Blank

Distribution:

| | | |
|---|---|---|
| 1 | MS-0101 | C. P. Robinson, 0001 |
| 1 | MS-0102 | J. B. Woodard, 0002 |
| 1 | MS-0513 | A. D. Romig, 1000 |
| 1 | MS-0457 | J. H. Stichman, 2000 |
| 1 | MS-0186 | D. H. Blanton, 3000 |
| 1 | MS-1231 | R. L. Hagengruber, 5000 |
| 10 | MS-0724 | R. J. Eagan, 6000 |
| 1 | MS-0918 | M. L. Jones, 7000 |
| 1 | MS-9001 | M. E. John, 8000 |
| 1 | MS-0151 | T. O. Hunter, 9000 |
| 1 | MS-0112 | F. A. Figueroa, 10000 |
| 1 | MS-0141 | M. R. Kestenbaum, 11000 |
| 1 | MS-0149 | J. L. Martinez, 14000 |
| 1 | MS-1221 | J. A. Tegnelia, 15000 |
| 1 | MS-0839 | G. Yonas, 16000 |
| 1 | MS-0701 | P. B. Davies, 6100 |
| 1 | MS-0741 | M. L. Tatro, 6200 |
| 1 | MS-0735 | T. E. Blejwas, 6400 |
| 1 | MS-0451 | S. G. Varnado, 6500 |
| 1 | MS-0771 | D. L. Berry, 6800 |
| 2 | MS-0769 | D. S. Miyoshi, 5800 |
| 10 | MS-0749 | A. B. Baker, 6010 |
| 1 | MS-0839 | R. L. Craft, 16000 |
| 1 | MS-9201 | P. K. Falcone, 8114 |
| 1 | MS-0961 | J. M. Harris, 14020 |
| 1 | MS-0157 | G. V. Herrera, 1310 |
| 1 | MS-0421 | W. C. Hines, 9810 |
| 1 | MS-0785 | R. L. Hutchinson, 6516 |
| 1 | MS-0425 | C. B. Layne, 9815 |
| 5 | MS-0762 | A. K. Moonka, 5801 |
| 1 | MS-1002 | M. L. Swinson, 15203 |
| 1 | MS-0735 | E. K. Webb, 6115 |
| 1 | MS-0451 | T. D. Woodall, 6502 |
| 1 | MS-0747 | G. D. Wyss, 6410 |
| 1 | MS-0451 | J. E. Nelson, 6518 |
| 1 | MS-0759 | I. G. Waddoups, 5845 |
| 1 | MS-0724 | C. M. Acosta, 6001 |
| 1 | MS-0724 | T. A. Mills, 6001 |
| 1 | MS-0724 | L. J. Segovia, 6000 |
| 1 | MS-0724 | K. J. Padilla, 6001 |
| 1 | MS-9018 | Central Technical Files, 8945-1 |
| 1 | MS-0899 | Technical Library, 9616 |
| 1 | MS-0612 | Review & Approval Desk, 9612<br>For DOE/OSTI |

Intentionally Left Blank