Order Code RL32561

CRS Report for Congress
Received through the CRS Web

Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences

Updated February 4, 2005

John Moteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
04 FEB 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service, The Library of Congress 101 Independence Ave, SE, Washington, DC 20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**28**	

Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences

Summary

The 9/11 Commission recommended that efforts to protect various modes of transportation and allocation of federal assistance to state and local governments should be based on an assessment of risk. In doing so, the Commission was reiterating existing federal policy regarding the protection of all the nation's critical infrastructures. The Homeland Security Act of 2002 (P.L. 107-296) and other Administration documents have assigned the Department of Homeland Security specific duties associated with coordinating the nation's efforts to protect its critical infrastructure, including using a risk management approach to set priorities. Many of these duties have been delegated to the Information Analysis and Infrastructure Protection (IA/IP) Directorate.

Risk assessment involves the integration of threat, vulnerability, and consequence information. Risk management involves deciding which protective measures to take based on an agreed upon risk reduction strategy. Many models/methodologies have been developed by which threats, vulnerabilities, and risks are integrated and then used to inform the allocation of resources to reduce those risks. For the most part, these methodologies consist of the following elements, performed, more or less, in the following order.

- identify assets and identify which are most critical
- identify, characterize, and assess threats
- assess the vulnerability of critical assets to specific threats
- determine the risk (i.e. the *expected* consequences of specific types of attacks on specific assets)
- identify ways to reduce those risks
- prioritize risk reduction measures based on a strategy

The IA/IP Directorate has been accumulating a list of infrastructure assets (specific sites and facilities). From this list the Directorate is selecting assets that have been judged to be critical from a national point of view. The Directorate intends to assess the vulnerability of all the assets on this shorter list. According to Directorate officials, vulnerability assessments and threat information are considered when determining the risk each asset poses to the nation. This risk assessment is then used to prioritize subsequent additional protection activities. The IA/IP Directorate's efforts to date, however, raise several concerns, ranging from the process and criteria used to populate its lists of assets, its prioritization strategy, and the extent to which the Directorate is coordinating its efforts with the intelligence community and other agencies both internal and external to the Department. This report will be updated as needed.

Contents

Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences

Introduction

As part of its chapter on a global strategy for protecting the United States against future terrorist attacks, the 9/11 Commission recommended that efforts to protect various modes of transportation and allocation of federal assistance to state and local governments should be based on an assessment of risk.[1] In doing so, the Commission was affirming existing federal policy regarding the protection of all the nation's critical infrastructures. The Homeland Security Act of 2002 and other Administration documents have assigned the Department of Homeland Security specific duties associated with coordinating the nation's efforts to protect its critical infrastructure. Many of these duties have been delegated to the Information Analysis and Infrastructure Protection (IA/IP) Directorate. In particular, the IA/IP Directorate is to integrate threat assessments with vulnerability assessments in an effort to identify and manage the risk associated with possible terrorist attacks on the nation's critical infrastructure. By doing so, the Directorate is to help the nation set priorities and take cost-effective protective measures.

This report is meant to support congressional oversight by discussing, in more detail, what this task entails and issues that need to be addressed. In particular, the report defines terms (e.g. threat, vulnerability, and risk), discusses how they fit together in a systematic analysis, describes processes and techniques that have been used to assess them, and discusses how the results of that analysis can inform resource allocation and policy.

While the IA/IP Directorate has been given this task as one of its primary missions, similar activities are being undertaken by other agencies under other authorities and by the private sector and states and local governments. Therefore, this report also discusses the Department's role in coordinating and/or integrating these activities.

---

[1] The Intelligence Reform and Terrorism Prevention Act of 2004 (S. 2845, P.L. 108-458), legislating some of the recommendations of the Commission's report, included a requirement to develop a National Strategy for Transportation Security that includes the development of risk-based priorities.

Background

IA/IP's Responsibilities

The Homeland Security Act of 2002 and other Administration documents have assigned the Department of Homeland Security specific duties associated with coordinating the nation's efforts to protect its critical infrastructure. Many of the duties discussed below have been delegated to the Information Analysis and Infrastructure Protection Directorate.

The *National Strategy for Homeland Security*,[2] anticipating the establishment of the Department of Homeland Security, stated:

- "... the Department would build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets across critical infrastructure sectors...[This assessment will] guide the rational long-term investment of effort and resources.[3]"
- "... we must carefully weigh the benefit of each homeland security endeavor and only allocate resources where the benefit of reducing risk is worth the amount of additional cost.[4]"

Among the specific tasks delegated to the Undersecretary for Information Analysis and Infrastructure Protection by Section 201(d) of the Homeland Security Act of 2002 (P.L. 107-296, enacted November 25, 2002) were:

- "... identify and assess the nature and scope of terrorist threats to the homeland;"
- "... understand such threats in light of actual and potential vulnerabilities of the homeland;"
- "... carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructures of the United States, including the performance of risk assessments to determine the risk posed by particular types of terrorist attacks within the United States ...."
- "... integrate relevant information, analyses, and vulnerability assessments ... in order to identify priorities for protective and support measures ...."
- "... develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States ...."
- "... recommend measures necessary to protect the key resources and critical infrastructure of the United States ...."

---

[2] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002.

[3] Ibid. p. 33.

[4] Ibid. p. 64.

The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* [5] stated:

- "DHS, in collaboration with other key stakeholders, will develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish federal, state, and local government, and the private-sector protection priorities. Using this methodology, DHS will build a comprehensive database to catalog these critical facility, systems, and functions.[6]"

Homeland Security Presidential Directive Number 7 (HSPD-7)[7] stated that the Secretary of Homeland Security was responsible for coordinating the overall national effort to identify, prioritize, and protect critical infrastructure and key resources. The Directive assigned Sector Specific Agencies[8] the responsibility of conducting or facilitating vulnerability assessments of their sector, and encouraging the use of risk management strategies to protect against or mitigate the effects of attacks against critical infrastructures or key resources. It also gave the Secretary to the end of calendar year 2004 to produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection.[9] That Plan shall include a strategy and a summary of activities to be undertaken to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources.

The terms "vulnerabilities," "threats," "risk," "integrated," and "prioritize" are used repeatedly in the documents cited above. However, none of the documents defined these terms or discussed how they were to be integrated and used. Also, in hearings, articles in the press, and other public discourse these terms are used loosely, clouding the intent of what is being proposed or discussed.[10] What might seem trivial

---

[5] Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* February 2003.

[6] Ibid. p. 23.

[7] Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003.

[8] The Clinton Administration referred to these as Lead Agencies in its Presidential Decision Directive Number 63 (PDD-63, May 1998). HSPD-7 supercedes PDD-63 in those instances where the two disagree.

[9] The Department did not meet this deadline. A draft plan is still in review. The Department intends to release elements of the plan in 2005. See, See CQ Homeland Security, Jan. 28, 2005, "Still Waiting: Plan to Protect Critical Infrastructure Overdue from DHS,"at [http://homeland.cq.com/hs/display.do?docid=1507251&sourcetype=31]. This site was last viewed on February 4, 2005. It is available only by subscription.

[10] Just as one example, the 9/11 Commission Report (released July 22, 2004, see page 396) when discussing the basis upon which federal resources should be allocated to states and localities, stated that such assistance should be based "strictly on an assessment of risks and vulnerabilities." Later, in the next paragraph, it stated "the allocation of funds should be based on an assessment of threats and vulnerabilities." In the next paragraph it stated that

(continued...)

differences in definitions can make a big difference in policy and implementation. The following section provides definitions and a generic model for integrating them in a systematic way.

A Generic Model for Assessing and Integrating Threat, Vulnerability, and Risk

Many models/methodologies have been developed by which threats, vulnerabilities, and risks are integrated and then used to inform the cost-effective allocation of resources to reduce those risks. For this report, CRS reviewed vulnerability assessment models or methodologies, including some developed and used, to varying degrees, in certain selected sectors (electric power, ports, oil and gas). These are listed in the Reference section of this report. In addition, this report draws upon information contained in a book by Carl Roper entitled *Risk Management for Security Professionals*.[11] Essential elements of these models/methods have been distilled and are presented below. They may provide some guidance in overseeing DHS's methodology as it is developed and employed.

For the most part, each of the methodologies reviewed consist of certain elements. These elements can be divided into: assessments per se; and, the use of the assessments to make decisions. The elements are performed, more or less, in the following sequence:

Assessments
- identify assets and identify which are most critical
- identify, characterize, and assess threats
- assess the vulnerability of critical assets to specific threats
- determine the risk (i.e. the *expected* consequences of specific types of attacks on specific assets)

Using Assessments to Identify and Prioritize Risk Reduction Activities
- identify and characterize ways to reduce those risks
- prioritize risk reduction activities based on a risk reduction strategy

Assessments.

Identifying Assets and Determining Criticality. The infrastructure of a facility, a company, or an economic sector, consists of an array of assets which are necessary for the production and/or delivery of a good or service. Similarly, the infrastructure of a city, state, or nation consists of an array of assets necessary for the economic and social activity of the city and region, and the public health and welfare of its citizens. The first step in the process is to determine which infrastructure assets to include in the study. The American Chemistry Council, the Chlorine Institute, and the Synthetic Organic Chemical Manufacturers Association, in their *Site Security*

---

[10] (...continued)
resources "must be allocated according to vulnerabilities."

[11] Roper, Carl. A. Risk Management for Security Professionals, Butterworth-Heinemann. 1999.

Guidelines for the U.S. Chemistry Industry, broadly define assets as people, property, and information. Roper's *Risk Management for Security Professionals* (and DOE's *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities*) broadly define assets as people, activities and operations, information, facilities (installations), and equipment and materials.

The methodologies reviewed do not provide a definitive list of such assets but suggest which ones might be considered. For example, people assets may include employees, customers, and/or the surrounding community. Property usually includes a long list of physical assets like buildings, vehicles, production equipment, storage tanks, control equipment, raw materials, power, water, communication systems, information systems, office equipment, supplies, etc. Information could include product designs, formulae, process data, operational data, business strategies, financial data, employee data, etc. Roper's examples of activities and operations assets include such things as intelligence gathering and special training programs. Many methodologies suggest considering, initially, as broad a set of assets as is reasonable.

However, not every asset is as important as another. In order to focus assessment resources, all of the methodologies reviewed suggest that the assessment should focus on those assets judged to be most critical. Criticality is typically defined as a measure of the consequences associated with the loss or degradation of a particular asset. The more the loss of an asset threatens the survival or viability of its owners, of those located nearby, or of others who depend on it (including the nation as a whole), the more critical it becomes.

Consequences can be categorized in a number of ways: economic; financial; environmental; health and safety; technological; operational; and, time. For example, a process control center may be essential for the safe production of a particular product. Its loss, or inability to function properly, could result not only in a disruption of production (with its concomitant loss of revenue and additional costs associated with replacing the lost capability), but it might also result in the loss of life, property damage, or environmental damage, if the process being controlled involves hazardous materials. The loss of an asset might also reduce a firm's competitive advantage, not only because of the financial costs associated with its loss, but also because of the loss of technological advantage or loss of unique knowledge or information that would be difficult to replace or reproduce. Individual firms, too, have to worry about loss of reputation. The American Petroleum Institute and the National Petrochemical and Refiners Association (API/NPRA) in their *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries* also suggested considering the possibility of "excessive media exposure and resulting public hysteria that may affect people that may be far removed from the actual event location.[12]"

---

[12] American Petroleum Institute and the National Petrochemical and Refiners Association, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, May 2003, p. 4.

While the immediate impact is important, so, too, is the amount of time and resources required to replace the lost capability. If losing the asset results in a large immediate disruption, but the asset can be replaced quickly and cheaply, or there are cost-effective substitutes, the total consequence may not be so great. Alternatively, the loss of an asset resulting in a small immediate consequence, but which continues for a long period of time because of the difficulty in reconstituting the lost capability, may result in a much greater total loss.

Another issue which decision makers may consider is if the loss of a particular asset could lead to cascading effects, not only within the facility or the company, but also cascading effects that might affect other infrastructures. For example, the loss of electric power can lead to problems in the supply of safe drinking water. The loss of a key communications node can impair the function of ATM machines.

The initial set of assets are categorized by their degree of criticality. Typically the degree of criticality is assessed qualitatively as high, medium, or low, or some variation of this type of measure. However, even if assessed qualitatively, a number of methodologies suggest being specific about what kind of consequence qualifies an asset to be placed in each category. For example, the electric utility sector methodology suggests that a highly critical asset might be one whose loss would require an immediate response by a company's board of directors, or whose loss carries with it the possibility of off-site fatalities, property damage in excess of a specified amount of dollars, or the interruption of operations for more than a specified amount of time. Alternatively, an asset whose loss results in no injuries, or shuts down operations for only a few days, may be designated as having low criticality.

For those sectors not vertically integrated, ownership of infrastructure assets may span a number of firms, or industries. Whoever is doing the analysis may feel constrained to consider only those assets owned and operated by the analyst or analyst's client. For example, transmission assets (whether pipeline, electric, or communication) may not be owned or operated by the same firms that produce the commodity being transmitted. Both the production assets and the transmission assets, however, are key elements of the overall infrastructure. Also, a firm may rely on the output from a specific asset owned and operated by someone else. The user may consider that asset critical, but the owner and operator may not. Some of the methodologies reviewed encourage the analyst to also consider (or at least account for) the vulnerability of those assets owned or operated by someone else that provide critical input into the system being analyzed. These "interdependency" problems have been talked about, mainly in the context of inter-sector dependencies (e.g the reliance of water systems on electric power), but they may also exist intra-sector. The interdependency issue is both a technical one (i.e. identifying them) and a political/legal one (i.e. how can entity A induce entity B to protect an asset).

Identify, Characterize, and Assess Threat. Roper and the API/NPRA define threat as "any indication, circumstance or event with the potential to cause loss

or damage to an asset.[13]" Roper includes an additional definition: "The intention and capability of an adversary to undertake actions that would be detrimental to U.S. interests.[14]"

To be helpful in assessing vulnerability and risk, threats need to be characterized in some detail. Important characteristics include type (e.g. insider, terrorist, military, or environmental (e.g. hurricane, tornado)); intent or motivation; triggers (i.e events that might initiate an attack); capability (e.g. skills, specific knowledge, access to materials or equipment); methods (e.g. use of individual suicide bombers, truck bombs, assault, cyber); and trends (what techniques have groups used in the past or have experimented with, etc.).

Information useful to characterizing the threat can come from the intelligence community, law enforcement, specialists, news reports, analysis and investigations of past incidents, received threats, or "red teams" whose purpose is to "think" like a terrorist. Threat assessment typically also involves assumptions and speculation since information on specific threats may be scant, incomplete, or vague.

Once potential threats have been identified (both generically, e.g. terrorists, and specifically, e.g. Al Qaeda) and characterized, a threat assessment estimates the "likelihood of adversary activity against a given asset or group of assets.[15]" The likelihood of an attack is a function of at least two parameters: a) whether or not the asset represents a tempting target based on the goals and motivation of the adversary (i.e. would a successful attack on that asset further the goals and objectives of the attacker); and, b) whether the adversary has the capability to attack the asset by various methods. Other parameters to consider include past history of such attacks against such targets by the same adversary or by others, the availability of the asset as a target (e.g. is the location of the target fixed or does it change and how would the adversary know of the target's existence or movement, etc.). The asset's vulnerability to various methods of attack (determined in the next step) may also affect the attractiveness of the asset as a target.

As an example of a threat assessment technique, the U.S. Coast Guard, using an expert panel made up of Coast Guard subject matter and risk experts, evaluated the likelihood of 12 different attack modes against 50 different potential targets (i.e. 600 scenarios). Attack modes included "... boat loaded with explosives exploding along side a docked tank vessel," or "... tank vessel being commandeered and intentionally damaged." The Coast Guard also considered scenarios where port assets could be stolen or commandeered and used as a weapon or used to transport terrorists or terrorism materials. Potential targets included various types of vessels (including ferries), container facilities, water intakes, utility pipelines, hazardous materials

---

[13] American Petroleum Institute, op. cit., p. 5.

[14] Roper, op. cit. , p. 43.

[15] This quote is taken from the Government Accountability Office testimony, *Homeland Security: Key Elements of a Risk Management Approach,* GAO-02-150T, before the Subcommittee on National Security, Veteran's Affairs, and International Relations, House Committee on Government Reform, October 21, 2001. It is used in several of the other methodologies reviewed.

barges, etc. The panel of experts judged the credibility of each scenario. For example, using a military vessel for transporting terrorists or terrorism materials was judged not to be credible given the inherent security measures in place, but an external attack on a military target was considered credible. Each credible scenario was assigned one of 5 threat levels representing the perceived probability (likelihood) of it occurring, after considering the hostile group's intent, its capabilities, prior incidents, and any existing intelligence.

The Electricity Sector's methodology uses a checklist which asks for the specific attack mode (such as the use of explosives, truck bomb, or cyber attack) and whether it is likely that such an attack would be carried out by: a) an individual; or b) by an assault team of up to five members. In this case, the analyst is to identify likely targets for each type of attack scenario and the objective that the adversary would achieve by such an attack.

Likelihood can be measured quantitatively, by assigning it a probability (e.g. an 85% chance of occurring), or qualitatively, such as "Very High Threat Level," which might mean there is a credible threat, with a demonstrated capability, and it has happened before. As with criticality, a number of methodologies suggested specific criteria be used to define what would constitute varying threat levels.

A threat assessment need not be static in time. Threats (i.e. the likelihood that an adversary may attack) may rise and fall over time, depending on events, anniversary dates, an increase in capability, or the need for the adversary to reassert itself. Intelligence may detect activity that indicates pre-attack activity or a lull in such activity, or an explicit threat may be made.

Assess Vulnerability. Roper defines vulnerability as a "weakness that can be exploited to gain access to a given asset.[16]" The API/NPRA expands this definition to include "... and subsequent destruction or theft of [the] ... asset.[17]" The Coast Guard defines vulnerability as "the conditional probability of success given that a threat scenario occurs.[18]"

Weaknesses, like criticality, can be categorized in a number of ways: physical (accessibility, relative locations, visibility, toughness, strength, etc.), technical (susceptible to cyber attack, energy surges, contamination, eavesdropping, etc.), operational (policies, procedures, personal habits), organizational (e.g. would taking out headquarters severely disrupt operations), etc.

Existing countermeasures may already exist to address these weaknesses. A vulnerability assessment must evaluate the reliability and effectiveness of those existing countermeasures in detail. For example, security guards may provide a certain degree of deterrence against unauthorized access to a certain asset. However,

---

[16] Roper, op. cit., p. 63.

[17] American Petroleum Institute, op. cit., p. 5.

[18] Federal Register, Department of Homeland Security, Coast Guard, *Implementation of National Maritime Security Initiatives*, Vol. 68, No. 126, July 1, 2003, p. 39245.

to assess their effectiveness, a number of additional questions may need to be asked. For example, how many security guards are on duty? Do they patrol or monitor surveillance equipment? How equipped or well trained are they to delay or repulse an attempt to gain access? Have they successfully repulsed any attempt to gain unauthorized access?

Vulnerabilities are assessed by the analyst against specific attacks. API/NPRA identifies three steps to assessing vulnerabilities: 1) determine how an adversary could carry out a specific kind of attack against a specific asset (or group of assets); 2) evaluate existing countermeasures for their reliability and their effectiveness to deter, detect, or delay the specific attack; and 3) estimate current state of vulnerability and assign it a value. Specific types of attacks can be informed by the preceding threat assessment.

The Coast Guard measured vulnerability of potential targets for each attack scenario in four areas: 1) is the target available (i.e. is it present and/or predictable as it relates to the adversary's ability to plan and operate); 2) is it accessible (i.e. how easily can the adversary get to or near the target); 3) what are the "organic" countermeasures in place (i.e. what is the existing security plan, communication capabilities, intrusion detection systems, guard force, etc.); and, 4) is the target hard (i.e. based on the target's design complexity and material construction characteristics, how effectively can it withstand the attack). Each of these four vectors were evaluated on a level of 1 to 5, with each level corresponding to a assigned probability of a successful attack. By comparison, the electricity sector process measures vulnerability as a probability that existing countermeasures can mitigate specific attack scenarios (e.g. probability of surviving attack = 80%).

Alternatively, the analyst can value vulnerability qualitatively. For example, a "highly vulnerable" asset might be one that is highly attractive as a target, for which no countermeasures currently exist against a highly credible threat. An asset with low vulnerability might be one that has multiple effective countermeasures.

Assess Risk. Risk implies uncertain consequences. Roper defines risk as the "... probability of loss or damage, and its impact ..."[19] The Coast Guard refers to a risk assessment as " essentially an estimate of the expected losses should a specific target/attack scenario occur."[20] "Expected" loss is determined by multiplying the estimated adverse impact caused by a successful threat/attack scenario by the probabilities associated with threat and vulnerability. API/NPRA defines risk as "a function of: consequences of a successful attack against an asset; and, likelihood of a successful attack against an asset."[21] "Likelihood" is defined as "a function of: the attractiveness of the target to the adversary [based on the adversary's intent and the target's perceived value to the adversary], degree of threat [based on adversary's

---

[19] Roper, op. cit., p. 73.

[20] Federal Register, op. cit., p. 39245.

[21] American Petroleum Institute, op. cit., p. 3.

capabilities], and degree of vulnerability of the asset.[22]" An important point is that risk, as defined here, is a discounted measure of consequence; i.e. discounted by the uncertainty of what might happen (see the example given below).

As noted in the first step, impact can be categorized in a number of ways. Impact or consequences may be measured more precisely at this point in the process, however, to better inform the prioritization of risk reduction steps that follows.

The Coast Guard considered six categories of impact: death/injury; economic; environmental; national defense; symbolic effect; and secondary national security issues. Each target/attack scenario measured the potential impact in each of these categories on a severity scale from 1 to 5 (from low to catastrophic). The assigned scale value was based on benchmarks. The API/NPRA, which used a similar construct, suggested the following benchmarks for its severity scale. The severity of death and injury varied from high to low depending on whether they occurred off-site or on-site, and whether they were certain or possible. The severity of environmental damage again varied from high to low depending on whether it was large scale (spreading off-site) or small scale (staying on-site). The severity of financial losses or economic disruptions were valued on threshold dollar amounts and time-frames.

The analyst can also try to measure risk quantitatively. For example, for a specific target/attack scenario, the analysis may determine that there is a 50/50 chance (i.e. we don't know) that the adversary will try to attack a particular government building. But, if they did, there is a 75% chance that they would use a truck bomb (i.e we are pretty sure that if they attack they would try to use a truck bomb). If they try use a truck bomb, the vulnerability assessment determined that they would have a 30% chance of succeeding (i.e. if they try, there is a good chance that the current protective measures will prevent them from getting close enough to the building to bring it down). The consequences of a successful attack (bringing the building down) could be 500 people killed and $300 million in property damage.[23] The risk associated with this scenario would be:

> expected loss = (consequence) x (probability that an attack will occur) x (conditional probability that the attacker uses a truck bomb) x (the conditional probability that they would be successful)[24], or
>
> (500 people killed + $300 million in damage) x (.5) x (.75) x (.3), or

---

[22] Ibid.

[23] Consequences, too, could be uncertain. For example, it may be determined that in the above scenario, a successful attack may cause a distribution of possible deaths between zero and 500 people.

[24] This formulation assumes that the uncertainties in this case are independent, which in many cases is not accurate. The attractiveness of a target (an element in determining threat) may very much depend on its vulnerability. Likewise, the consequence of an attack may also depend on a target's vulnerability. This complicates the calculation.

risk = 56 expected deaths and $33.8 million in expected damages.[25]

Risk is often measured qualitatively (e.g. high, medium, low). Since consequences may be measured along a number of different vectors, and threat and vulnerability have been measured separately, a qualitative measure of risk must have some criteria for integrating the number of different qualitative measures. For example, how should the assessment decide what risk rating to give a medium threat against a highly vulnerable target that would have a low death/injury impact, a medium environmental impact, but a high short-term financial impact? Does this scenario equal a high, medium, or low level of risk?

Using Assessments to Identify and Prioritize Risk Reduction Activities.

Identify Ways to Reduce Risk. Risks can be reduced in a number of ways: by reducing threats (e.g. through eliminating or intercepting the adversary before he strikes); by reducing vulnerabilities (e.g. harden or toughen the asset to withstand the attack); or, by reducing the impact or consequences (e.g. build back-ups systems or isolate facilities from major populations). For each potential countermeasure, the benefit in risk reduction should also be determined.[26] More than one countermeasure may exist for a particular asset, or one countermeasure may reduce the risk for a number of assets. Multiple countermeasures should be assessed together to determine their net effects. The analyst should also assess the feasibility of the countermeasure.

The cost of each countermeasure must also be determined. Costs, too, are multidimensional. There may be up-front financial costs with associated materials, equipment, installation, and training. There are also longer term operational costs of the new protective measures, including maintenance and repair. There may also be operational costs associated with changes to overall operations. Costs also include time and impact on staff, customers, and vendors, etc. Expenditures on the protection of assets also results in opportunity costs, i.e. costs associated with not being able to invest those resources in something else.

Prioritize and Decide In What to Invest. Once a set of countermeasures have been assessed and characterized by their impact on risk, feasibility, and cost, priorities may be set. Decision makers would have to come to a consensus on which risk reduction strategy to use to set priorities.

Most of the methods reviewed suggest a cost-effective selection process (i.e. implementation of the risk-reduction method(s) should not cost more than the benefit

---

[25] Note: the risk in this scenario is not 500 people dead, but 56 expected deaths. That is not to say that if an attack were actually successfully carried out only 56 people might die. In fact, in this scenario, it has been judged that 500 people would likely die. If one chose to use the 500 potential deaths in subsequent decisions, they would be called risk averse in this construct. Taking a risk averse position is a legitimate policy option. See further discussion on risk aversion below.

[26] Again, dependencies between threat, risk, and consequences need to be considered.

derived by the reduced risk). Cost-effectiveness could also imply that the country invest in risk reduction to the point where the marginal cost to society equals the marginal benefit. Alternatively, given a fixed budget, cost-effectiveness might imply investing in protections that maximize the benefits for that investment. Countermeasures that lower risk to a number of assets may prove to be most cost-effective. Also, focusing attention on those assets associated with the highest risks may yield the greatest risk reduction and be one way to implement a cost-effective approach.

While cost-effectiveness is usually the recommended measure for setting priorities, decision makers may use others. For example, decision makers may be risk averse. In other words, even if the chance of an attack is small, or the potential target is not particularly vulnerable, the consequences may be too adverse to contemplate. In this case, decision makers may wish to bear the costs of additional protection that exceed the "expected" reduction in risk. Roper notes, however, that, in general, protection costs should not exceed a reasonable percentage of the total value of the asset.[27]

Another measure by which to select protective actions might be to favor maximizing the number or geographical distribution of assets for which risks are reduced. Alternatively, decision makers might want to focus efforts on reducing a specific threat scenario (e.g. dirty bombs) or protecting specific targets (e.g. events where large numbers of people attend).

The electric utility checklist states that the ultimate goal of risk management is to select and implement security improvements to achieve an "acceptable level of risk" at an acceptable cost. The concept of acceptable risk is mentioned in a number of methodologies, and it needs to be determined by decision makers.

After selecting which protective measures to pursue, programs, responsibilities, and mechanisms for implementing them must be established. Many of the reviewed methodologies conclude with the recommendation to revisit the analysis on a regular basis.

Status of DHS's Implementation of Its Critical Infrastructure Protection Effort

Programming. The IA/IP Directorate's FY2005 budget justification document provided a glimpse into how DHS intends to implement its responsibilities in critical infrastructure protection. Below is a list of budget activities that most relate to the topic of this report.

- *Threat Determination and Assessment:* This activity involves the development of tools and techniques to help model terrorist organizations, to develop a terrorist capabilities baseline, and to facilitate collaboration and fusion of intelligence information and the coordinated analysis of that information.

---

[27] Roper, op. cit., p. 88.

- *Critical Infrastructure and Asset Identification:* This activity involves identifying critical infrastructure and assets, assessing potential risk of successful attacks to those assets, and prioritizing protective measures.

- *Critical Infrastructure Vulnerability and Field Assessments:* This activity supports specialized teams of experts that are sent to high priority sites to assess their vulnerabilities.

- *Infrastructure and Key Asset Protection Implementation:* This activity supports an array of services offered by the IA/IP Directorate to assist state, local, and private stakeholders in risk mitigation measures for high priority assets. These services include training, protection and response planning, pilot programs, technology transfers, and sharing of best practices.

- *National Infrastructure Risk Analysis:* This activity supports the development of comprehensive risk and vulnerability analyses on a national scale. These analyses are cross-sector in nature, focusing on problems affecting multiple infrastructures. The goal is to provide timely, actionable information that is more meaningful to industry. It is not clear how this activity differs from the Critical Infrastructure and Asset Identification activity mentioned above.

- *Threat/Vulnerability/Asset Databases:* This activity supports the development, operation, and maintenance of an integrated data warehouse of threat, vulnerability, and risks posed to specific facilities and assets (including the probability of attack and associated consequences). The description of this activity implies that data would be located in disparate places, and technology would be developed to allow access and integration of the information.

- *Competitive Analysis and Evaluation:* This activity supports activities that evaluate the effectiveness of IA/IP products and processes. This could involve "red teaming" to test, via exercises, gaming, and alternate hypothesizing analyses, IA/IP assessments and protective actions.

Progress. Testimony given by the Undersecretary for Information Analysis and Infrastructure Protection, Frank Libutti, before the House Appropriations Committee's Subcommittee on Homeland Security, April 1, 2004, provided another glimpse into the IA/IP Directorate's process and progress in integrating threat, vulnerability, and risk and using that information to set help set priorities. In that testimony, the Undersecretary stated that the Directorate had 28,000 sites or facilities in a national infrastructure database. A few days later, this number had grown to

33,000.[28] By the end of 2004, the number of assets in the database has reportedly reached 80,000.[29] According to the testimony, these are sites, facilities, and assets that state Homeland Security Advisers have identified as being critical. They include public and private assets.

According to the above testimony, the Directorate, working with state, local, and private stakeholders, had identified 1,700 assets from the larger list on which it intends to conduct, or lead, vulnerability field assessments.[30] Presumably, these assets have been identified by IA/IP as being the most critical. According to the testimony, IA/IP intended to lead vulnerability assessments teams to each of these 1,700 assets in 2004.[31] Based on these vulnerability assessments and the associated risk (the Undersecretary did not elaborate on how risk would be determined), the Undersecretary stated that IA/IP intends to follow-up with asset owners/operators to help them develop "operational plans" for improving the security (both physical and cyber) of these assets, if needed.

A statement by the Director of the Protection Services Division (a division within the IA/IP Directorate), James McDonnell, before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Affairs, and the Census on March 30, 2004 offered some additional insight. According to his statement, the IA/IP Directorate identified those sites or assets that may be most attractive as targets and have sent or plan to send a team of specialized security experts to the site to assess its vulnerabilities and how those vulnerabilities might be exploited. The IA/IP Directorate then maps threat and vulnerability information to determine risk. Base on the risk information, the Directorate then prioritizes the implementation of protective measures that address vulnerabilities. No where in this statement are the criteria that govern these decisions (assessing target attractiveness, mapping threat and vulnerability to determine risk, prioritization) mentioned.

According to the Director, protective measures focus on near-term technical and procedural changes that can harden the site against attack. The FY2005 budget request referred to the type of protective measures that IA/IP may recommend. These included 1) including the detection of weapons of mass destruction in the development of protection plans; 2) measures to disrupt attack planning by making information gathering and surveillance by terrorist difficult; and 3) ensure counter-

---

[28] The article cited below makes reference to testimony by the Undersecretary before a joint hearing of the House Select Committee's subcommittees on Cybersecurity, Science and Research & Development and Infrastructure and Border Security held on April 21, 2004. See, [http://www.fcw.com/geb/articles/2004/0419/web-assets-04-21-04.asp], "DHS needs asset info." This site was last visited on February 4, 2005.

[29] See, "Terror Target List Way Behind," USA Today, December 9, 2004. p.A1.

[30] It is not clear if this number, too, has grown since the testimony was given.

[31] Report language in the Senate Appropriations Committee's report accompanying its FY2005 Department of Homeland Security Appropriations bill (see reference below) stated that 150 of these were expected to be completed in FY2004, with another 400 expected to be completed in FY2005. This only would be about one third of the 1700 assets which IA/IP had said it would like to assess by the end of the calender year, 2004.

assault capabilities. The Senate Appropriations Committee's report on DHS's appropriation bill[32] made reference to Buffer Zone Protection Plans (BZPP) which the Protective Services Division assists stakeholders in developing. The Director, in the statement cited above, described the BZPP as being a community-based approach, incorporating local law enforcement and emergency personnel into a security plan that extends beyond the fence (i.e. outside the property limits of the site or facility).

In addition to the above mentioned efforts, and as required by HSPD-7, the IA/IP Directorate is in the process of developing a national plan for protecting critical infrastructure. The national plan will use as its foundation sector-level plans, to be developed cooperatively by Sector Specific Agencies and representatives of their sector. According to testimony by DHS officials responsible for the transportation sector,[33] these sector level plans are in progress (at least within the Transportation Security Administration and the Coast Guard). The IA/IP Directorate has prepared guidance for developing Sector Specific Plans that contain many of the steps discussed in the generic model above, and which require Sector Specific Agencies to be specific about methodology, criteria, etc.

From the above discussion it appears the IA/IP Directorate is in the process of carrying out the fundamental steps identified in the preceding discussion. However, some questions and issues remain.

Questions and Issues

Identifying Assets

By the end of 2004, the IA/IP Directorate has compiled a list of 80,000 assets. Policy makers, from both sides of the aisle, however, have raised several concerns about this list.[34] From where does the information for this list come? Is there a systematic approach to generating this list? How comprehensive is it? How accurate is the data? In what form does this information exist?

According to the testimony of the Undersecretary discussed above, the list is populated by assets identified by state Homeland Security Advisors. The process by which the states have provided this information is not discussed in the testimony. However, according to Democratic members of the House Select Committee on

---

[32] U.S. Congress, Senate, Appropriations Committee, Report accompanying S. 2537, S.Rept. 108-280, June 17, 2004.

[33] Stephen McHale, Deputy Administrator, Transportation Security Administration, Statement before the Subcommittee on Infrastructure and Border Security, House Select Committee on Homeland Security, May 12, 2004. Also, Rear Admiral David S. Belz, Assistant Commandant for Operations, U.S. Coast Guard, et.al., Statement before the House Select Committee on Homeland Security, May 5, 2004.

[34] See, "Terror Target List Way Behind," USA Today, December 9, 2004. p. A1.

Homeland Security, in a letter to the Secretary of Homeland Security,[35] DHS's efforts to coordinate submissions by the states' Homeland Security Advisors have not included specific guidelines or a specific reporting mechanism, and in some cases, state officials contend they were never contacted even though assets from their states appear on the list.

There is a mechanism in place by which the IA/IP could received state and local information on critical infrastructure assets. The Office of State and Local Government Coordination and Preparedness (OSLGCP) administers two grant programs that give states the opportunity to identify critical infrastructure assets: the State Homeland Security Grant Program and the Urban Area Security Initiative Grants, both of which are to be submitted through a state's designated Homeland Security Advisor. While both of these grant programs focus primarily on the needs of first responders, they both also support activities related to critical infrastructure protection, including the purchase of equipment such as chemical, biological, radiological, nuclear, and explosive (CBRNE) detectors, physical security equipment such as surveillance cameras, fences, cybersecurity hardware and software, interoperable communications equipment, etc.

Allocation of funds through the State grant program is based on a formula determined by Congress in the U.S.A. PATRIOT Act (P.L. 107-56). All states, the District of Columbia, and U.S. territories receive funds. States must develop a State Homeland Security Strategy before they can spend their funds.

Urban Areas grants (to which have been added Port Security Grants and Transit System Security Grants) are allocated to cities, selected by DHS, based on a formula developed by the Office of Domestic Preparedness (ODP).[36] While the grant application guidelines do not elaborate, the formula considers current threat estimates, critical assets within the urban area, and population density. According to the application guidelines, grantees must provide a risk assessment for review. The risk assessment must also include threat and vulnerability assessments.[37] The

---

[35] The letter, dated August 3, 2004, is available on the Democrat's Select Committee on Homeland Security website: see [http://www.house.gov/hsc/democrats]. The letter was last viewed at this site on February 4, 2004 and can be found on the Critical Infrastructure link.

[36] The Office of Domestic Preparedness (ODP) was transferred from the Department of Justice to the Department of Homeland Security by the Homeland Security Act of 2002. The ODP has since been integrated with the Office of State and Local Government Coordination, established by the Homeland Security Act, into the Office of State and Local Government Coordination and Preparedness (OSLGCP). The OSLGCP now administers the grants programs.

[37] According to the guidance, threat assessment determines the relative likelihood of a known potential threat element attempting to attack using a weapon of mass destruction. A potential threat element includes any group or individual in which there are allegations or information indicating a possibility of the unlawful use of force or violence, specifically the utilization of weapons of mass destruction. Threat factors include evidence of the existence, violent history, intentions, motivations, targeting, and weapons of mass destruction capability of a known potential threat element. For each potential target, the vulnerability assessment is to consider factors such as target visibility, its criticality to the

(continued...)

risk assessment informs a capabilities and a needs assessment also required of the states. The states must submit these assessments to qualify for the grant and to justify their expenditures of grant resources.

Assets eligible for protection in either grant program include drinking water systems; primary data storage facilities, stock markets and major banking centers; chemical facilities located near large populations; major power generators generating in excess of 2 gigawatts of power and whose disruption would affect a regional grid; hydroelectric facilities and dams that produce in excess of 2 gigawatts of power and could result in catastrophic loss of life if breached; nuclear power plants; electric substations critical to service areas in excess of one million people; rail and highway bridges and tunnels and whose loss would cause catastrophic economic loss and/or loss of life; natural gas pipelines with throughput in excess of 3000 billion cubic feet; liquified natural gas facilities; major petroleum handling facilities including pipelines, ports, refineries, and terminals; and mass transit systems.

Nothing in the grant guidelines or in the testimony cited above indicates that the IA/IP Directorate was involved in the development of the criteria for these grant programs. Apparently the IA/IP Directorate did not generate its list using these grant applications. Nor is it clear what role, if any, the IA/IP Directorate's subsequent vulnerability and/or risk assessments have informed the allocations of grant resources. However, the Senate Appropriation's Committee, in the appropriations bill report cited above, stated that it was encouraged by the initial cooperation between the IA/IP Directorate and ODP, and expected it to improve and for the IA/IP Directorate to be a full partner in the grant award process.

There are other potential sources of information for identifying assets. Title II, Subtitle B of the Homeland Security Act of 2002 established a new category of information called Critical Infrastructure Information. Critical Infrastructure Information is defined as "information not customarily in the public domain and related to the security of critical infrastructure ...." It includes a broad range of information, including information related to actual, potential or threatened interference or attacks that could compromise or incapacitate a critical infrastructure, the ability of a critical infrastructure to resist interference or attack, and any planned or past operational problems. Such information, if voluntarily provided to the DHS state, local, or private entities, either directly or indirectly through another agency, is accorded a number of protections.[38] The purpose for encouraging owners/operators of critical infrastructures to supply this information is to help DHS assess vulnerabilities and threat, mitigation strategies and to monitor the operational status of the infrastructures. It is not known how much critical infrastructure information has been submitted to DHS, and to what extent, if any, it has helped to populate the

---

[37] (...continued)
jurisdiction, its impact outside the jurisdiction, the potential access of a threat element to the target, the target's population capacity, and the potential for mass casualties. Note that the guidance on vulnerability assessment mixes vulnerability and consequence considerations.

[38] DHS published its interim rule on the procedures associated with the sharing and handling of information designated as Critical Infrastructure Information in February 2004. Federal Register, No. 69, Vol. 34, pp 8074-8089. February 20, 2004.

list of 80,000 assets. Nor is it clear how DHS uses the information it receives or if it is helpful at all to IA/IP in accomplishing its mission.

Another source of asset information could be other agencies, especially the Sector Specific Agencies, that have been tasked with helping their sectors assess their vulnerabilities and to encourage them to use risk management techniques to set priorities. While Sector Specific Agencies are apparently in the midst of developing Sector Specific Plans for submission to the IA/IP Directorate, many of these Agencies have already engaged in facilitating vulnerability assessments within their sectors.[39] It is not clear what the connection is between the specific sector planning process and the on-going assessments associated with the list of 1,700 assets. Nor is it clear to what extent, if any, the list of 80,000 assets generated by the IA/IP Directorate, or any of the subsequent vulnerability assessments led by the IA/IP Directorate, reflect or duplicate information accumulated by these Agencies. Does the IA/IP Directorate use these outside analyses in lieu of doing their own vulnerability assessments or does the Directorate use the information to help direct its own separate analyses?

Other potential sources could be public (open source) and private databases. For example, there are private databases used by U.S. industry that map and monitor the operations of the nation's systems of electric grids. Much of this information may be proprietary.

Regardless of where DHS's data comes from, the accuracy of the data is important. For example, DHS compiled a preliminary list of critical infrastructure in electric power and circulated that list to certain infrastructure owners for comment. Among utilities operators, there was some confusion as to why certain assets were included in the list, since some were not currently in use, while others which were considered critical by industry standards were not on the list.[40] The previously referenced letter from the Democrats to Secretary Ridge also stated that IA/IP's list included sites that no longer existed. Reportedly, DHS initially had Disneyland in California located in Los Angeles County, not Orange Country.[41] For criticality and potential consequences to be assessed accurately, location and utilization must be known.

Nor is it clear in what form the IA/IP Directorate has collected its information, whether it is being entered into a single database, or if it exists in multiple databases. If the latter, is it formatted consistently and is it accessible to all those who need to use it? Also, it is not clear if the IA/IP's current list of 80, 000 assets, or its refined list of 1,700 assets, constitute the foundation of the integrated data warehouses referenced in IA/IP's budget justification above.

---

[39] For example, the Department of Energy for electric utilities, the Environmental Protection Agency for drinking water, and Treasury for financial services.

[40] Based on a personal communication with industry official, September 29, 2003.

[41] See, CQ Homeland Security. July 29, 2004. [http://homeland.cq.com/hs/display.do?docid=1278697&sourcetype=31]. This site was last viewed on February 4, 2005. It is available by subscription only.

Selecting High Priority Assets

On what basis did the IA/IP Directorate select, in consultation with other stakeholders, the 1,700 assets for further attention? According to the Undersecretary, in his testimony referenced above, the 1,700 assets were ones with a credible potential for loss of life and loss of citizen confidence and that these impacts would be felt nationally. He described these assets as ones the nation cannot afford to lose.

Roper, and other methodologies reviewed for this report, recommended the criteria for assessing the level of criticality be specific. For example, at what point is the impact of an attack felt nationally versus one felt primarily locally or regionally? How many casualties rise to the level of having a national impact? What level of economic impact or what measure of reduced confidence would rank an asset as nationally critical? Again, the answers to these questions would probably require a consensus among decision makers.

The list of assets that qualify for Urban Area Security grants provides a little more specificity for some of the assets. For example, power generating plants in excess of 2 gigawatts, and whose disruption would affect a regional grid or electric substations critical to service areas in excess of one million people, qualify for grants. Presumably these thresholds were arrived at based on some assessment of the relative impacts the loss of those assets would have. Other qualifying assets are less well characterized, such as rail and highway bridges over major waterways that, if destroyed, would cause catastrophic economic loss. What constitutes catastrophic?

An example of an analysis that provides more detail as to what might be considered nationally critical can be found in a white paper entitled *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*. The authors of the white paper, the Federal Reserve Board, U.S. Security Exchange Commission, and Office of the Comptroller of the Currency, determined that a disruption in the services of certain "core clearing and settlement" organizations could, by virtue of their market share, present a systemic risk to the smooth operations of the financial markets they service. The paper defined "systemic risk" as the risk that failure of one participant to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems and threatening the stability of financial markets. The white paper identified a threshold market share, above which a firm's plans associated with back-up capacity, geographic location, and recovery would be subject to review by the appropriate agency.

Another important issue is how to adjudicate disagreements about what should and should not be on the list. What the IA/IP Directorate might, through careful and accurate analysis, determine to be critical (or not) at the national level may not necessarily agree with what other stakeholders or policy makers consider to be critical or not (and even need not agree as long as the data analyzed is consistent, accurate, and comprehensive).

Assessing Threat

The Homeland Security Act assigned to the IA/IP Directorate the responsibility of integrating all-source information in order to identify and assess the nature and scope of terrorist threats against the homeland and to detect and identify threats of terrorism against the United States. However, shortly after the act was passed, the Bush Administration, in January 2003, established the Terrorist Threat Integration Center (TTIC), within the intelligence community. Many observers felt that the TTIC assumed many of the same responsibilities of the IA/IP Directorate. The Homeland Security Act designated DHS a member of the intelligence community and it has a seat at the TTIC. The issues and concerns associated with the division of labor between TTIC and the IA/IP Directorate is beyond the scope of this report. For information on this, see CRS Report RS21283.[42] There are, however, two key questions that are relevant to this report. Is there a consistent characterization of the threat used throughout the intelligence community and made available to the IA/IP Directorate and beyond to other stakeholders? Is that characterization used consistently to inform the teams sent out to do vulnerability assessments or those agencies and other stakeholders tasked with assessing the vulnerabilities of the sectors for which they are responsible?

In a written response to a list of questions submitted by the House Select Committee on Homeland Security, after its joint hearing with the Judiciary Committee on July 22, 2003, the DHS gave a few examples of threat information that has been passed on to stakeholders to inform their decision-making. These included an advisory to the oil and gas industry that discussed recent terrorist behavior overseas, including general characteristics of terrorist surveillance; and, an advisory on how nitrocellulose could be used by terrorists to create a bomb. The answer did not discuss if or how this information may have influenced subsequent vulnerability or risk assessments.

Another issue is whether the IA/IP Directorate values all threats equally. For example, Al Qaeda has demonstrated capabilities in a number of attack modes (e.g. bombs, hijacking and piloting planes). But, their capability in other attack modes are not necessarily as well developed. How does IA/IP consider this in their threat assessments?

Assessing Vulnerabilities

The testimony of IA/IP officials implies that the IA/IP Directorate will either perform or lead vulnerability assessments in the field. However, much of the work being performed by the IA/IP Directorate is being done by contractors or details from other agencies until the IA/IP Directorate is more fully staffed. Also, as mentioned earlier, it is not clear if the IA/IP Directorate uses the vulnerability assessments performed by other agencies or stakeholders in lieu of doing their own. A key question is whether or not contractors, details, or other agencies and stakeholders follow a similar protocol in doing their vulnerability assessments? As discussed

---

[42] Congressional Research Service. *Homeland Security: Intelligence Support*. CRS Report RS21283, by Richard Best.

above, there are many models by which to assess vulnerabilities. It is not necessarily important that all vulnerability assessments follow the exact same methodology. However, Congress might want to ensure that certain general considerations are included. For example, what vectors of vulnerability are examined? Are dependencies on assets beyond the control of the immediate owner/operator considered? As discussed above, is the threat sufficiently characterized?

Assessing Risks

As discussed above, risk is a function of threat, vulnerability, and consequences. What consequences does the IA/IP Directorate consider when assessing risk? The Undersecretary of Information Analysis and Infrastructure Protection, in the testimony discussed above, mentioned that the criticality of an asset was measured in part by loss of life and loss of citizen confidence, and the IA/IP budget justification alludes to forecasting national security, economic, and public safety implications.

HSPD-7 lists the types of attacks that animate national critical infrastructure policy. These are attacks that could: cause catastrophic health effects or mass casualties; impair federal agencies' ability to perform essential missions; undermine the ability of state and local governments' to maintain order and provide essential services; damage the orderly function of the economy; or undermine the public's morale or confidence.

One may assume that the IA/IP Directorate considers these factors when determining risk. But, are they all considered together? How are different consequences integrated into an overall risk rating for a given scenario?[43] Does IA/IP weigh each category of consequence equally? HSPD-7 stated that the Secretary of Homeland Security, when identifying, prioritizing, and coordinating the protection of critical infrastructures, should emphasis those infrastructures that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction. In this case, might preventing an attack on the Super Bowl take precedent over an attack on one of those core clearing and settlement facilities mentioned above, the destruction of which might significantly disrupt national financial markets? To what extent, if any, is the Directorate risk averse? The grant application guidelines for the State and Urban Areas Security grants imply a risk aversion when it focuses on weapons of mass destruction, even though the threat of this might be lower than the threat of conventional attacks.

Another question is how are these consequences measured? Are potential deaths based on experiential data or models or best estimates? How is confidence or morale, and the impact on morale measured? Are economic models used to

---

[43] For example, the Coast Guard considered six categories of consequences, including death/injury, economic, environmental and symbolic impacts, all equally weighted, and assigned a value of 1 to 5 to each of these, based on severity. An overall level of risk was determined by the sum total value.

determine economic impact? How are cascading effects due to interdependencies determined? How far down the chain of reactions does IA/IP consider[44]?

Risk Mitigation

The risk associated with a specific attack on an asset can be reduced by reducing the level of threat to it, by reducing its vulnerability to that threat, or by reducing the consequences or impact of an attack should it happen. This parallels the Bush Administration's overall strategy for homeland security—1) prevent terrorist attacks, 2) reduce America's vulnerability to terrorism, and 3) minimize the damage and recover from attacks that do occur.[45] The Department of Defense, the Central Intelligence Agency, the Federal Bureau of Investigations, elements of DHS's Border and Transportation Directorate, and other law enforcement and intelligence agencies (including the Information Analysis side of the IA/IP Directorate) have the primary role of reducing threat, by disrupting, finding, detaining, or eliminating individuals that threaten the United States. The DHS's Emergency Preparedness and Response Directorate is principally responsible for trying to mitigate the consequences of an attack, through rapid response and quick recovery. The IA/IP Directorate's primary role is to reduce an asset's vulnerability. As discussed above, it is doing so mainly by hardening the asset against attack, by improving the ability of those protecting the asset to deny access to the asset and to improve their ability to repulse an attack. This begs the question, however, of whether or not, and by what mechanism, are the various efforts to reduce threat (prevent), vulnerability (protect), and consequences (prepare) coordinated both within DHS and between DHS and other agencies and to what extent, and by what mechanism, are the allocation of federal resources to these three areas influenced at all by comparing the risk reduction achieved by each? This would likely require a level of risk management currently beyond the IA/IP Directorate's mandate.

Prioritizing Protection Activities

According to the statement of Director McDonnell, the IA/IP Directorate conducts a risk assessment, mapping threat and vulnerability information. The risk information is then used to prioritize the implementation of protective measures. It is not clear, however, how the risk assessment is used by IA/IP to prioritize subsequent activity. The implication is that the IA/IP Directorate ranks further its list of 1,700 assets based on the risk. But several question remain. Does the IA/IP Directorate rank assets as high, medium, and low risk and focus it subsequent efforts on those ranked as high? Does it estimate the risk reduction associated with its recommendations? Does it seek to maximize the risk reduction of the highest at-risk assets or does it seek to maximize the risk reduction across all of the assets it has identified as critical?

---

[44] The Senate Appropriation Committee, in its FY2005 appropriations bill's report, recommended continued funding for risk analysis activities that include evaluating second- and third-order cascade effects associated with market interdependencies.

[45] See, Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, p. 1.

HSPD-7 gives some guidance in addressing these questions. According to the Directive, the Secretary will "identify, prioritize, and coordinate the protection of critical infrastructure and key assets with an emphasis on critical infrastructures and key assets that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction." This implies that greater weight should be given to loss of life consequences than economic impact, or continuity of government services, or loss of national morale or confidence.

Conclusion

The IA/IP Directorate has been tasked with a very complex problem. Security oriented risk management is typically done at the site or facility level or at the corporate level. The IA/IP Directorate is being asked to do this at the national level, assessing and comparing at least 1,700 disparate sites and facilities it has judged as being nationally important.

The IA/IP Directorate is also asked to consider not only economic impacts and loss of life, but the possible impact on national morale and the ability of state and local governments to maintain order and deliver essential services. None of these are easy to measure and all are difficult to trade off one against the other, should the analysis come down to that. To determine the economic impact of the loss of an asset is more difficult than determining the effect on a company's bottom line. The IA/IP is being instructed to determine economic impacts two to three levels through the supply chain. It is not clear how the Directorate can or intends to measure the impact on national morale associated with the loss of an asset, especially a cultural icon. Comparing the potential loss of life in one scenario with the potential loss of life in another scenario, while sensitive, presents a direct comparison. However, comparing the importance of an asset whose loss may result in a relatively small loss of life with another asset the loss of which might result in a large economic impact is much harder.

The exercise will be less than perfect and probably less than objective. The Bush Administration and Congress are allocating resources in any event, so these choices are getting made implicitly. If such processes were more transparent, Congress could better oversee them and offer guidance if necessary.

The 9/11 Commission, in discussing a need for a layered security system for public transportation systems, stated that the Transportation Security Administration should be able to identify for Congress the array of potential terrorist attacks, the layers of security in place, and the reliability provided by each layer.[46] Expanding on this, the IA/IP Directorate should be able to tell Congress what criteria it used to select assets of national importance, the basic strategy it uses to determine which assets warrant additional protective measures, and by how much these measures could reduce the risk to the nation. It should also be able to tell how much these

---

[46] The National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, W.W. Norton and Company, 2004, p. 392.

additional measures might cost. Who pays for these measures is another issue, beyond the scope of this report. The national plan called for by HSPD-7 could be a good vehicle for presenting this information. Alternatively, the IA/IP Directorate could develop a written protocol that outlines specifically the steps taken in the risk assessment and risk management process and the assumptions, criteria, and tradeoffs that are made. Such a protocol could not only help keep Congress informed, but could also ensure consistency in carrying out assessments and in making decisions. Some critics of this approach might suggest that each sector and each asset is different and "one size can't fit all." However, while each sector and each asset presents their own unique situations, a common set of consequences that measure risk and by which to measure risk reduction will act to normalize the analysis across assets.

Finally, Congress may choose to offer its guidance to the IA/IP Directorate on some of these criteria or tradeoffs. To do so with the same systematic approach that the IA/IP Directorate has been asked to do, the different committees with jurisdiction over different infrastructures may want to consider coordinating their advice.

References

Carl Roper, Risk Management for Security Professionals, Butterworth-Heinemann, 1999.

U.S. Coast Guard, *Implementation of National Maritime Security Initiatives*, Federal Register, Vol. 68, No. 126, July 1, 2003, pp 39240-39250.

American Petroleum Institute and the National Petrochemical & Refiners Association, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, May2003.

U.S. Department of Energy, Office of Energy Assurance, *Vulnerability Assessment Methodology, Electric Power Infrastructure (Draft)*, September 30, 2002.

National Communications Systems, Office of the Manager, *Public Switched Network Security Assessment Guidelines*, September 2000.

Association of Metropolitan Sewerage Agencies, *Protecting Wastewater Infrastructure Assets: Asset Based Vulnerability Checklist for Wastewater Utilities*, 2002.

Government Accountability Office, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T, October 12, 2001.

American Chemistry Council, the Chlorine Institute, and the Synthetic Organic Chemical Manufacturers Association, in their *Site Security Guidelines for the U.S. Chemistry Industry.*

Argonne National Laboratory, et al., prepared for the Office of Energy Assurance, U.S. Department of Energy, *Energy Infrastructure Vulnerability Survey Checklists*, February 22, 2002.