Order Code RS21348
October 31, 2002

Risk Assessment in the President's National Strategy for Homeland Security

Rob Buschmann
Analyst in American National Government
Government and Finance Division

Summary

The President's National Strategy for Homeland Security suggests that agencies responsible for homeland security may use risk assessment techniques as tools to accomplish their missions. Agencies may perform risk assessments on a national scale in some areas, such as critical infrastructure. National homeland security risk assessments may be beneficial, or even essential, but a number of limitations could reduce or eliminate their usefulness. In addition, awareness of risk assessment's basic methods and potential shortcomings can help Congress to effectively oversee agencies responsible for homeland security. This report is intended to provide background on the use of risk assessment in the homeland security context and will not be updated.

Risk Assessment and Its Components: Defining the Terms

Risk assessment is a policy tool designed to help decision makers understand risks to human welfare, safety, and property. Risk experts debate the exact meaning of the term "risk," but most accept two concepts as central: chance and consequence. Chance refers to the probability that an adverse event will happen; consequence, to the loss associated with that event. Risk assessment assists decision makers by providing quantitative and qualitative estimates of the chance of, and possible consequences from, an adverse event. Many existing laws, new legislation, and newspaper articles, however, refer to "threat" and "vulnerability" assessments. How are these processes related to risk assessment?

Threat assessment usually refers to the process of identifying possible "initiators" of adverse events, although the term, along with others in the risk assessment process, is sometimes used loosely.[1] A threat assessment is typically the earliest step of a risk assessment – the threat assessment defines or identifies the dangerous actors, their intents

[1] For more precise definitions of threat, vulnerability, and risk assessments as used here, see CRS terrorism briefing book entry, "Assessing Risks," at [http://www.congress.gov/brbk/html/ebter225.html].

and capabilities, and what events they might initiate. The succeeding portions of the risk assessment attempt to quantify the chance of specific consequences of those events.

While threat assessments focus on the initiators of events, *vulnerability assessments* tend to focus on who or what is threatened and the nature and extent of the damage adverse events might cause. A vulnerability assessment typically names the things, persons, or populations that could be affected by an event. In addition, some vulnerability assessments attempt to measure the "toughness" of targets — their susceptibility to certain types of attack. For terrorists, the actual or perceived toughness of a target can be a factor in determining which targets to attack. Therefore, in addition to consequences, a homeland security vulnerability assessment might inform the assessor about the probability of an attack as well as the probability of its success.

In short, a risk assessment usually contains threat and vulnerability components which contribute to an overall picture of probability, and possible consequences, of an adverse event. In this report, risk assessment means a process that includes both threat and vulnerability assessments. Recent press coverage suggests that risk assessment and its components may be significant tools in homeland security; the Bush Administration has started to address this in its *National Strategy for Homeland Security* (the President's Strategy).[2]

Risk Assessment in the President's Strategy

The President's Strategy begins with a definition of homeland security that reads like a prescription for risk assessment and risk assessment-based management: "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[3] White House official Richard Falkenrath, director of policy and plans for the Office of Homeland Security, has added that comparing threats to vulnerabilities will, in the long run, be the most useful exercise for determining how to allocate homeland security resources. However, it is unclear exactly how risk assessment will be used, since the threat from terrorism seems to differ considerably from the threats that risk assessment methods normally evaluate, such as cancer risks from environmental pollutants or the chance of a bridge collapsing. Falkenrath has stated that the ability to perform risk assessments for terrorist attacks does not exist adequately in the government today and needs to be established.[4]

---

[2] See Sydney J. Freedberg, Jr. and Siobhan Gorman, "Are We Safer?" *National Journal*, Aug. 10, 2002.

[3] Executive Office of the President, Office of Homeland Security, *National Strategy for Homeland Security*, p. 2. Available at [http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf], visited 9/30/2002. The homeland security bills, H.R. 5005 and its Senate counterparts, do not contain such a definition.

[4] See The Brookings Institution, *Homeland Security: The White House Plan Explained and Examined*, Sept. 4, 2002. Available at [http://www.brookings.org/comm/events/20020904homeland.htm], visited 9/30/2002.

The President's Strategy includes the following broad plans for dealing with homeland security issues, plans that include what some experts indicate are good risk assessment practices:

- Threats will be matched with vulnerabilities to reach a measure of risk;[5]
- Vulnerability and threat assessments will be maintained and updated to keep up with a constantly changing environment;[6]
- Assessments of all national infrastructure risks will be done so "risk-shifting" between sectors does not occur when management decisions are made.[7]

The President's Strategy focuses on six "critical mission areas": intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response. Two of these areas, intelligence and warning and protecting critical infrastructure, appear to give risk assessment a central role. The other four areas in the President's Strategy also refer to risk assessment or its threat and vulnerability components, though risk assessment does not seem to play as large a part in their missions.

In intelligence and warning, the President's Strategy envisions analysts and operatives from various existing agencies combining their efforts to create a complete threat assessment for domestic terrorism. The proposed Department of Homeland Security (DHS) would have the lead in domestic vulnerability assessments, which DHS would then match against the threats provided by the intelligence community to produce a complete picture of the risks facing the United States.

In protecting critical infrastructure, the DHS would undertake comprehensive national assessments of threats and vulnerabilities across all critical infrastructure and key asset areas. The goal is to "build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets" and "to ensure we reduce the overall risk to our country, instead of inadvertently shifting risk from one potential set of targets to another."[8] In addition, through this initiative, the DHS would be responsible for maintaining and updating this national assessment and using it to create a current image of the threats and vulnerabilities facing the United States.

---

[5] See the U.S. General Accounting Office, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74, April 1998.

[6] See The National Research Council, *Science and Judgement in Risk Assessment* (Washington, D.C.: Taylor and Francis, 1994); also relevant is the Council's recommendation of an "iterative approach," which demands among other things that risk assessments increase in detail as the consequences from the events they analyze increase in probability and severity.

[7] See John D. Graham and Jonathan Baert Wiener, eds., *Risk vs. Risk: Tradeoffs in Protecting Health and the Environment* (Cambridge: Harvard University Press, 1995) for an explanation of how risks are changed and shifted between populations.

[8] *National Strategy*, p. 31-33.

As a final note, the President's Strategy's use of risk assessment could provide a framework for budgeting. Agencies involved in homeland security seem likely to be instructed by the President to use risk assessment techniques to help set priorities and assign resources. Many already do, such as the Coast Guard and the Customs Service. Effective oversight of these agencies may require an understanding of how they use risk assessment techniques in budget allocation.

Issues in Risk Assessment

To its advocates, risk assessment is a rational, systematic way to deal with society's risks, from the discovery of those risks to the formulation of policy options to reduce them. Some experts, however, note that improper or incomplete use of risk assessment can result in misinformed decision making and a loss of public faith in government. While the President's Strategy does not clearly explain how agencies focused on homeland security are to employ risk assessment or its components, several generic issues seem to arise whenever those techniques are used, especially on a national level.[9] The policy implications of these issues likely will be of interest to Congress as it reviews the President's Strategy and contemplates the enactment of legislation.

Uncertainty.

Every risk assessment is an estimate. A common criticism of risk assessment is that few assessments are accompanied by statements of the confidence that risk assessors have in their conclusions. Some critics of risk assessment observe that risk numbers are useless without a clear presentation of the data upon which those numbers are based. Many risk assessments, they argue, draw conclusions that are not the only ones that can realistically be drawn from the data. Critics are concerned that once a conclusion is stated in a risk assessment, further discussion about alternative conclusions tends to disappear along with the uncertainty risk assessors have about the judgment they have made. On the other hand, some advocates of risk assessment argue that uncertainty is hard to measure and that constantly reporting uncertainty and ranges of possibility can unnecessarily confuse the issues. A national-level risk assessment may lose meaning as a public policy tool and public credibility if vulnerability and threat assessments are not accompanied by uncertainty estimates. However, advocates are concerned that too much information may cause a risk assessment to be disregarded as overly technical.

Risk Interactions.

Risk assessments generally analyze specific events or categories of events, producing probabilities and consequences for each. Such a process can miss risk interactions, when two or more risks influence each other. For example, should three separate events occur in a single community — an attack on a mobile communications system, another on a power grid, and the release of biological weapons in a crowded shopping center — the calculations, and the results, change. When considered separately, each event's chance and consequences may be able to be estimated. If all of the attacks happen

---

[9] A further discussion on some of these issues can be found in Bernard D. Goldstein's chapter titled "Risk Assessment as an Indicator for Decision Making" in Robert W. Hahn, ed., *Risks, Costs, and Lives Saved* (Washington, D.C.: The AEI Press, 1996), p. 67-84.

simultaneously, however, one cannot simply add the consequences from each to find the result; the whole could be greater than the sum of the parts. A power grid shutdown would likely cause more confusion when combined with a biological attack, as the lights go out in the shopping center; a communications outage could prevent emergency workers from responding quickly to the attack. Some risk assessment methods are being developed which will attempt to handle such complicated scenarios.[10]

Data Quality.

Some risk assessors attempt to find the chance and the consequences of an adverse event to the most precise degree possible. The more numbers are used to create a risk assessment, the more likely a risk assessor will look at events for which probability and consequences can be easily quantified. Most often, easily quantified chance and consequences come only after analysis of years of relatively common events when the circumstances of those events and their effects can be clearly measured. Critics claim that what risk assessment cannot measure, it implicitly disregards as unimportant, and with rare events (such as terrorist attacks) this problem becomes significant. A national valuation of key assets and critical infrastructure may take into account only the "most measurable" damage, possibly de-emphasizing less easily quantified things, such as environmental or psychological damage from terrorist attacks. In a related issue, the Office of Management and Budget (OMB) recently released its Information Quality Guidelines for federal agencies.[11] The guidelines attempt to ensure that data used by executive agencies in their decision making is accurate and produced by a rigorous application of the scientific method. Some groups have expressed concern that these guidelines may lead to agencies being limited by OMB to making decisions based only on completely quantified data — perhaps limiting the effect of important, but less measurable, issues. Congressional oversight of agencies using risk assessment in homeland security decisions may need to include a review of the scope, quantity, and validity of data used in those decisions.

Disregarding Very Rare Catastrophes.

Risk assessors sometimes, through choice or inadvertence, do not consider very unlikely and catastrophic adverse events, especially if a large amount of time passes without any such events occurring. Some scholars have noted that this tendency is "particularly noteworthy for relatively complex systems and for estimates of extremely low probabilities.... (I)t has even earned a name: the 'disqualification heuristic', or the

---

[10] These methods are beginning to be discussed and used by the insurance industry. Models are being developed that play out terrorist scenarios in the same manner as military war games. For insurance models, see Joseph B. Treaster, "The Race to Predict Terror's Costs," *New York Times*, Sept. 1, 2002, Money and Business/Financial Desk. For war game scenarios, see Karen Kaplan, "The Sims Take On Al Qaeda," *Los Angeles Times*, Nov. 2, 2001, Financial Desk.

[11] Office of Management and Budget, "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by the Office of Management and Budget," *Federal Register*, vol. 67, no. 84, May 1, 2002, p. 21779.

temptation to conclude that certain highly unpalatable outcomes simply couldn't occur."[12] It seems that a terrorist attack with catastrophic consequences in the United States could be the result of just such a complex system failure of law enforcement, security forces, and intelligence. In other words, there is a possibility that as time goes by and very rare and catastrophic events do not occur, an agency's risk assessors may begin to disregard the risk of those types of events entirely.[13]

Differing Agency Risk Assessment Methods.

Many of the agencies that will manage homeland security functions have existing methods for risk assessment, many if not all of which have been tailored for the specific problems those agencies face. A national risk assessment may alter or appear inconsistent with these risk assessment methods if imposed as a new model. On the other hand, if the national risk assessment relies upon each of these agencies for information about risks without specifying a consistent method, the results could be difficult to integrate into a meaningful whole, as each agency bases its assessments on its own criteria.

Distribution of Consequences.

A national risk assessment may not take regional considerations into account. Consequences tend to be aggregated and are averaged over time and space in large-scale risk analyses. Such aggregation may hide areas of extremely high and low vulnerability and threat within a single "average" area or industry. This may be particularly significant in homeland security, where symbolism may be as important to terrorists as large-scale destruction. An attack on a target of minor national importance as defined by a national risk assessment – perhaps a remote chemical or nuclear plant – may incapacitate a small community and give terrorists a symbolic victory, widely reported by the media.

Conclusion

The use of risk assessment in homeland security could aid decision makers by more clearly delineating the probability of, and consequences from, terrorist attacks. Risk assessment is used in many forms throughout government and private industry to help set priorities, anticipate problems, and allocate resources. However, Congress may want to consider the many uncertainties and policy choices that are present in almost any risk assessment, regardless of the area in which it is performed. The issues discussed here, and others related to risk assessment, may be raised in congressional consideration of homeland security.[14]

---

[12] William R. Freudenburg, "Heuristics, Biases, and the Not-So-General Public: Expertise and Error in the Assessment of Risks," in *Social Theories of Risk*, edited by Sheldon Krimsky and Dominic Golding (Westport, CT: Praeger Publishers, 1992), p. 232.

[13] Ibid., p. 242.

[14] For additional reading on the use of risk assessment in a specific issue area, see CRS Issue Brief IB94036, *The Role of Risk Analysis and Risk Management in Environmental Protection*, by Linda-Jo Schierow.

Strategic Risk Management in Government: A Look at Homeland Security. Managing for Performance and Results Series. Improving Strategic Risk Management at the Department of Homeland Security. David H. Schanzer Associate Professor of the Practice Sanford School of Public Policy Duke University.Â President Bush reversed his initial opposition to the concept later that year and signed legislation into law in December 2002 creating the Department of Homeland Security (DHS).Â Increased funding for enhanced homeland security flowed freely in the initial months following 9/11 through supplemental appropriations measures and large increases for particular programs, such as trans-portation security. As relevant to Homeland Security issues, however, risk is more particularly the likelihood that a terrorist threat will endanger or affect some asset. That asset can be an individual (like the President), a structure (like the Pentagon), or even a function (like America's stock exchange system).[3]. When one thinks of such risks, one must therefore think of any number of underlying elements that go into an evaluation. These might includeÂ Mangers can then use this perspective to create a risk reduction strategy, which guides resource allocation. Making Risk Management a Reality.Â Alane Kochems is a National Security Policy Analyst in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. risk management. The National Strategy for Homeland Security was issued in: 2002. When discussing our National Infrastructure Protection, there has been a primary focus on security and _. resiliency. T or F In regards to definitions, "hard and fast" working criteria do not exist based on the legislation enacted for critical infrastructure assets. True. Critical infrastructure risks are assessed and analyzed through all of the following except: Correct Answer: location Wrong answer chose: consequence.Â T or F FEMA is responsible for quick, short, and long-term response and is activated once the President declares an area a disaster. True. Direction was given to the DHS to develop a national critical infrastructure database by the The risk assessments leverage the Federal Information Security Modernization Act of 2014 (FISMA) Chief Information Officer (CIO) metrics from Fiscal Year (FY) 2017 and the Inspectors General (IG) metrics from FY 2016.Â At the conclusion of the risk assessment process, OMB required each agencyâ€™s Senior Accountable Official responsible for implementing Executive Order 13800 to submit a signed letter describing their agencyâ€™s plan to accept, mitigate, avoid, or transfer cybersecurity risks in the near term. This Risk Report uses summary data from the agency metrics, narrative responses, and Senior Accountable Official letters to support findings and actions described herein.Â Accordingly, over the next year OMB will work with DHS, the National Security Agency A New National Strategy for Homeland Security. In October 2007, the Homeland Security Council issued a new National Strategy for Homeland Security.Â The new Strategy directly discussed the establishment and institutionalization of a comprehensive Homeland Security Management System that would build on the planning and operations detailed in the National Preparedness Guidelines. The System was to have activity in the four phases of (1) guidance (presidential directives and other key policies); (2) planning (family of strategic, operational and tactical plans); (3) execution of operational and tactical level plans; and (4) assessment and evaluation of both operations and exercises.