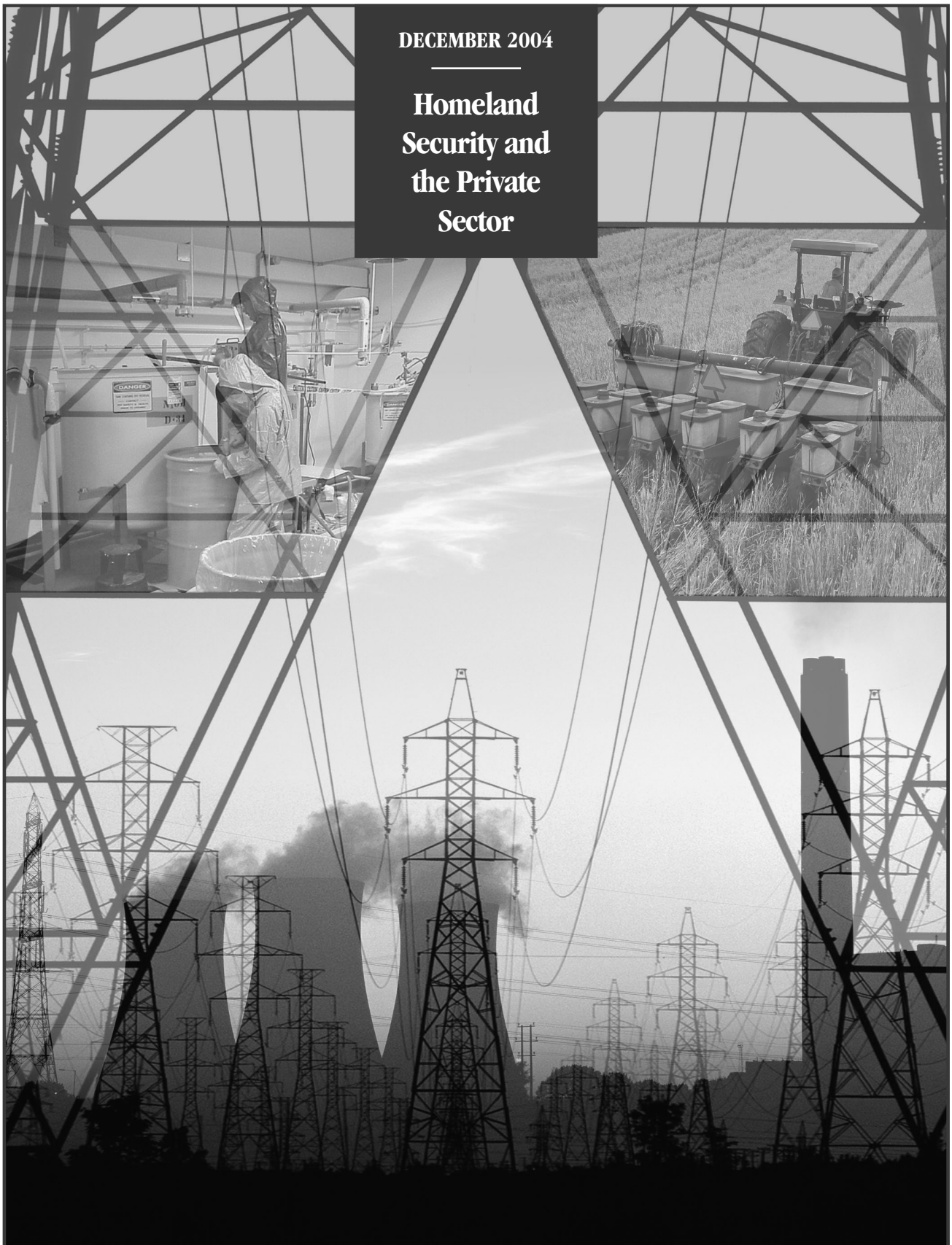
CONGRESS OF THE UNITED STATES
CONGRESSIONAL BUDGET OFFICE

A
CBO
PAPER

DECEMBER 2004

Homeland Security and the Private Sector



A

CBO

PAPER

Homeland Security and the Private Sector

December 2004

The Congress of the United States ■ Congressional Budget Office

Note

On the cover, the photograph of the barley crop in Washington County, Virginia, is by Jeff Vanuga, courtesy of the U.S. Department of Agriculture, National Resources Conservation Service. The photograph of the chemical decontamination room is courtesy of the Department of Energy's Office of Environmental Management.

Preface

The events of September 11, 2001, raised the nation's awareness of the threat of terrorist attacks. The private sector generates the vast majority of the nation's economic output, and businesses may find it in their interest to undertake measures that can help reduce the nation's vulnerability to attack and the subsequent potential losses. This Congressional Budget Office (CBO) paper, prepared at the request of the Ranking Member of the House Select Committee on Homeland Security, examines the role of the private sector in responding to the threat of terrorism in the United States since September 11. In keeping with CBO's mandate to provide objective, impartial analysis, the paper makes no recommendations.

Richard D. Farmer wrote the paper, with contributions from Andrew Goett, Nathan Musick, and David Torregrosa, under the supervision of Roger Hitchner and David Moore, all of CBO's Microeconomic and Financial Studies Division. Robert Shackleton and Michael Gilmore of CBO provided helpful comments on earlier drafts of this paper. Paige Piper-Bach reviewed the manuscript for factual accuracy. The paper also benefited from comments by Jay Apt of the Tepper School of Business at Carnegie Mellon University, James C. Belke of the Environmental Protection Agency, and Kevin Crowley of the National Research Council's Board on Radioactive Waste Management, as well as from conversations with Alison Silverstein, former senior adviser to the Chair of the Federal Energy Regulatory Commission. (The assistance of external participants implies no responsibility for the final product, which rests solely with CBO.)

Janey Cohen edited the manuscript, and Christian Spoor proofread it. Maureen Costantino prepared the paper for publication and designed the cover, Lenny Skutnik produced the printed copies, and Annette Kalicki prepared the electronic versions for CBO's Web site (www.cbo.gov).

Douglas Holtz-Eakin
Director

December 2004

CONTENTS

Summary *ix*

1

Introduction *1*
What Is Homeland Security? *1*
A Focus of Security Concerns: Critical Industries *2*
Why the Private Sector Might Spend Too Little on Security *2*
What Is the Government's Role? *3*
The Government's Response Since September 11—A Baseline for Further Change *4*
Improving Homeland Security—A General Framework *5*
Scope of the Analysis *8*

2

Civilian Nuclear Power *9*
Vulnerabilities from Attacks on Power Reactors and Spent Material *9*
Potential Losses from Exposure to Radioactivity and Destruction of Power Facilities *11*
Current Programs for Plant Safety, Control over Nuclear Materials, and Compensation for Losses *13*
Ideas for New Approaches to Nuclear Power Security *16*

3

Chemicals and Hazardous Materials *21*
Vulnerabilities from Processes,Transportation, and Misuse of Materials *21*
Potential Losses from Explosions and Toxic Releases *23*
Current Programs for Safety and Emergency Preparedness *25*
Ideas for New Approaches to Chemical and Hazardous-Material Security *26*

4

Electricity Service *29*
Vulnerabilities from Disruption of Regional Transmission *29*
Potential Losses from Disruption of Vital Services *32*
Regulating for Reliable Electricity Service *34*
Ideas for New Approaches to Reliable Electricity Service *35*

5 **Food and Agriculture** *39*
Vulnerabilities from Contamination, Loss of Food Sources, and Use of Agricultural Resources as Weapons *39*
Potential Losses from Threats to Health or Consumers' Aversion to Contaminated Products *40*
Current Programs for Food Safety *42*
Ideas for New Approaches to Food and Agriculture Security *43*

Boxes

1-1. Changing Concepts of Critical Infrastructure 3

1-2. Government Efforts to Share Information with Industry 6

4-1. Vulnerabilities, Potential Losses, and Regulatory Regimes for Large Dams and Reservoirs 30

Summary

The events of September 11, 2001, raised the nation's awareness of the potential scale of terrorist attacks, the likelihood of such attacks, and the benefits of spending on homeland security. Since that date, the public sector has undertaken efforts to boost security against terrorism. At the same time, there have been calls for new laws or regulations that would require businesses to assume an increased role in the nation's defense against terrorists. Those calls rest on the premise that the social benefits from private spending to enhance security are greater than the private benefits to the businesses making those spending decisions. If not, then businesses already have incentives to do as much as the nation would find cost-effective to enhance homeland security.

This paper examines issues surrounding enhanced security efforts by private industry. For several important industries, it describes the vulnerabilities and potential losses—to both the private sector and the nation as a whole—that would underlie the expected costs of terrorist attacks and, hence, the broader benefits of security. The paper also reviews the incentives for private actions to limit vulnerabilities and losses for those industries and the existing government programs that address those incentives.

Although September 11 stands out as a unique event in U.S. history, many situations exist in which the social benefits from private actions to "take care" exceed the private benefits of such activities. In fact, existing regulatory requirements for the industries examined here provide incentives—and in some case, clear directives—for private parties to take care. Many of those requirements were initiated to meet policy goals for public safety and environmental protection. The overall effect of current programs constitutes a "baseline" of incentives and institutions for protecting the nation, against which any new efforts can be assessed. Finally, the paper lists ideas in three broad groups for new approaches that might prompt industries to do more to enhance security: those that would cause businesses to internalize more of the social costs of terrorist attacks; those that would have the government assume more of the direct responsibility for actions to reduce vulnerabilities and losses from attacks on industry; and those that would improve information that might facilitate private actions.

In the more than three years since the September 11 attacks, lawmakers have enacted legislation affecting homeland security. They have created the Department of Homeland Security and federalized aviation security. To support the Congress's consideration of homeland security policy, this paper presents ideas that could improve security in several key industries. The evaluation is necessarily incomplete because agencies and the Congress both are engaged in ongoing processes to evaluate threats and develop options to address them. The analysis is also at a general level and does not address policy specifics or costs.

Industries Analyzed

This paper focuses on those industries for which the expected human and economic losses from a terrorist attack would be highest—the country's "critical infrastructure." The analysis more narrowly focuses on those industries that reside largely in the private sector and for which an attack could lead to a direct loss of life. The four activities reviewed here, selected from a longer list of critical industries identified by the Department of Homeland Security and chosen because attacks on them could be an immediate threat to lives and health, are:

- Civilian nuclear power,
- Chemicals and hazardous materials (including oil and natural gas),
- Electricity service, and
- Food and agriculture.

Civilian Nuclear Power

Nuclear power plants and the nuclear materials that are being processed or transported or have accumulated as radioactive wastes may be subject to attacks. Safety incidents at U.S. nuclear plants and attacks by terrorists abroad have illustrated the potential to harm people and have long-lasting effects on the environment. Two broad classes of attack that are of special concern are direct attacks (or sabotage) on either nuclear power reactors or the large amounts of spent fuel stored at nuclear plants.

The human, environmental, and economic costs from a successful attack on the nuclear power industry could far exceed the value of the nuclear plants themselves. In the most significant incident in the United States to date—the partial meltdown that occurred at Three Mile Island in Pennsylvania—private economic losses have totaled more than $2 billion. (That sum includes the loss of the nuclear facility, costs of decontamination at the site, costs for decommissioning the destroyed plant, costs associated with initial evacuation of neighbors, and ongoing costs for monitoring the health of local residents.)

Assessments of the actual vulnerability of and potential losses to the nuclear power industry vary widely, with some industry experts believing that little danger exists. However, even according to studies in which the probability of an extreme accident has been postulated to be very remote, the losses from such as accident could be severe. For example, a study by Sandia National Laboratories indicated that in an extreme scenario—with full release of nuclear materials, worst-case atmospheric conditions, and no emergency response—there could be very high losses associated with reactors near population centers. For a reactor near Limerick, Pennsylvania, just outside Philadelphia, the study estimated 75,000 fatalities within a year of the accident, 700,000 injuries, and about $200 billion in costs. Concerning releases from spent nuclear fuel, a study by Brookhaven National Laboratory estimated that a severe accident involving only that waste could cause up to 20,000 cancer fatalities and nearly $60 billion in damages. In contrast, the Nuclear Regulatory Commission said the laboratory's estimate overstates the scope of radiation release that is reasonable to consider, even in a worst case. Such differences in loss and probability assessments highlight the fact that estimates are fraught with uncertainty even when prepared for accidental occurrences, not terrorist-instigated events.

The Nuclear Regulatory Commission has principal authority for regulating civilian nuclear power for public safety. That regulation covers nuclear fuels, nuclear reactors, and spent fuels. Regarding the latter, the Department of Energy (DOE) has primary responsibility for the planning and construction of a permanent disposal facility for high-level radioactive wastes at Yucca Mountain, Nevada—funded in large part from fees paid by nuclear power producers. In addition, other federal programs act to promote nuclear power. They include the indemnity program under the Price-Anderson Act, through which the government addresses the negative financial impact on industry from uncertainty about nuclear accidents, and DOE programs that fund research and development of nuclear technologies.

Chemicals and Hazardous Materials

The security of the chemical industry is important primarily because of the dangers that flammable and toxic chemicals pose for release into the air or water or for immediate explosion and fire. Attacks could be launched on facilities handling such chemicals or the vehicles that routinely transport chemicals through densely populated areas. Alternatively, the chemicals themselves could be used as a weapon. Although an individual business and perhaps a local economy would be harmed by an attack, the national economy would be largely unaffected because many alternative sources exist for almost every chemical—including inventories, other suppliers, and substitute chemicals.

Flammable petrochemicals (including fuels, solvents, and the raw materials to make plastics) are concentrated at a relatively few large production facilities. Another flammable substance, nitrate fertilizer, is available from thousands of agricultural distributors across the country and can form the key ingredient of explosive devices. However, because the areas affected by the explosion or burning of flammable substances are generally limited to the immediate site, relatively few people are expected to be affected by those types of incidents, even in a worst case.

In contrast, small volumes of highly toxic substances released into the air or water could spread farther and affect larger populations. Those substances include ammonia and chlorine, which are used in refrigeration, municipal water purification, and many commercial applications. Each would be poisonous if released in industrial concentration. The great majority of facilities and vessels that

hold ammonia and chlorine are small and would put relatively few people at risk.

Federal, state, and local programs already exist to require or encourage the operators of chemical facilities and the transporters and holders of dangerous chemicals to boost their efforts to promote safety and security and to share information that can help local governments plan for emergencies. Much of the state and local effort is oriented toward emergency preparedness. The federal effort includes worker-safety, environmental, and information programs. Key federal legislation related to the safety of chemical facilities includes the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) and the Clean Air Act Amendments of 1990 (CAAA). The EPCRA requires operators of chemical facilities to prepare contingency plans for possible accidents, provide information to local planners on the chemicals they handle, and notify local officials of any sudden release. The CAAA mandates a role for the Environmental Protection Agency in overseeing risk-management planning by facilities that handle threshold volumes of certain hazardous chemicals identified in the act and by the agency. (Thresholds for toxic substances are based on toxicity and volatility, while thresholds for flammable substances are based on the potential for a vapor-cloud explosion.)

Electricity Service

The vulnerabilities that the nation's electricity supply faces from terrorism are similar to those that the electricity industry confronts from extreme weather and other natural events, accidents, and equipment failures. A terrorist event could disable major physical components of the supply network or disrupt the performance of the network's control centers. The potential losses from such disruptions would be limited and of relatively short duration because the industry and electricity customers are generally well prepared for such failures. Concerns about terrorist attacks may give additional support to proposals that have been discussed to improve the reliability of power supplies, including several related to the competitive restructuring of power markets.

The major vulnerabilities of electricity supplies probably are associated most with regional transmission systems—the power grids that carry electricity at high voltage from power sources to communities. Experiences with major outages involving regional grids suggest ways that a targeted attack could lead to widespread loss, although still for only short periods. Outages that could be longer lasting would be those resulting from attacks on high-voltage transformers, which are difficult to replace quickly.

The costs of an attack on the nation's power supply are likely to be small. The electricity industry is generally well prepared to prevent and mitigate disruptions attributable to many types of system failures—regardless of the cause—so the scale and duration of a disruption would be limited. The prospect of disruptions resulting from the simultaneous loss of several high-voltage transformers could raise the costs of an attack on a targeted community. However, even in that event, the flexibility of electricity consumers and the economy in general to adapt to power losses would help limit the costs of any disruptions that did occur.

Apprehensions about terrorism are part of the industry's more general concern about providing a reliable supply. Investments and operational practices intended to make electricity service reliable are recognized costs covered in the regulated rates that utilities charge their customers. Many groups are involved in ensuring a reliable supply. Historically, the industry has been structured and regulated as regional, vertically integrated monopolies, with state public utility commissions overseeing local operations and approving rates for retail sales and the Federal Electric Regulatory Commission overseeing interstate transmission and rates for wholesale trade. For those utilities, regulators approve investments that reflect the social and private costs of service interruptions—generally providing for sufficient excess capacity to overcome the loss of at least one important component at a time. The North American Electric Reliability Council, an industry group, also establishes voluntary standards as part of its mission to oversee a reliable wholesale electricity supply in North America.

Food and Agriculture

The food and agriculture industry faces vulnerability to attack because of the great number of products at risk and the many unsecured points of access in production, storage, and distribution. In addition to posing threats to health and public safety, disruptions could cause economic harm.

The food and agriculture industry is vulnerable to four basic types of assaults: contamination of food with natural agents (such as botulism and E. coli bacteria), contamination of food with man-made contaminants (such as poisons and foreign objects), attacks to disrupt food sup-

plies (including the use of fires, floods, or biological agents such as foot-and-mouth disease and insects), and use of agricultural resources as weapons for attacks on other targets (such as wildfires that spread to residential areas, nitrate fertilizer for use in explosives, pesticides for poisoning, crop dusters to spread toxins, or radioactive materials used in food irradiation).

Many systems are in place to ensure the safety of food supplies and thus reduce the vulnerability to a terrorist act involving food and agriculture as well as limit any resulting losses. However, risks remain from attacks involving substances that the government does not regularly test for and that may not be readily identified by government agencies and public health officials. The number of publicly documented crimes that have been perpetrated with the intent of harming people or disrupting supplies is small. At the same time, those few known assaults and a number of incidents involving the unintentional contamination of food confirm the potential threats of terrorism to public health.

The nation's economic costs from a disruption of particular food supplies would probably be small, primarily because the food and agriculture industry is well adapted to the prospect of disruptions from weather, pests, and occasional health incidents.

The regulation of the food and agriculture industry involves a number of organizations within four different federal agencies: the Department of Health and Human Services (HHS), the Department of Agriculture, the Department of Commerce, and the Environmental Protection Agency. In the food safety system, HHS's Food and Drug Administration has perhaps the biggest responsibility, regulating about 80 percent of the nation's food supplies to protect consumers against impure, unsafe, and fraudulently labeled foods. The nation's public health system, including the Public Health Service and the Centers for Disease Control and Prevention, is organized to help identify, contain, and treat food-related attacks. Existing government programs also sustain the income of agricultural producers.

The Private Sector's Role in Homeland Security—A General Framework

Markets provide a variety of incentives to producers, their customers, and local communities to guard against a wide range of risks, including the possibility of terrorism. Private producers of goods and services generally will benefit from safe operating practices (including physical security) and the purchase of insurance to help limit any financial losses. But the incentives for private businesses to reduce their vulnerability to attack, and the potential losses for those who would be affected, may be inadequate when the private costs of the threat of terrorism are lower than the social costs (or, equivalently, when the private benefits from security measures are less than the social benefits).

Private costs would be closely associated with damages to production and distribution facilities and the harm to industry workers, as well as the potential loss of business. But the total social costs could go further and include the harm or loss of life to individuals (such as the neighbors of a targeted facility or the consumers of a tainted product), damage to the local environment, and negative effects on other businesses dependent on the targeted industry. If the product of the targeted industry became a potential weapon in attacks elsewhere, the social costs could be broader still. For example, stolen chemicals could be used to attack an office building. If the disparity between private costs and social costs is significant, the result is that private firms have insufficient incentive to meet social objectives.

Many of the government programs that existed before September 11 are intended to bring private and social costs into line. Many firms, especially those in the four critical industries studied here, had long been subject to extensive government intervention because of the dangers that those industries' operations or products can pose to public safety, environmental quality, and local economies.

Existing government programs provide a starting point for examining possible new efforts. Those programs may be adequate to prompt businesses to address much or all of the increased terrorist threat. But if private efforts are inadequate, policy options for prompting additional efforts will probably build on the incentives generated by existing requirements. Cost-effective policies for enhancing homeland security may involve expanding some programs that have nonsecurity goals while reducing others. For example, programs that were intended primarily to help protect the public from relatively common threats, such as industrial accidents or food contamination, could be expanded to help address the terrorist threat. But programs that were intended to disseminate information on critical industries, such as the production and storage ca-

pacities of hazardous facilities, might need to be curtailed to keep that information out of the hands of terrorists.

This paper generally groups government intervention to align the private and social costs of business decisions about security into three broad areas:

- Programs that would internalize the costs of security to private markets by establishing new standards or incentives to make businesses and customers in an industry face the full costs of possible losses.
- Programs that would socialize the costs of security by having the government and taxpayers directly bear the costs of reducing losses, whether through the government's own efforts or its financing of efforts by businesses and customers.
- Programs that would provide the private sector with information on the risk of attacks, the losses from attack, and opportunities to reduce losses.

If a chemical production facility was subject to an attack, for example, the ensuing fire or explosion could expose the surrounding community to dangerous toxins. That added exposure would represent a social cost that the private firm would not face—especially if the damage exceeded the limits of the owner's insurance coverage and other financial resources. As a result, the owner would have less incentive than otherwise to guard against such attacks, scale back operations, or relocate. Current government programs affecting the safety of chemical-plant operations and supporting local emergency preparations are a response to that social cost and also contribute to homeland security. However, the increased awareness of the terrorist threat since September 11—if not the threat itself—also may indicate a need to step up security efforts since the social benefits of spending on security have increased.

The type of intervention that would force industry to internalize the costs of security (and for which it would bear the immediate costs) would include requirements to take preventive measures, assessment of penalties for failing to take certain actions, or imposition of taxes on certain activities or products.

The type of intervention that would have the government socialize the cost—so that everyone paid for the enhanced security—would include new programs that rewarded industry for taking measures to protect vulnerable facilities or make those facilities less dangerous (for example, by supporting the adoption of safer production processes or the use of safer chemicals).

Alternatively, rather than force or pay industry to make certain changes, new programs could help inform nearby residents of the dangers of an attack or inform industry of currently available options for reducing its vulnerabilities.

Strategies to Enhance Homeland Security

The broad strategies described in this paper are not policy recommendations, nor do they delineate policies in any detail. Many of the ideas build on programs now in place for one industry that may be applicable to another industry or, where several industries already are subject to similar requirements, that may help identify effective alternative approaches. Some of the ideas are currently being considered by the Congress or have been proposed elsewhere.

For nuclear power and chemicals, some common themes emerge. Among new approaches that would internalize more of the costs of terrorist attacks within an industry are:

- Establishing fees or taxes on sales of the industry's product or service to discourage its use (in cases in which less production would mean lower potential losses);
- Establishing new regulations for tracking the ownership of hazardous chemicals that could be used as weapons;
- Establishing new, more stringent regulations that would require safe production practices (for example, increasing monitoring for toxic chemical releases or limiting volumes of the spent nuclear material stored near reactors);
- Creating financial disincentives for businesses or residents to locate in danger zones (for example, by requiring higher insurance coverage or limiting other available business tax incentives);

- Establishing enhanced incentives and protection for reporting unsafe practices, conflicts with best-technology safety practices, or other sources of vulnerability and potential losses; and

- Requiring additional insurance coverage.

Alternatively or in combination, new approaches for the nuclear and chemical industries could socialize the costs of security—placing the direct costs of enhancing security on taxpayers. If the federal government has a strong cost advantage over the private sector in performing certain security activities, federalizing those activities may be cost-effective. New initiatives could include:

- Establishing positive fiscal incentives for businesses to adopt safer designs or production processes;

- Providing financial assistance to people and businesses to move away from potentially hazardous sites; and

- Federalizing and expanding the current level of perimeter security, structural defenses, and employee screening.

Businesses and neighboring communities may underestimate the likelihood of a terrorist attack and thus misgauge the risks and costs of such an incident. Some ideas for new approaches related to nuclear power and chemicals that could help improve information include:

- Preparing vulnerability assessments and potential damage assessments that better reflect the worst-case scenarios for terrorist attacks (rather than accident scenarios);

- Making additional information available to governments on the vulnerability of certain facilities and products, both to aid in emergency planning and to encourage businesses to reduce those vulnerabilities;

- Establishing emergency planning zones that better reflect current information on estimates of losses and account for more-complex worst-case failures (for example, involving multiple systems or attacks on multiple industries); and

- Establishing a national zoning system (for chemical plants and nuclear plants) to help inform property owners of their risks.

Potential strategies for electricity service include preparing for the threat of attack on critical equipment that might require significant time to replace (such as high-voltage transformers) and supporting reforms that would make the electricity supply more reliable in the event of a disruption. Providing more information on alternative supplies of electricity could enable consumers to reduce their dependence on single, vulnerable suppliers.

For the food and agriculture industry, initiatives that would help internalize the costs of attacks within the industry could include requirements for enhanced product labeling and tracking (to help identify and contain a potential contamination) and changes in the product specifications or tracking requirements for dangerous agricultural supplies (in particular, nitrate fertilizers and pesticides that can be used as weapons). Some of those costs might be borne by the public if the government increased its inspection of food supplies.

CHAPTER

1

Introduction

The events of September 11, 2001, and subsequent revelations of terrorist plans raised the nation's awareness of the potential scale of terrorist attacks, the likelihood of such attacks, and, as a result, the potential losses from terrorism. Federal, state, and local governments as well as the private sector may contribute to security efforts to help reduce the chances of attack and the losses from an attack at the lowest overall cost to the economy. The private sector generates the vast majority of the nation's economic output, and there are corresponding incentives and opportunities for businesses to undertake security measures. Nevertheless, the few data that are available suggest that since September 11, relatively little additional spending has come from the private sector.[1]

There have been calls for new laws or regulations that would require businesses to take an increased role in the nation's defense against terrorists, an approach that assumes it would be cost-effective for the private sector to enhance homeland security. This paper reviews the vulnerabilities and potential losses for several key industries and the current market and government incentives and institutions for undertaking security efforts. The paper describes a broad range of policy approaches for each industry that could enhance the existing, or "baseline," incentives for security. The baseline consists of current programs, laws, and regulations that affect the likelihood of attack, the potential damage from attack, and the response to (and ultimate cost of) an attack. The options for new initiatives are not policy recommendations, nor do they delineate policies in any detail.

What Is Homeland Security?

Homeland security has been described as 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."[2] At a basic level, enhancing security means reducing the potential losses from terrorist attacks and the risk of such attacks. "Terrorism" means criminal acts by individuals or groups (whether of domestic or foreign origin) motivated by political or social agendas. Statutory definitions of terrorism refer to criminal acts that are dangerous to human life and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government.[3] In common usage (and in this paper), terrorism also includes acts that may be designed to harm property and, more broadly, economic infrastructure, with the intent of furthering some political or social objective.

From a public policy perspective, attacks by similar means may be associated with national security threats (perpetrated by foreign governments) and criminal threats (perpetrated by individuals for their personal gain). And similar damages may occur from natural events, technological failures, or human error. As a result, homeland security activities are closely related to ongoing

1. For example, see the Conference Board, *Corporate Security Management: Organization and Spending Since 9/11* (New York: Conference Board, July 2003); Council on Competitiveness, *Creating Opportunity Out of Adversity: Proceedings of the National Symposium on Competitiveness and Security* (Washington, D.C.: Council on Competitiveness, December 2002); Council of Insurance Agents & Brokers, "Many Commercial Interests Are Not Buying Terrorism Insurance, New CIAB Survey Shows" (press release, Washington, D.C., March 24, 2004); and Bart Hobijn, "What Will Homeland Security Cost?" *Economic Policy Review,* Federal Reserve Bank of New York (November 2002).

2. Office of Homeland Security (predecessor to the Department of Homeland Security), *The National Strategy for Homeland Security* (July 2002), p. 2.

3. The basic legal definitions of international and domestic terrorism appear in 18 U.S.C. 2331.

activities by businesses and governments to promote general safety.

Viewed from the perspective of existing policies, businesses already may be doing as much as is in the national interest to enhance homeland security, given that the lowest-cost options may be dominated by the public sector. However, private incentives for security that were adequate before September 11 may now be considered insufficient. If so, new government interventions to enhance private security efforts may be appropriate.

A Focus of Security Concerns: Critical Industries

Critical industries are those in which the expected human and economic losses from a terrorist attack would be highest. Expected losses reflect both the probability of attack (as jointly determined by the attractiveness of a target and its vulnerability) and the amount of damage that could occur. Losses may be associated with the incidental damage and loss of life that result from the destruction of facilities or the diversion of hazardous materials to attacks elsewhere, with the direct harm from contamination of products, or with the indirect harm from the loss of products or services. The risk of such attacks may also entail losses, including direct emotional trauma and economic losses because employees or customers want to avoid the industry.

Of immediate concern in protecting homeland security are the physical assets that could be attacked (including factories, buildings, transmission lines, and the like) and the less-tangible assets (such as networks for moving goods, energy, or information) that could be threatened. People could be harmed from a disruption of emergency services during a power outage as well as in a direct assault on a factory. The nation has adopted the term "critical infrastructure" to describe such targets (see Box 1-1 for more details about the concept of critical infrastructure).

The Department of Homeland Security has identified a number of critical industries with "infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security."[4] Those critical-infrastructure sectors are agriculture, food, water, public health, emergency services, government, defense, information and telecommunications, energy, transportation, banking and finance, chemicals, and postal and shipping services.[5]

This paper focuses on four of those critical-infrastructure industries that reside largely in the private sector. Those industries are:

- Civilian nuclear power,
- Chemicals and hazardous materials (including oil and natural gas),
- Electricity service, and
- Food and agriculture.

Why the Private Sector Might Spend Too Little on Security

Businesses would be inclined to spend less on security than might be appropriate for the nation as a whole if they faced losses from an attack that would be less than the overall losses for society. A number of common circumstances can exist in private industry in which there is a gap between the private and public costs of a terrorism event.

Private costs for businesses or individuals could include spending for defensive measures to lower their vulnerability to attack, changes in location or operations to reduce their losses from an actual attack, or emergency-response capabilities to help contain those losses. Businesses could also reduce exposure to some types of losses by scaling back operations. But when terrorists target a business, they put others at risk, too. Those other businesses and individuals may not be in a position to undertake their own security efforts—for example, they may not know about the threat. And in some cases, they may not be able to hold the targeted business liable for the damages that they incur. The social costs of terrorism would be the sum of those costs incurred by others and the private costs incurred by the targeted business.

---

4. Executive Order 13010, "Critical Infrastructure Protection," *Federal Register,* vol. 61, no. 138 (July 17, 1996), p. 37347.

5. Office of Homeland Security, *The National Strategy for Homeland Security.*

Box 1-1.

Changing Concepts of Critical Infrastructure

In an executive order authorizing federal agencies to adopt protective measures, President Clinton defined critical infrastructures as those that are "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[1] The concept of critical infrastructure and critical assets has broadened in the past few years to go beyond concerns just about defense and economic security. The PATRIOT Act of 2002 refers to those "systems and assets, whether physical or virtual, so vital to the United States that [their incapacitation] . . . would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [2]

A related concept is that of a target industry. Some critical industries may be the target of attack, with the losses at stake closely associated with production and distribution in those industries. In the case of other critical industries, their products may be more akin to weapons used to carry out attacks elsewhere (such as highly flammable chemicals used to make explosives). Still other industries may be critical to homeland security because their products are part of the solution to terrorism—in particular, the finance and telecommunications industries, which can contribute to efforts to stem flows of money or communication among terrorist groups.

1. Executive Order 13010, "Critical Infrastructure Protection," *Federal Register*, vol. 61, no. 138 (July 17, 1996), p. 37347, available at www.ntia.doc.gov/osmhome/cip/eo13010.pdf.

2. Further discussion of the concept of critical infrastructure appears in Office of Homeland Security, *The National Strategy for Homeland Security* (July 2002).

Incomplete information about the nature of the vulnerabilities, the potential losses, or the costs of options for enhancing security can lead to too little private spending on security, especially when all of the affected players do not have access to the same information. For example, a business may know about its exposure to attack, but the firm's customers or the surrounding community (and local emergency planners) may not. Or the government may have knowledge of threats, losses, or solutions that private businesses do not have. (In some cases, there may be an argument for withholding available information on vulnerabilities or losses if that disclosure would increase the attractiveness of a particular target to terrorists. That possibility should be weighed in considering policy operations to improve private incentives for spending on security.)

The term "moral hazard" describes the reluctance of businesses or individuals to undertake protective measures that are otherwise in their interest because they believe that someone else will pay the bill for any damages that are incurred. Insurance companies try to avoid that problem by requiring their customers to take preventive measures or encouraging them to do so through the premium structure or copayments. In the case of homeland security, the prospect of moral hazard can create a gap between social and private costs if, for example, businesses expect the government to compensate them for major losses from an attack.

What Is the Government's Role?

If the social costs of terrorism exceed the private costs, governments may be able to help correct the consequences of any differences between social and private perspectives. Broadly speaking, the government can choose among three approaches to affect the behavior of businesses:

- *Internalizing the costs of security.* Policies could include new regulations affecting the behavior of businesses or consumers. They could also include new taxes or penalties that would raise the cost of not undertaking such activities. The effect would be to make businesses, their customers, or at-risk populations (such as the neighbors of an at-risk facility) face more fully the costs of potential losses.

- *Socializing the costs of security.* The government (and indirectly the general tax-paying public) could assume the costs of reducing risks and potential losses, either by undertaking protective measures itself or by financing efforts by businesses, their customers, and affected populations to enhance security.

- *Providing better information for making security decisions.* For example, programs could be created to give businesses and individuals additional information on the risks of attacks, potential losses from attacks, and opportunities for reducing risks. Such programs could include information collection and dissemination, as well as research and development—either by the government or, in response to regulatory or financial incentives, by businesses.

Those approaches sometimes overlap. For example, the Transportation Security Administration imposes a fee on private airlines to help pay for government screening of passengers. That program both forces airlines and their customers to internalize costs of security and, if the fee does not cover all of the costs, socializes the remaining costs of providing security by paying for them from general revenues.

The choice among both general approaches and specific options will depend in large part on the cost-effectiveness of the action—how fully it improves security and at what cost. In some instances, the government will have a cost advantage over the private sector in performing an activity. (For example, cost-effectiveness was among the arguments used in support of the federal takeover of airline passenger screening.) Areas where the government is likely to have a cost advantage are related to services that the government already provides, such as intelligence gathering, law enforcement (including potential screening of employees), and research and development. Similarly, local governments have an advantage in providing first-responder services.

Some specific options have serious drawbacks. For example, making more information on terrorist threats, vulnerabilities, and potential losses generally available means that potential terrorists also might access that information. Further, not all communication among businesses provides a social benefit. Antitrust concerns cause the government to restrict information sharing among competitors.

The Government's Response Since September 11—A Baseline for Further Change

All of the critical industries discussed in this paper were subject to extensive government intervention before September 11 to mitigate the danger that they—or disruption of their operations—can pose to public safety, environmental quality, and the national or local economies. Since that date, additional measures that specifically address security concerns have been implemented. Those new programs—plus the earlier ones that restrict industry activity to prevent or mitigate industrial accidents, natural disasters, or crime—serve as a starting point for identifying additional efforts needed to address an increased terrorist threat.

Numerous programs are in the domain of state and local governments. Containing the losses from a terrorist attack frequently falls to the emergency first-responder services of local governments—including the fire, police, medical services, and relief-support agencies. State and local governments have an active role in preparing for emergencies involving many of the critical industries that may be vulnerable to terrorist attacks. In some of those industries, state and local governments may have a regulatory or a direct ownership role. For example, local governments provide electricity services to many communities and also own some of the nation's large dams—any of which may be the target of attack. State and local governments also participate in emergency preparedness by regulating activities of industries that may be subject to attack and establishing zoning requirements that restrict activity near hazardous facilities.

The federal government responded to the increased threat of terrorism after September 11 with a number of administrative and legislative initiatives to address perceived immediate needs. The President issued a series of Homeland Security Presidential Directives establishing a Homeland Security Council to coordinate the actions of federal agencies, setting up the homeland security advisory system, directing changes in immigration policy and the tracking of foreign visitors, and implementing other measures to reduce the immediate risk of attack and spread information on the threat. The Congress also took a number of actions in the period immediately following September 11 in the areas of aviation security, surveillance powers for law enforcement, and funding of state and local first responders. In addition, it acted to reim-

burse many of the direct victims of the attacks and to limit the liability of airlines used in the attacks by passing, respectively, the Victims of Terrorism Tax Relief Act of 2001 and the Air Transportation Safety and System Stabilization Act of 2001.

The Administration and the Congress now are assessing broad strategies to improve security that will be funded and overseen by the Congress. Those include programs to facilitate the sharing of information between government and the private sector (see Box 1-2).

Among the important new laws enacted since September 11 are:

- The Aviation and Transportation Security Act of 2001, establishing the Transportation Security Administration and federalizing airline passenger screening;
- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (or the USA PATRIOT Act) of 2001, introducing legislative changes to increase the surveillance and investigative powers of law enforcement agencies in the United States;
- The Homeland Security Act of 2002, reorganizing federal agencies to establish the new Department of Homeland Security;
- The Support Anti-Terrorism by Fostering Effective Technologies Act (or SAFETY Act) of 2002, protecting merchants from liability for technologies that do not perform as intended in a terrorist attack;
- The Terrorism Risk Insurance Act of 2002, establishing a temporary federal terrorism reinsurance program to provide some public compensation for insured losses from terrorism;
- The Public Health Security and Bioterrorism Preparedness and Response Act of 2002, authorizing the creation of medical stockpiles to prepare for biological attacks and other measures;
- The Maritime Transportation Security Act of 2002, requiring the Coast Guard and other agencies to improve security at the nation's ports and waterways by requiring security assessments, new security plans, and new security measures;
- The Enhanced Border Security and Visa Entry Reform Act of 2002, requiring measures to help counter illegal aliens and track potential terrorists in the country;
- The Federal Information Security Management Act of 2002, requiring measures to protect federal information and information systems; and
- The Project BioShield Act of 2004, requiring measures to expand and expedite the availability of vaccines and treatments to combat potential bioterrorism agents.

Among new legislation that the Congress is considering are measures that would affect the reliability of electricity supplies and require further security actions in such areas as civilian nuclear power, air freight, and chemical facilities. Also under consideration are revisions to some of the laws already enacted, including the USA PATRIOT Act. The Terrorism Risk Insurance Act is scheduled to lapse at the end of 2005, and bills to reauthorize the terrorism reinsurance program are before the Congress.[6]

Improving Homeland Security—A General Framework

This paper examines additional approaches that may be appropriate to bring incentives for private-sector spending on homeland security in line with social objectives. Many of those approaches are under discussion. For example, the Government Accountability Office (GAO, formerly the General Accounting Office) has summarized the many recommendations from commissions created by the Congress to look at the nation's security in general.[7] Further suggestions have come from the National Research Council, the Brookings Institution, and the

6. See Congressional Budget Office, *Federal Terrorism Insurance: An Update* (forthcoming, January 2005).

7. General Accounting Office, *Homeland Security: Selected Recommendations from Congressionally Chartered Commissions and GAO*, GAO-04-591 (March 2004). The findings reviewed are those of the National Commission on Terror (or Bremmer Commission), the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (or Gilmore Commission), and the U.S. Commission on National Security/21st Century (or Hart-Rudman Commission).

Box 1-2.

Government Efforts to Share Information with Industry

Many formal and informal relationships exist to share information that is relevant to homeland security. Some of those relationships encompass basic government efforts to open lines of communication—describing government services and funding opportunities, hosting informational conferences, and providing training sessions.[1] Other federal initiatives, such as disaster-preparedness grants from the Federal Emergency Management Agency, involve directly funding the coordination efforts of local governments and businesses.

One initiative that is particularly relevant to homeland security is the Information Sharing and Analysis Centers, or ISACs. ISACs generally are private-sector organizations (or networks of organizations) that the federal government has helped create to disseminate real-time information on threats to critical industries (see table on facing page). In addition to helping get the word out on imminent threats, ISACs can serve as forums to help coordinate efforts to identify and reduce vulnerabilities.

The government first encouraged the development of ISACs in 1998 through Presidential Decision Directive-63, calling for ISACs to serve as a mechanism for gathering, analyzing, and disseminating private-sector information and sharing that information with the government.[2] ISACs are generally funded by membership fees or federal grants, although the ISAC for information technology is operated by the federal National Communications System, with participation by federal agencies and industry.[3] Some of the major trade organizations represented in the ISACs (including the American Petroleum Institute, the American Chemistry Council, and the North American Electric Reliability Council) have been active both in establishing standards for safety and security in their industries and in working with local governments to plan for emergencies.

1. For example, see the description of public/private partnerships by the Department of Energy's Office of Assurance at www.ea.doe.gov/partnerships.html.

2. Presidential Decision Directive/NSC-63, May 22, 1998, available at www.fas.org/irp/offdocs/pdd/pdd63.htm.

3. Information on membership of the ISAC for information technology is available at www.ncs.gov/ncc/main.html.

House Select Committee on Homeland Security.[8] GAO has provided its own analyses for specific industries, too, as has the Congressional Research Service. The Congressional Budget Office has provided cost estimates for some of the proposals that have already been offered in the form of new legislation.[9]

In this analysis, the ideas for new approaches in each industry are organized into three areas: approaches that would cause private actors (businesses, their immediate customers, and the neighbors of potential physical targets) to internalize more of the social costs of an attack, those that would have the government and taxpayers assume more of the direct responsibility for reducing the social costs of an attack, and those that would improve information on the risks and costs of an attack so that private actors could make better decisions about security.

The following example may help explain the problem facing policymakers. If a chemical production facility was subject to an attack, the ensuing fire or explosion could expose the surrounding community to dangerous toxins as well as destroy the facility. That broad exposure would represent a social cost of continued operation that would

8. Michael E. O'Hanlon and others, *Protecting the American Homeland* (Washington, D.C.: Brookings Institution Press, 2002); National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: National Academies Press, 2002); and Democratic Staff of the House Select Committee on Homeland Security, *America at Risk: Closing the Security Gap* (February 2004).

9. Congressional Budget Office cost estimates are available at www.cbo.gov.

Box 1-2.

Continued

Information Sharing and Analysis Centers for Selected Critical Industries[a]

ISAC	Lead Industry Group(s)	Major Activities
Chemical Industry	American Chemistry Council (Chemtrec)	Provides public-service hotline for firefighters, law enforcement, and other emergency responders to obtain information on and assistance for emergency incidents involving chemicals and hazardous materials. Maintains material-safety information and emergency contacts for manufacturers and shippers. More information at www.chemtrec.com.
Electric Power	North American Electric Reliability Council (NERC)	Disseminates threat indications, analyses, and warnings, together with interpretations, to help participants in the electricity sector take protective actions. NERC further coordinates cyber security, physical security, and operational security through its Critical Infrastructure Protection Committee. More information at www.nerc.com/~filez/cip.html.
Energy (Oil and Gas)	American Petroleum Institute, American Gas Association, National Petrochemicals & Refiners Association (operated by Science Applications International Corporation)	Maintains industrywide database of electronic security threats, vulnerabilities, incidents, and solutions. Provides a confidential venue for sharing security vulnerabilities, solutions, and best practices. More information at www.energyisac.com.
Food Industry	Food Marketing Institute	Disseminates warnings (from the Federal Bureau of Investigation) to participants, reports incidents, provides technical expertise to help evaluate reports, and coordinates industrywide response to attack. More information at www.fmi.org/isac/isacorgstructure.pdf.

Source: Department of Homeland Security.

Note: Web links for all of those organizations may be found at www.dhs.gov/dhspublic/display?theme=73&content=1375

a. There is no ISAC for nuclear power. That function is covered in part by the ISACs for electric power, surface transportation, and emergency services. Information on specific threats to the nuclear power industry is disseminated primarily by the Nuclear Regulatory Commission and law enforcement agencies, although general information is also available to nuclear-plant operators from the Nuclear Energy Institute and other trade associations.

exceed the private costs if those broad losses did not fall fully on the facility owner, especially if the damage exceeded the limits of the owner's insurance coverage and other financial resources.

In that situation, the owner's losses alone would provide less incentive to undertake preventive actions than would the full costs of an attack.

Many different types of programs could help address such a problem. Programs that would internalize the costs of security could include requiring the relocation of an at-risk facility (or a reduction in the neighboring population), requiring businesses to adopt the use of less volatile materials, or establishing regulations that would change protective services or production processes. Programs that would socialize the costs could include providing tax incentives or direct subsidies for businesses to add physical protections or to adopt the use of less volatile materials and increasing public funding for local emergency services. Information programs could include helping local populations learn about risks and plan for contingencies.

Scope of the Analysis

This paper aims to develop a useful framework for thinking about homeland security policies and to formulate ideas for new programs in the context of that framework. Those ideas are all subject to limitations and caveats. First and foremost, because the costs of a terrorist attack in each industry cannot be known, the return from implementing the approaches outlined here cannot be known. Also, this paper does not present the options in detail; thus, a cost-benefit analysis of them is not possible. Instead, the paper generally characterizes the economic effects of different options, noting their impact on resource allocation and, where possible, the magnitude of their cost. In some cases, it could be inferred that additional security motivated solely by potential terrorist attacks is not likely to be worthwhile.

Further, this analysis is limited in that it narrowly focuses on four industries. Terrorists could well choose targets that are not a part of those industries. Regarding alternative targets, a target's attractiveness to terrorists is generally thought to depend in part on the security of other potential targets. That is, the various options described here may not achieve their full potential to enhance total security if they cause terrorists to look elsewhere.

CHAPTER

2

Civilian Nuclear Power

Members of the terrorist group that attacked the World Trade Center and the Pentagon on September 11, 2001, indicated that they also were interested in attacking the nation's nuclear power plants. That information, in the context of an increased national threat, is drawing attention to concerns about the vulnerability of nuclear reactor cores and the spent nuclear material stored at power plants, as well as the need to guard nuclear material in transit and at different stages of production. Two notable accidents involving nuclear plants—Chernobyl in Ukraine and Three Mile Island outside Harrisburg, Pennsylvania—indicate the potential losses from an attack, as do studies of the possible consequences of accidental releases. This chapter focuses on security concerns associated with nuclear power used for electricity generation. It excludes concerns about the use of low-level radioactive materials in medical applications, research, and food irradiation—large amounts of which would be needed to fashion any kind of weapon.[1]

Vulnerabilities from Attacks on Power Reactors and Spent Material

The staff of the National Commission on Terrorist Attacks Upon the United States reports that a precursor to the September 11 plan included crashing two airplanes into two unspecified nuclear plants.[2] In 2003, Energy Secretary Spencer Abraham said there was evidence that terrorists may have specifically targeted the Palo Verde nuclear power plant near Wintersburg, Arizona—the largest commercial nuclear facility in the country.[3] A year earlier, a National Research Council report concluded that nuclear power plants "may present a tempting high-visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high."[4]

Where Nuclear Plants Are Vulnerable

Nuclear facilities and nuclear materials in the private sector could present several different types of targets to a terrorist—wherever nuclear fuels are produced, transported, and consumed, and wherever production wastes are accumulated.[5] Currently, 104 licensed nuclear reactors are operating at 65 power plants in 31 states; they supply about 20 percent of the nation's electricity.[6]

Power plant operators are most concerned about direct attacks and sabotage that may target nuclear reactors or the spent fuel stored by nuclear plants. (If the government proceeds with plans to transport spent material to long-term storage facilities, the security of material in transit also will become a concern.) Reactor cores are contained in concrete structures to prevent accidental releases

1. For a discussion of security issues involving low-level radioactive material, see General Accounting Office, *Federal and State Action Needed to Improve Security of Sealed Radioactive Sources*, GAO-03-804 (August 2003).

2. "Outline of the 9/11 Plot" (Staff statement no. 16 to the National Commission on Terrorist Attacks Upon the United States, June 16, 2004), p. 13, available at www.mint.org/pdf/NCTAUTUS-staff-statement-16.pdf. Also see reports by CNN on an internal memorandum of the Nuclear Regulatory Commission citing the debriefing of a senior al Qaeda operative, available at www.cnn.com/2002/US/01/31/ret.terror.threats/.

3. Statement of Spencer Abraham, Secretary of Energy, before the Senate Committee on Armed Services, March 20, 2003, available at armedservices.senate.gov/statemnt/2003/March/Abraham.pdf.

4. National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, D.C.: National Academies Press, 2002), p. 50.

5. For a review, see Congressional Research Service, *Nuclear Power Plants: Vulnerability to Terrorist Attack*, CRS Report for Congress RS21131 (updated September 17, 2004).

6. Congressional Research Service, *Nuclear Energy Policy,* CRS Issue Brief IB88090 (updated October 26, 2004), pp. 1-2.

of radiation—a design feature that also can afford some protection against physical assaults. To further limit the possibility that a ground attack or internal sabotage could cause a major release of radioactive material, facilities observe internal safeguards (such as backup electric power for pumps) and take measures to ensure secure perimeters. Further, the Nuclear Regulatory Commission (NRC) requires background checks of all nuclear operations.[7] The NRC periodically issues directives on the types of attacks that its licensees must protect against. The latest directive requires plants to prepare for the "largest reasonable threat against which a regulated private guard force should be expected to defend under existing law."[8] However, NRC policy specifically exempts nuclear plants in the United States from any requirement to be built or operated "for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States . . . or (b) use or deployment of weapons incident to U.S. defense activities."[9]

Nuclear power plants are also vulnerable to attacks on the large quantities of spent nuclear fuel stored on-site.[10] That fuel, which is held outside the reactor core containment structures, may be more vulnerable than the reactor cores. Most of the spent material currently is stored in cooling pools. At some plants, the storage areas for those pools are built with thick concrete walls and located partially below ground level, which would afford them some protection. But at other plants, the pools are covered only by lightly constructed steel frame buildings. Regardless, the fuel stored in those pools would remain at risk to any attack that harmed the water cooling systems. As the radioactivity of the spent fuel diminishes with time, some of the fuel can be moved to storage in dry casks, where its low radioactivity makes it of less concern. At the end of 2002, U.S. electric utilities were holding more than 47,000 metric tons of spent nuclear fuel, in both wet and dry storage, accumulated from about 35 years of nuclear power generation.[11]

A terrorist attack could cause greatest harm if radioactive materials were released, whether as a direct consequence of an explosion or an ensuing fire or as an indirect consequence of disabling a plant's cooling systems or other system safeguards. Any attack that breached the containment structure for the reactor core or the spent fuel kept in wet or dry storage could cause an explosion or fire. An attack that resulted in coolant loss in the reactor core could lead to core damage or a melting of the fuel.

Other systems at risk in a nuclear power plant include electricity supplies, circulation pumps, the intakes for cooling water, and other piping. Problems in any of those areas could cause temperatures to rise excessively or lead to excessive steam pressure. An attack could also complicate the shutdown of the fission process. Normally, operators insert neutron-absorbing control rods among the uranium fuel rods in the reactor core or remove the fuel rods altogether to halt fission. Without water, the fission process would stop, but removing the fuel from the core at that point would be nearly impossible, and the radioactive material could be spread by any fire. (In the event of a fire, radioactive material might be vented unintentionally to the outside even if the walls of the containment structure for the reactor core were not breached.)

Concerning the intentional crashing of a large aircraft, research provides conflicting information about how well the reactor core or spent-fuel storage areas of a nuclear plant could withstand such an assault. For example, the Electric Power Research Institute conducted a study for the Nuclear Energy Institute using a computer simulation of a wide-bodied aircraft striking a nuclear plant. It concluded that although the structure housing spent fuel could be breached, cooling water would not be lost, and

7. The Nuclear Energy Institute, a trade group representing the industry, provides brief descriptions of security measures at nuclear plants (available at www.nei.org/index.asp?catum =2&catid=274) and of the special security for reactor cores (available at www.nei.org/index.asp?catnum=2&catid=276).

8. For a discussion of the most recent directives, known as a design basis threat, see Government Accountability Office, *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*, GAO-04-1064T (September 14, 2004).

9. 10 C.F.R. 50.13.

10. See Robert Alverez and others, "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States," *Science and Global Security*, vol. 11, no. 1 (2003), pp. 1-60. For a critique, see Nuclear Regulatory Commission, *Fact Sheet on NRC Review of Paper on Reducing Hazards from Stored Spent Nuclear Fuel* (August 2003), available at www.nrc.gov/reading-rm/doc-collections/fact-sheets/reducing-hazards-spent-fuel.html.

11. Department of Energy, Energy Information Administration, *Detailed U.S. Spent Nuclear Fuel Data as of December 31, 2002* (October 1, 2004), available at www.eia.doe.gov/cneaf/nuclear/spent_fuel/ussnfdata.html.

the concrete containment structure for the reactor would not be ruptured.[12] In contrast, the Nuclear Control Institute reported that by its calculations, a Boeing 767 could penetrate at least 3 feet of reinforced concrete at a full cruising speed of 530 miles per hour.[13] (Typical reactor containment structures have walls 3½ feet to 6 feet thick.)[14] Variables that would determine actual vulnerability to attack by air include the plane's size, the speed and angle of descent, and the amount of fuel (or other explosives) on board, as well as the topography of the area and the design of the plant and other structures. An aircraft collision that disrupted water cooling and external safety equipment could start a fire even without fully penetrating the containment structure.

History of Accidents and Assaults

The nature of technological vulnerabilities is revealed by the history of safety incidents involving nuclear plants (including civilian, military, and research facilities), uranium enrichment facilities, and nuclear material in transit that have caused or threatened the release of radioactive material.[15] Among such incidents, the accidents at Chernobyl in 1986 and Three Mile Island in 1979 are the most noteworthy.

Further evidence of nuclear plants' direct vulnerability to attack comes from the history of actual assaults on nuclear facilities. Although plants in the United States have not experienced an armed assault, much less a large-scale attack, facilities in other countries have been attacked by politically motivated groups. Among those events were multiple assaults by Basque separatists in Spain, multiple attacks by Chechen fighters in Russia, an apartheid-era attack by ground forces in South Africa, and a rocket attack in France.[16]

Future attacks in the United States could come on the ground (possibly using high explosives or military weapons such as rocket-propelled grenades) or involve a collision by a large or small aircraft loaded with explosives. To counter potential ground attacks, plants' security guards now generally train to prevent intruders from taking over a facility or causing harm at close quarters. NRC-supervised mock attacks involve lightly armed attackers and periodic tests of those security measures suggest that weaknesses may exist.[17]

Potential Losses from Exposure to Radioactivity and Destruction of Power Facilities

The human, environmental, and economic costs from a successful attack on a nuclear power plant that results in the release of substantial quantities of radioactive material to the environment could be great. The losses from an attack on civilian nuclear facilities could include not just the immediate personal injury and economic and environmental damage but also the long-term harm. People who survive initial exposure to substantial amounts of radiation will remain at an elevated risk for reproductive problems and cancer for their entire lives. Other people will face continued risk of exposure to any radioactive material that remains in the environment. Further costs include the loss of electricity-generating capacity and expenses required for a best-effort cleanup and decontamination of the attack site. In 2002, the National Research

12. See Nuclear Energy Institute, *Deterring Terrorism: Aircraft Crash Impact Analyses Demonstrate Nuclear Power Plant's Structural Strength* (December 2002), available at www.nei.org/documents/eprinuclearplantstructuralstudy200212.pdf.

13. Letter from the Nuclear Control Institute and the Committee to Bridge the Gap to Richard Meserve, Chairman of the Nuclear Regulatory Commission, September 14, 2001, available at www.nci.org/01nci/09/letter-mserve-14.htm.

14. Paul Gaukler, D. Sean Barnett, and Douglas J. Rosinski, "Nuclear Energy and Terrorism," *Natural Resources & Environment*, vol. 16, no. 3 (Winter 2002), available at www.abanet.org/environ/pubs/nre/specissue/gauklerbarnettrosinski.pdf.

15. For information on collective radiation exposure, unplanned capability losses, and industrial safety involving U.S. nuclear plants, see Institute of Nuclear Power Operations, *2002 Performance Indicators for the U.S. Nuclear Industry*, available at www.nei.org/documents/Wano_Performance_Indicators_2002.pdf. For international safety statistics, see World Association of Nuclear Operators, *WANO Performance Indicators 2002* (London: WANO, June 2003), available at www.wano.org.uk/PerformanceIndicators/PI_Trifold/PI_2002_TriFold.pdf. For a list of incidents involving nuclear materials, see Wm. Robert Johnston, *Nuclear Terrorism Incidents* (September 23, 2003), available at www.johnstonsarchive.net/nuclear/wrjp1855.html.

16. For additional information on terrorist attacks on nuclear power plants, see Gavin Cameron, "Nuclear Terrorism Reconsidered," *Current History*, vol. 99 (April 2000), pp. 154-157.

17. For discussions of concerns about security preparedness, see Nuclear Control Institute letter to the Chairman of the Nuclear Regulatory Commission, September 14, 2001; and Government Accountability Office, *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*.

Council concluded that a September 11-type attack could have "severe consequences" depending on the scale of the attack and the design of the plant involved.[18]

Studies of Health Costs

Research on health threats from large-scale radiation exposure has yielded considerable disagreement over what constitutes a reasonable worst-case scenario to analyze—in terms of how an accident could occur, how far radioactive material could be dispersed, and how effective the emergency response would be. In studies that have shown large potential losses, the probability of such accidents was deemed minuscule. In one study of nuclear reactor cores conducted in the early 1980s for the NRC, Sandia National Laboratories reported on the likelihood of deaths and injuries from accidents at individual reactors across the country. It evaluated an extreme scenario that assumed a full release of nuclear materials, worst-case atmospheric conditions, and no emergency response. For reactors near population centers, the potential losses were quite high, with the most extreme being from a severe release from one of the reactors in Limerick, Pennsylvania, northwest of Philadelphia—more than 75,000 fatalities within a year of the accident, about 700,000 injuries in the same time frame, and about $200 billion in costs (not adjusted for inflation).[19] In a separate study for the NRC, Brookhaven National Laboratory considered the consequences of a severe accident involving only spent fuel and concluded that such an accident could cause up to 20,000 cancer fatalities and nearly $60 billion in damages.[20]

Such estimates are fraught with uncertainty. For example, according to the NRC, the Brookhaven study's estimate overstates the scope of radiation release that is reasonable to consider, even in a worst case.[21] However, loss and probability assessments based on accidental occurrences, such as the estimate in that study, were not prepared with terrorist-instigated events in mind. The extreme circumstances of a full release and an impeded emergency response might indeed be relevant for a terrorist attack and could be useful in deciding how to prioritize security efforts.

Evidence of Potential Losses from Past Accidents

Some indication of potential losses comes from the Chernobyl and Three Mile Island accidents—events in which many unanticipated circumstances combined. Chernobyl in particular demonstrates the consequences of a broad dispersal of nuclear material and an impeded emergency response—although even in that case, conditions could have been worse. The fire and meltdown at Chernobyl resulted from a coincidence of design deficiencies (not present in U.S. reactors), workers' violations of standard procedures, and the lack of a "safety culture" in the responsible organizations.[22] The operators had bypassed or disconnected important safety systems, including emergency cooling and backup power, as part of an experiment to increase power output. After the fire started, the operators and the Soviet government did not give prompt warnings about the fire and the release of radioactive material. The fire, largely fueled by the graphite core of the reactor, spread radioactive substances across northern Europe. Because the power plant was built without a full concrete containment structure, the meltdown also allowed radioactive materials to burn down into the ground and contaminate groundwater. A concrete "sarcophagus" was subsequently built around the core to limit further contamination.

Some 50,000 square miles of land in Ukraine, Belarus, and Russia were contaminated to the extent that the health of local residents and the safety of agricultural

18. National Research Council, *Making the Nation Safer,* p. 43.

19. Sandia National Laboratories, *Technical Guidance for Siting Criteria Development*, NUREG/CR-2239, SAND81-1549 (November 1982).

20. Brookhaven National Laboratory, "Severe Accidents in Spent Fuel Pools in Support of Generic Safety Issue 82," BNL Report NUREG/CR-4982, 1997, published in *Science and Global Security* (Spring 2003).

21. The Nuclear Regulatory Commission's critique of that study is available at www.nrc.gov/reading-rm/doc-collections/fact-sheets/reducing-hazards-spent-fuel.html.

22. See summary of the *Proceedings of the International Conference on One Decade After Chernobyl: Summing up the Consequences of the Accident*, jointly sponsored by the European Commission, the International Atomic Energy Agency, and the World Health Organization in cooperation with the United Nations, held in Vienna, Austria, April 8-12, 1996, available at www.dcisc.org/chernobyl.html.

products were jeopardized.[23] According to the Congressional Research Service (CRS), studies indicate that at least 31 people died outright from radiation exposure and other injuries during the fire.[24] Since that time, about 1,000 cases of thyroid cancer in children have been reported in the region surrounding the reactor, or 100 times more cases than before the accident. (Thyroid cancer can result from exposure to radioactive iodine, which accumulates in the thyroid gland of growing children.) And workers involved in accident cleanup have experienced an increased death rate. Among the economic costs, the people of Chernobyl and nearby communities had to permanently relocate, and agricultural lands were permanently contaminated.

The incident at Three Mile Island was much less severe than the one at Chernobyl. The Three Mile Island accident was triggered when the main feed water pumps stopped, steam pressure began to build, and a safety valve designed to relieve that pressure stuck open, allowing coolant to flow out of the reactor core. The Pennsylvania power plant had a containment structure and was able to withstand a partial meltdown of the reactor core, although there had been fears of an explosion and breach of containment. Also, its reactor core was not constructed with graphite, which had made the Chernobyl fire so difficult to contain. In the end, some highly radioactive material did escape into the atmosphere before the reactor could be shut down.[25]

CRS points to studies indicating that even that brief public exposure may ultimately cause perhaps five deaths over the ensuing 30 years. At the time of the accident, nearly 150,000 people left their homes until the situation was stabilized. The Susquehanna River, along which the nuclear facility was located, flows past productive farmland surrounding Harrisburg and into the Chesapeake Bay. The Philadelphia, New York, and New Jersey population centers are immediately downwind.

Information on the costs of the Three Mile Island incident to the nuclear industry comes from court settlements, facility losses, and a changed investment environment. Expenses arising from claims and litigation to date total about $70 million, mainly for costs relating to the evacuation.[26] The courts also required that the plant operator finance a fund to pay for continued monitoring of local health. By far the biggest costs were from the loss of Three Mile Island's Unit 2, which had cost rate payers $700 million to build, and the approximately $1 billion spent to defuel the facility and decontaminate the grounds. In 1995, retirement costs for the destroyed unit were estimated to be $399 million for radiological decommissioning and $34 million for nonradiological removal.[27] The incident also precipitated a broad market reassessment of nuclear power: dozens of plants in planning or under construction at the time were canceled, at a direct cost to rate payers across the country, and no utilities in the United States have ordered new units since then.

Current Programs for Plant Safety, Control over Nuclear Materials, and Compensation for Losses

The Nuclear Regulatory Commission has principal authority for regulating civilian nuclear power and can balance incentives between producing power and ensuring safety and security. Concerns about the safe disposal of high-level radioactive wastes are being addressed (although not yet resolved) through programs of the Department of Energy (DOE), financed in part by industry contributions to the Nuclear Waste Fund. Separately, through the Price-Anderson Act, the federal government has acted to address the negative impact on industry of uncertainty about accidents, and DOE supports the industry by financing research and development of new production technologies.

23. For information on the city of Chernobyl and the broader exposed populations of Belarus, Ukraine, and Russia, see David R. Marples, "The Chernobyl Disaster: Its Effect on Belarus and Ukraine," in James K. Mitchell, ed., *The Long Road to Recovery: Community Responses to Industrial Disaster* (New York: United Nations University, 1996), available at www.unu.edu/unupress/unupbooks/uu21le/uu21le0h.htm.

24. Congressional Research Service, *Nuclear Energy Policy* (updated October 26, 2004).

25. For a chronology of events, see Nuclear Regulatory Commission, *Fact Sheet on the Accident at Three Mile Island* (March 2004), available at www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html.

26. See Nuclear Energy Institute, *Price-Anderson Act Provides Effective Nuclear Insurance at No Cost to the Public* (September 2003), available at www.nei.org/doc.asp?catnum=4&catid=319&docid=&format=print.

27. As reported by Eric Epstein in *Three Mile Island at Nineteen* (April 3, 1998), available at www.dep.state.pa.us/dep/pa_env-her/tmi/tmiepstein.htm.

Regulating the Safety of Nuclear Power Operations

The Nuclear Regulatory Commission is the principal federal agency tasked with regulating civilian use of nuclear materials.[28] It was established in 1974, when the Congress acted to separate the regulatory role of the Atomic Energy Commission from what many people viewed as that agency's role in advocating nuclear power. The NRC oversees the safety and security of nuclear reactors (including their construction, operation, and decommissioning), production and transportation of nuclear materials (including uranium oxide, uranium hexafluoride, and enriched uranium), storage and transportation of spent fuel, and disposal of high-level waste. (Under agreements with the NRC and subject to NRC minimum standards, the states may regulate low-level radioactive materials, including materials used by medical, research, and food irradiation facilities, as well as disposal sites for low-level wastes.)

Other federal agencies are involved as well. DOE is directly responsible for developing disposal sites for high-level wastes, and the Environmental Protection Agency (EPA) is responsible for developing environmental standards for such sites. However, the NRC licenses the construction and operation of disposal and storage sites. It coordinates its security program with the Department of Homeland Security (including the Federal Emergency Management Agency) and other federal agencies and with state and local emergency planners.

Through its licensing process, the NRC helps ensure the safety of nuclear power plants by requiring that they be built with important safeguards such as automatic shutdown mechanisms and backup electricity supplies. It also requires that operators regularly test nearby air and water for radiation leaks. The NRC has established rules governing preparations for various classes of threats and requiring that plants be secure against ground attacks and inside saboteurs. In addition to approving plants' security measures as a precondition to licensing, the NRC conducts security drills to test those defenses.

The NRC requires that emergency plans include preparations for evacuation or other actions to protect residents in the vicinity of nuclear plants in the event of a serious incident.[29] Each plant must have on-site and off-site emergency plans. For on-site planning and response, the NRC takes the lead in reviewing and assessing operators' plans. For off-site planning, the Federal Emergency Management Agency (FEMA) has the lead role in reviewing and assessing operators' emergency plans and in assisting state and local governments.

For planning purposes, the NRC defines two emergency planning zones (EPZs) around each nuclear power plant—one circling at a 10-mile radius and the other circling 50 miles. The 10-mile EPZ reflects the potential area in which people could be directly exposed to the airborne radioactive material released in a fire. The 50-mile EPZ is described as the area in which people could be exposed by the ingestion of contaminated food and water. The size and configuration of the zones may vary from plant to plant because of local emergency-response needs and capabilities, as determined by the number of people, the terrain, access routes, and local government boundaries. The emergency response within the 10-mile EPZ calls for providing emergency shelter or evacuation and using potassium iodide (a medication to reduce absorption of radioactive isotopes of iodine in children's thyroids). The response for the 50-mile EPZ calls for limiting access to the area and halting the distribution of potentially contaminated food and water.

Since the NRC was established, it has modified security-plan requirements for its licensed nuclear plants several times, partly in response to new information on the nature of threats.[30] Since 1977, plants have been required to add physical barriers that protect vital equipment and restrict access, upgrade alarm and electronic security systems, and maintain minimum numbers of armed guards. In 1993, plants had to specifically address the ground threat from a vehicle bomb by installing vehicle barriers. And in 2003, plants were required more generally to address the "largest reasonable threat against which a regulated private guard force should be expected to defend." On several occasions since the attacks of September 11, some states have ordered National Guard units to augment perimeter security at nuclear plants.

28. The NRC's regulatory authority is described on the agency's Web site, www.nrc.gov.

29. See Nuclear Regulatory Commission, *Fact Sheet on Emergency Planning and Preparedness at Nuclear Power Plants* (November 2004), available at www.nrc.gov/reading-rm/doc-collections/fact-sheets/emer-plan-prep-pwr-plants.html.

30. General Accounting Office, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (September 2003).

The Nuclear Waste Fund and Yucca Mountain

The safe disposal of spent nuclear fuel and other high-level wastes from nuclear power activities requires isolation of that material in perpetuity at secure sites distant from population centers and commercially valuable property.[31] As far back as 1957, the National Academy of Sciences suggested that the best way to protect the environment and public health and safety would be to store that waste in geologically stable rock formations deep underground. In 1982, the Nuclear Waste Policy Act established legislative authority to construct such a long-term disposal facility. And in 1987 amendments to that law, the Congress directed DOE to concentrate on the Yucca Mountain region—near Las Vegas, Nevada—as the only site to consider for waste disposal. Controversy continues to surround the Yucca Mountain site and the safety of transporting spent fuel to Nevada. Thus, despite support from the current Administration, completion of the storage facility is not certain.

Current DOE plans call for the site to accept its first shipments of waste in 2010. Given the planned capacity of the site (established in legislation) to hold 70,000 metric tons, it is likely that the amount of commercial spent fuel on hand by that date will exhaust the space allotted to it. (Electric utilities added about 10,000 metric tons in just four years to reach their 2002 on-site storage of 47,000 metric tons.) Even if the current plans are successful, a second repository—not yet planned and requiring additional decades to construct—would be needed to service continuing commercial generation.

Price-Anderson Indemnification and Liability Limits

The Price-Anderson Act, a 1957 amendment to the Atomic Energy Act of 1954, provides financial support for the nuclear power industry by creating an insurance pool with compensation limits that are greater than what would otherwise be available through commercial insurance. In addition, that law limits the total liability of an individual nuclear operator and of the industry. The law was also intended to help victims of a catastrophic nuclear accident by potentially making more resources available to settle claims than might otherwise exist and by simplifying the legal process of bringing claims against the industry. Without Price-Anderson, electric utilities would most likely have had difficulty raising the capital to build the nuclear power plants in operation today or perhaps even continuing operations at current levels.

The law requires nuclear plant operators (specifically, whoever holds an NRC license) to carry the maximum amount of commercial insurance that is available (currently $300 million).[32] But it also requires all operators to commit to providing additional resources (currently up to about $100 million per reactor, to be paid out over time) to help any one operator settle claims. That secondary insurance pool includes firms involved in nuclear fuel production, shipment, and storage, as well as DOE contractors who operate government nuclear facilities.

Contributions from Price-Anderson pool members would be available and legal proceedings would be restricted in the event of what the act calls an "extraordinary nuclear occurrence" (or ENO). An ENO is any event that causes a release of radioactive material beyond the plant site that the Nuclear Regulatory Commission (or DOE, for its contractor facilities) determines to be substantial and likely to result in substantial damages to people or property off-site.[33]

If the NRC makes a finding that a release constitutes an ENO, operators indemnified under the Price-Anderson Act waive certain legal defenses, relieving the claimant of having to prove a defendant's negligence and of having to disprove such defenses as contributory negligence. Claimants need only demonstrate personal injury or property damage, the value of that loss, and the causal link between their loss and the release of radioactive material. Claimants need not establish the fault of any party to prevail in their claims—the law essentially provides "no

31. See Congressional Research Service, *Civilian Nuclear Waste Disposal*, CRS Issue Brief IB92059 (updated August 31, 2004).

32. For further discussion of Price-Anderson, see Congressional Research Service, *Nuclear Energy Policy* (updated October 26, 2004); American Nuclear Society, *The Price-Anderson Act: Position Statement 54* (revised March 2003), available at www.ans.org/pi/ps/docs/ps54.pdf; and David S. Ziegler, *Report on the Price-Anderson Act and Its Potential Effects on Eureka County, Nevada* (prepared for the Board of Eureka County Commissioners, March 10, 2003), available at www.yuccamountain.org/price003.htm.

33. 42 U.S.C. 2014(j). A discussion of factors considered in making that determination and how they have changed appears in Nuclear Regulatory Commission, *Rulemaking Issue Notation Vote, Withdrawal of Proposed Rule and Denial of Petition for Rulemaking Submitted by the Public Citizen Litigation Group and the Critical Mass Energy Project (Wits No. W8100014)*, SECY-00-0160 (July 26, 2000), available at www.nrc.gov/reading-rm/doc-collections/commission/secys/2000/secy2000-0160/2000-0160scy.html.

fault" insurance. Under that law, the plant operator alone is liable for any damages. That feature is intended to simplify the process of making claims against the industry—plaintiffs can make all of their claims against just one defendant in just one court. Individuals affected by an ENO may make a personal-injury claim within three years of discovering an injury, such as cancer, regardless of how long it has been since the incident. However, those benefits depend on the NRC's declaring an ENO—which, for example, it did not do after the accident at Three Mile Island.

With 104 commercial nuclear reactors contributing about $100 million each to the industry insurance pool, the maximum liability of any single operator for any single incident today would be about $10.6 billion.[34] Presumably, parties harmed by a nuclear accident or attack also would be eligible for federal disaster relief, including any emergency funds that the Congress might elect to appropriate for losses that exceeded $10.6 billion. Commercial insurance is the primary insurance for power plants, and to date, no claims have been paid from the secondary Price-Anderson pool.

Further federal assistance could be available under two other laws. The first is the Robert T. Stafford Disaster Relief and Emergency Assistance Act, which would compensate state and local governments for up to 75 percent of their efforts to provide early assistance to victims of accidents that the President declared to be an emergency or major disaster.[35] The other is the Terrorism Risk Insurance Act of 2002 (TRIA). The TRIA program, which is scheduled to lapse at the end of 2005, is designed to reimburse insurers, including federally approved insurers such as those in the Price-Anderson indemnity program, for a significant portion of their terrorism claims.[36]

Ideas for New Approaches to Nuclear Power Security

Nuclear power plants may be relatively attractive as terrorist targets because of the potential for mass casualties and long-term environmental damage. Civilian reactor cores were not designed to protect against the type of attacks that are now of such concern. Moreover, spent nuclear fuel stored by electric power producers remains vulnerable unless the security of that on-site storage can be improved or the material can be safely moved to a secure central facility, such as the one being constructed at Yucca Mountain. Despite the many efforts by nuclear plants since September 11, emergency preparedness that would help to contain losses may not fully reflect the realities of the current terrorist threat. A range of options exists that could increase the nuclear industry's liability for the costs of preventing or paying for an attack, give the government greater responsibility for reducing those vulnerabilities and losses, and correct problems with incomplete information that could help improve decisionmaking about security.

Since September 11, all of the parties involved in the nuclear power industry have recognized a need to reassess security. On the regulatory front, an NRC official testified before the Congress in early 2003 that the agency has issued orders requiring "increases in security staffing, posts, and patrols [and] installation of substantial physical barriers."[37] The same testimony highlighted the NRC's efforts, in coordination with the Department of Homeland Security, to devise realistic attack scenarios and responses. It also cited ongoing studies of the vulnerability of reactor cores and on-site storage of spent materials to attacks by air.

Many of the options that the Congress might choose to implement would be likely to build on actions already under way or being examined. The Government Accountability Office has reviewed the many recommendations from commissions created by the Congress and has provided its own analyses of some specific concerns about nuclear security.[38] The National Research Council also has reported recommendations for addressing nuclear

34. The actual cost to the industry would be less than $10.6 billion in present-value terms because it would be paid out over time.

35. For a description of that program, see Federal Emergency Management Agency, *Response and Recovery*, at www.fema.gov/rrr/.

36. *Federal Register,* vol. 68, no. 40 (February 28, 2003), p. 9807.

37. Statement of Hubert Miller, Regional Administrator, Region I, Nuclear Regulatory Commission, before the Subcommittee on National Security, Emerging Threats, and International Relations of the House Committee on Government Affairs, March 10, 2003.

38. General Accounting Office, *Homeland Security: Selected Recommendations from Congressionally Chartered Commissions and GAO*, GAO-04-591 (March 2004), *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened,* and *Spent Nuclear Fuel: Options Exist to Further Enhance Security*, GAO-03-426 (July 2003).

and radiological threats and recently released a classified report related to the specific threat from spent fuel.[39] Richard Meserve, former Chairman of the Nuclear Regulatory Commission, has offered further suggestions.[40]

Homeland security is just one of several considerations that drive national policy on civilian nuclear power. Advocates of federal programs to support nuclear energy cite many positive attributes of nuclear power generation for the nation's energy supply and environment (such as an absence of emissions associated with global warming, acid rain, and ambient ozone, as well as the haze that can come from coal-fired generation). Policies that would have the effect of restricting nuclear power activities to promote increased security would need to be balanced with those other considerations.

Internalizing the Costs of Nuclear Security

Any accident or attack involving nuclear power presents risks to health and the environment well into the future, and the losses from a large release of radioactive material at a nuclear power plant would far exceed the value of the electricity such a facility would generate. In creating the NRC, the Congress recognized that low private costs mean the industry would have greater incentive to produce nuclear power and less incentive to invest in plant security than may be optimal for society as a whole. A number of options exist that could help address that continuing concern by internalizing the costs of potential attacks within the industry.

One approach would be to increase the share of the costs to nuclear power operators and investors in the case of a severe incident, or to make those costs more apparent to the neighbors of nuclear power plants. That would add private incentives to take security precautions or perhaps just to operate the number of nuclear power plants that would be most consistent with the relative benefits and costs of nuclear energy.

Other options more generally would mandate changes in industry practices to improve the security of power reactors and spent fuel against ground and air assaults. Those options include:

- Requiring utilities to increase the physical security of reactor cores against both ground and air assaults (for example, by employing security forces that could resist a more significant armed attack or by adding physical features that would better shield containment structures against attacks by heavy arms or by aircraft than is now the case).
- Requiring utilities to construct safer interim storage facilities for spent nuclear materials (for example, by increasing the physical security of storage areas or the use of dry-cask storage).
- Establishing requirements for safer transport casks or, alternatively, establishing safer transportation routes that nuclear fuel and spent fuel should follow. Safer routes might involve constructing new rail lines to avoid city centers.
- Establishing enhanced incentives and protections for reporting on unsafe practices and security breaches.

Concerning improved security against ground assaults, two months after the September 11 attacks, the NRC proposed that private guards at nuclear plants be permitted to use deadly force in a wider array of circumstances and be given better armament. (Federal law now precludes the use of automatic weapons by guards at civilian nuclear power plants.) It also proposed that federal authority supersede state laws that would otherwise restrict private guards from using deadly force or certain weapons.[41] Those proposals have not yet been acted on.

Other options that would have the effect of forcing industry to internalize the expected costs of a terrorist attack relate to changes in the Price-Anderson Act. Insurance coverage under that program may be too low because it does not consider a worst-case attack or attacks

39. Concerning radiological threats, see National Research Council, *Making the Nation Safer.* Concerning spent fuel, see background and meetings of the National Research Council, Board on Radioactive Waste Management, Committee on Safety and Security of Spent Nuclear Fuel Storage, available at dels.nas.edu/sfs/presentations.html.

40. Richard A. Meserve, "Nuclear Security: Challenges for Today and Tomorrow" (presentation at the conference "Future of Nuclear Energy in Wisconsin," Madison, Wisconsin, October 2003), available at www.engr.wisc.edu/ep/conference_papers/NuclrConf-Security5.pdf.

41. General Accounting Office, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Plants Needs to Be Strengthened*, pp. 20-21.

on multiple targets. Such considerations suggest options that include:

- Increasing insurance coverage to reflect the full costs of a nuclear disaster—for example, by raising the maximum liability per licensed reactor in the Price-Anderson pool or requiring plant operators to purchase (and commercial insurers to offer) additional coverage. There could be a requirement for individuals and businesses residing in emergency zones to carry their own nuclear incident coverage (and for commercial insurers to offer that coverage).

- Revising the Price-Anderson Act's indemnity so that more of any payout would come from the investors in those utilities rather than from the rate payers.

- Placing authority for determining an extraordinary nuclear occurrence—the prerequisite for activating the expedited judicial process under Price-Anderson—with the courts or some other agency or establishing explicit criteria in legislation for the Nuclear Regulatory Commission to determine an ENO. Such action could raise the industry's financial exposure and increase the likelihood of a payout from the Price-Anderson pool.

Socializing the Costs of Nuclear Security

Many nuclear security enhancements could instead be addressed by having the government take over or pay for those activities. Some options that would socialize the costs of nuclear attacks include:

- Establishing fiscal incentives for utilities to construct safer interim storage (for example, tax credits for spending on dry-cask storage or stronger structures for wet storage).

- Establishing fiscal incentives for studying and, if feasible, adopting inherently safer reactor designs and safer containment structures.

- Providing financial assistance to people and businesses to move away from nuclear sites.

If the federal government has a strong cost advantage over the private sector in performing certain security activities, federalizing those activities may be cost-effective. One activity that the government is already addressing is the disposal of high-level radioactive wastes through the development of the Yucca Mountain disposal site, funded in part by fees on utilities. However, completion of that site is not yet certain. The federal government may also have some advantages over private firms in directly providing physical security. For example, many people believe that the authority to use deadly force and to use certain high-powered weapons should reside with a government entity. Some options reflecting that position include:

- Federalizing and expanding the current level of perimeter security, structural defenses, and employee screening to help protect nuclear power plants and the spent material stored there.

- Constructing a secure, central disposal site for spent fuel, such as Yucca Mountain—and possibly expanding storage capacity beyond current plans to accommodate the additional wastes that are likely to accumulate in the next few years. The threat of terrorism increases the benefits of completing a central site to lower the risk of an attack on the spent fuel now stored at plants across the country.

- Subsidizing the construction of safer transport casks and safer transportation routes that the spent fuel should follow. The latter could involve subsidizing the construction of new rail lines to avoid city centers.

Since the attacks of September 11, the Congress has considered a number of measures that would create a federal force dedicated to securing nuclear plants or taking action if an attack occurred. For example, the Congressional Research Service notes that the proposed Nuclear Security Act of 2001 would have created a federal security force to replace the private security guards now in place at nuclear plants.[42] Another legislative proposal, the Nuclear Security Act of 2002, would have stopped short of replacing the security forces already guarding nuclear plants but would have augmented those forces with federal personnel and National Guard troops.[43] Among other things, that bill would have created new rules on security compliance at nuclear facilities and a program to classify, track, and monitor radioactive sources throughout the country. On the basis of information from the Nuclear Regulatory Commission, the Congressional

42. H.R. 3382, 107th Cong. (2001).

43. S.1746, 107th Cong. (2002).

Budget Office (CBO) estimated that implementing the Nuclear Security Act of 2002 would have had a gross cost of $486 million over the 2003-2007 period. However, the NRC has the authority to offset a substantial portion of its annual appropriation with fees charged to the facilities it regulates. Accounting for such collections, CBO estimated that implementation would have resulted in a net federal cost of $126 million over that period, assuming appropriation of the necessary amounts.[44]

Improving Information

If the owners of nuclear power plants underestimate the likelihood of a terrorist attack on their facilities or underestimate the loss—even their own direct loss—from such an incident, they may be inclined to operate more nuclear power plants or utilize more of their existing capacity than is consistent with homeland security. They may also not spend enough on safety at those plants. Similarly, many people will reside too close to a nuclear plant if they misgauge the risks and costs of an incident. The task of recognizing personal risk is especially difficult because many of the health effects of radiation exposure can be delayed for decades and because the effects vary among individuals. Contamination and exposure may continue for decades. Some policy options that could help improve information include:

- Providing better information to the public on the safety record of individual nuclear plants.
- Expanding NRC emergency zones to reflect worst-case events, tailored to individual plants.
- Preparing individual vulnerability assessments for localities that would reflect the danger from spent fuel as well as from the reactor core.
- Establishing national property zoning (like FEMA flood zones) to inform new-home purchasers and businesses of the zone designation.

44. See Congressional Budget Office, Cost Estimate for S. 1746, *Nuclear Security Act of 2002* (October 25, 2002).

CHAPTER

3

Chemicals and Hazardous Materials

The security of the chemical industry—which includes oil and gas production, processing, and transportation—was a concern before September 11, but after that date, the increased national threat of terrorism amplified the expected losses for individual chemical facilities and transport systems that many people already deemed vulnerable. No information suggests that the relative attractiveness of attacks on the chemical industry has increased, although September 11 did indicate that the scope of potential attacks is now larger. In addition, certain types of attacks, such as those using fuel oil and nitrates to fashion weapons for use elsewhere, may be more likely now than before.

Vulnerabilities from Processes, Transportation, and Misuse of Materials

Ensuring the security of the chemical industry is important primarily because of the special dangers that flammable and toxic substances can pose, including immediate explosion and fire, release into the air or water, or theft (and subsequent use in attacks elsewhere).[1] The major groups of chemical products include basic industrial chemicals, plastics and rubbers, drugs, detergents, paints, and agricultural chemicals. However, only a small subset of the many thousands of chemicals produced and consumed in the United States are of concern for homeland security.

Extremely Hazardous Chemicals

The Environmental Protection Agency—the primary federal agency tasked with protecting the public and the environment from chemical accidents—lists more than 300 chemicals as "extremely hazardous."[2] Focusing on those chemicals that could harm people after exposure for only a short time, the agency closely monitors chemical facilities with the capacity to process amounts in excess of threshold quantities from a list of 77 acutely toxic chemicals and 63 flammable gases and liquids.[3] Even on that shorter list, just 13 substances or mixtures account for more than 90 percent of the total mass (by weight) of hazardous materials.

The most hazardous chemical substances come largely from three segments of the industry:

- Petrochemicals (organic industrial chemicals),
- Nitrates (agricultural chemicals), and
- Ammonia and chlorine (inorganic industrial chemicals).

Petrochemicals—such as fuels, solvents, and raw materials to make plastics—are of concern not only because

1. Linda-Jo Schierow, *Chemical Plant Security*, CRS Report for Congress RL31530 (Congressional Research Service, updated October 22, 2004).

2. That list is compiled as part of section 302 of the Emergency Planning and Community Right-to-Know Act. Information on the complete list and descriptions of chemicals described as extremely hazardous are available at yosemite.epa.gov/oswer/ceppoweb.nsf/content/ehs_2003.htm?openDocument.

3. See James C. Belke, "Chemical Accident Risks in U.S. Industry—A Preliminary Analysis of Accident Risk Data from U.S. Hazardous Chemical Facilities," *Proceedings of the 10th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Stockholm, Sweden* (Amsterdam: Elsevier Science, 2001), copy available at www.epa.gov/swercepp/pubs/stockholm-paper.pdf. Threshold quantities for toxic substances range from 500 pounds to 20,000 pounds. For all listed flammable substances, the threshold quantity is 10,000 pounds. For explosive substances, the threshold quantity is 5,000 pounds. See Environmental Protection Agency, *List of Regulated Substances and Thresholds for Accidental Release Prevention,* 40 C.F.R. 9, available at www.epa.gov/swercepp/rules/listrule.html.

they are highly flammable but also because they are found at very large and complex facilities, often in close proximity to one another. Thus, the immediate dangers from an attack and the resulting economic disruption would be greater than otherwise. In sufficient concentrations, the atmospheric release of many of those substances (by fire or spills) could also be immediately toxic or, over time, be associated with cancer and other health problems or with environmental damage.

Nitrates, produced from ammonia or urea, include a variety of nitrogen-based compounds used to make fertilizers, pesticides, and explosives, and they are highly flammable. Nitrate-fertilizer plants themselves could be targets for attack, but the fertilizers stored at thousands of warehouses across the country (accounting for the largest number of sites that EPA monitors) are perhaps of greater concern for homeland security, primarily because of the difficulty in securing fertilizers against misuse. The sale of ammonium nitrate fertilizer is legal. However, retail outlets could be vulnerable as targets for diversion of fertilizers by terrorists, and weakly guarded storage facilities could be targets for theft. Ammonium nitrate combined with diesel oil was used as the explosive in the World Trade Center bombing in 1993 and the Oklahoma City bombing in 1995.

Some toxic substances—especially ammonia and chlorine—are a homeland security concern in large part because of their preponderance and, hence, their accessibility. They can be very poisonous if released into the air or water in high concentrations. Ammonia is present in one-third of the facilities handling at least threshold volumes of hazardous material and in more than half of the facilities handling toxic substances. (At those facilities, the volume of anhydrous ammonia is of greatest concern; the threat from aqueous ammonia, which is common in household cleaners, is much less significant.) The major use of ammonia and its compounds is as fertilizers. Relatively smaller amounts of ammonia solutions also are present in thousands of cold-storage facilities, where they are used as refrigeration coolants. Other uses include cleaning; making soap; bleaching (and processing paper); etching aluminum products; and manufacturing other chemicals, drugs, and plastics.

Chlorine, too, is widely present. It is used in purifying water in communities across the country as well as in producing vinyl plastics and making many medicines. Concern over chlorine stems from both its storage at facilities and its transportation in rail tank cars. A related concern is the flammability of hydrogen, a byproduct in the extraction of chlorine from salt water.

Monitoring Facilities Through EPA's Risk Management Program

Concerns about hazardous chemicals—whether flammable or toxic—relate to both the suppliers and the users of those chemicals, including those who transport and store such materials. On the basis of data provided by businesses to EPA's Risk Management Program, EPA reported in 2000 that nearly 15,000 facilities were handling at least one hazardous substance in a quantity greater than threshold limits. Those facilities themselves represent a subset of a much larger number of businesses handling a "significant" quantity.

EPA's Risk Management Program monitors large chemical producers, including petroleum refiners, petrochemical manufacturers, and nitrate-fertilizer manufacturers. It also monitors many small facilities involved with fertilizer storage, refrigerated storage, and water treatment. The greatest number of chemical processes that EPA tracks involve just two toxic substances: ammonia and chlorine. Relatively few chemical processes, other than production of nitrate fertilizers, involve flammable substances. However, because the facilities that handle many flammable substances—petroleum refineries, petrochemical plants, natural gas plants, wholesale-fuel terminals, and propane distribution centers—have such large capacities, the greatest volume of hazardous chemicals that EPA regulates are flammable.

In addition to the facilities monitored by the Risk Management Program, numerous facilities with smaller quantities of such chemicals can raise homeland security concerns. In particular, the 15,000 facilities in the program exclude retail outlets for flammable chemicals used as fuel, such as gasoline stations and retail propane distributors, which are not required to report to EPA. The many smaller suppliers, transporters, and consumers of those chemicals may hold sufficient quantities of dangerous materials to cause harm if the materials were released or set on fire. They may also have the information or equipment necessary to make more-dangerous substances. Further, because those smaller potential targets are especially dispersed and potentially more difficult to defend, they may be attractive as terrorist targets.

Potential Losses from Explosions and Toxic Releases

Indications of the possible costs of an attack on chemical facilities come from several sources, including assessments of accidental-release scenarios prepared for EPA; assessments of attack scenarios that the Department of Homeland Security (DHS) has recently been preparing on its own; and information about the human, environmental, and economic losses from previous major accidents involving chemicals. As distinct from the immediate economic costs to targeted facilities (and, possibly, associated businesses and nearby communities), economic costs to the nation as a whole from an attack would derive mainly from any disruption of current supply to the businesses and consumers that purchase the output of the targeted facilities and from any loss of productive facilities (and future supply).

EPA's Accidental Release Scenarios

Chemical-facility operators covered by EPA's Risk Management Program must submit analyses, referred to as offsite consequence analyses, of the possible consequences of hypothetical worst-case release and alternative-release scenarios for the most hazardous substance present. (Those analyses are separate from the five-year histories of accidents that those businesses must also report.) Although the scenarios are intended as a source of information on potential accidents, they also can provide insights into the numbers of people potentially at risk from an attack on those facilities.

In the "worst-case release" scenarios, operators describe the maximum quantities of release from the rupture of the single largest vessel or process line at the facility and the maximum range (or end-point distance) that a toxic cloud or a blast could reach. (The end-point is the distance a toxic vapor cloud, heat from a fire, or blast wave from an explosion could travel before dissipating to the point that serious injuries from short-term exposures would no longer occur.) The analyses also include information on the number of people or sensitive sites that such a release could harm. The results reflect the population present in the full circle around the chemical facility—not necessarily the number that would be harmed—and are intended only to show the consequences of worst-case atmospheric conditions with no measures taken to prevent or mitigate a release.

In contrast, EPA's "alternative-release" scenarios describe the consequences of incidents that may be more representative of actual emergencies. In particular, toxic clouds are assumed to disperse farther, but only in the direction of the prevailing winds, and any losses would be mitigated by early-warning systems and emergency response. For that reason, EPA recommends that communities make use of alternative-release-scenario assessments in their emergency planning for chemical accidents.

When considering a terrorist attack, it may not be reasonable to assume the presence of mitigating circumstances. For example, emergency vehicles may not be able to reach the release site. Or the attack may be timed so that the wind is blowing in the worst possible direction. Therefore, reviewing the worst-case release data is also useful.

EPA's worst-case release data indicate that, in general, the distances and thus the populations that could be threatened are greater for toxic substances than for flammable substances.[4] Measured as end-point distances from the facility, releases of toxic substances in those worst-case scenarios encompass 1.6 miles—the median distance for all facilities reporting. For facilities handling flammable substances, the median distance affected by a vapor-cloud explosion would be 0.4 miles. Similarly, the median population size that those releases would affect are 1,500 people for toxic substances and 15 for vapor-cloud explosions involving flammable substances.

Those statistics, however, mask far greater dispersions for a significant number of facilities. Models of atmospheric dispersion indicate that the chlorine stored by many facilities in 90-ton rail tank cars can spread as far as 14 miles in urban settings and 25 miles in rural settings. Models provide similar estimates for the dispersion of large quantities of several other toxic chemicals.

Concerning the populations at risk, about 8,000 facilities that handle toxic substances reported worst-case release scenarios that each could endanger at least 1,000 people. Those figures do not represent deaths or injuries but

4. Data on Environmental Protection Agency release scenarios come from Paul R. Kleindorfer and others, "Accident Epidemiology and the U.S. Chemical Industry: Accident History and Worst-Case Data from RMP* Info," *Risk Analysis*, vol. 23, no. 5 (2003), pp. 865-881, available at opim.wharton.upenn.edu/risk/downloads/03-24-PK.pdf; and from conversations with James C. Belke of EPA.

rather the numbers residing within a circle that encompasses the facilities' worst-case end-point distance. With the short end-point distances for explosions of flammable substances, relatively few people would be endangered by such events, even at the largest chemical facilities in the country. Nearly 300 of those large facilities reported worst-case release scenarios involving flammable substances that could affect more than 1,000 people, and none could endanger more than 100,000.

Department of Homeland Security's Release Scenarios

To help identify the facilities most at risk and to prioritize security efforts, the Department of Homeland Security has been working with the EPA model to prepare its own assessments of likely attack scenarios and consequences.[5] The chemical releases addressed in DHS's scenarios generally pose a greater danger than those in EPA's worst-case release because all chemicals at each facility are assumed to be at risk. However, as with EPA's alternative-release scenarios, DHS assumes that the plume of release only blows in one direction and that an emergency response is able to further mitigate the losses. On net, the number of people at risk is generally lower in those DHS scenarios than in an EPA worst-case release, but the threat to them is likely to be greater. Such an assessment can be of value in determining how to prioritize security efforts—in contrast with the EPA program's purpose, which is to understand and prevent accidents. DHS reports that only about 3,700 plants (handling either toxic or flammable substances or both) would threaten more than 1,000 people.[6] And only two plants would endanger more than a million people.

Evidence of Potential Losses from Past Accidents

Further indication of the potential human and environmental losses and economic costs from an attack on a large chemical facility comes from major accidents that have occurred both abroad and in the United States. Those events indicate that the human and environmental losses could be significant.

The most notable example of a chemical accident that caused widespread losses is the 1984 accidental release of a fatal pesticide ingredient in Bhopal, India. By some estimates, that accident killed nearly 4,000 people outright. India's courts ordered the Union Carbide Corporation, which owned the facility, to pay $470 million in compensation to more than 566,000 survivors and dependents, including thousands of victims who were permanently disabled.[7] Bhopal involved the release of a single substance from a single vessel but under the worst atmospheric conditions and with no emergency response—much as in an EPA worst-case scenario—and was compounded by inadequate building standards and no effective zoning to limit residential housing around the plant. The greatest loss of life in the United States from a chemical accident came from the 1947 explosion of a fertilizer-laden ship in Texas City, Texas, which spread fire to nearby ships and to industrial facilities onshore and claimed about 600 lives.[8] Because it involved multiple substances, the explosion was more akin to the DHS attack scenarios.

In both of those cases, the chemicals involved were widely available, so the costs of those accidents to the private sector were largely confined to the value of the facilities and product that were lost and, in the Bhopal case, the subsequent court judgment against Union Carbide.

Recent experience with chemical accidents in the United States is much less extreme. Many of the accidents have involved freight derailments, tanker spills, pipeline leaks, or fires at major production facilities. The nation appears to be particularly vulnerable in the transportation stage, as hazardous materials move by truck and rail through population centers, although the history of chemical accidents includes very few events with a loss of life beyond a facility site.

The Exxon Valdez oil spill of 1989 is an example of such transportation risks. As with Bhopal, it appears that the immediate economic costs of that spill to the Exxon Corporation were less than the associated human and envi-

5. The Department of Homeland Security has not released those assessments in any public documents. A discussion of its methodology and some results—numbers of facilities that may be associated with harm to critical levels of population if attacked—appear in Robert Block, "Chemical Plants Still Have Few Terror Controls," *Wall Street Journal,* August 20, 2004, p. B1.

6. Estimate from telephone conversation with staff of the Department of Homeland Security.

7. For a recent discussion, see Harbaksh Singh Nanda, "Bhopal Gas Leak Award 20 Years Later," *United Press International,* July 21, 2004, available at washingtontimes.com/upi-breaking/20040721-104226-4298r.htm.

8. For a description of the accident, see "The Texas City Disaster, April 16 and 17, 1947," available at www.ezl.com/~fireball/Disaster20.htm.

ronmental losses, although the company subsequently was held liable for much of the broader loss to society. The net economic costs to the oil industry were probably small. When the Exxon Valdez ran aground, the value of the 240,000 barrels of crude oil spilled (a measure of the immediate economic harm) was only about $25 million. In addition, there was the lost value of the tanker. On top of those immediate costs, Exxon incurred further private costs to compensate for the damage that it caused. The company reportedly paid more than $2 billion for cleanup activities, as well as about $1 billion in criminal restitution and civil penalties—much of which went to pay for further cleanup, restoration, and compensation (largely through purchasing land that would be permanently protected as wildlife habitat, parks, and refuges).[9]

Economic Costs to the Nation Versus Immediate Costs to the Owner

In previous major accidents involving chemicals, it appears that the economic costs to the whole nation in question were even smaller than the immediate costs to the owners from the loss of production facilities and sales. The national cost derives only from any resulting disruption of current supply to the businesses and consumers purchasing the output of the targeted facilities and from any loss of productive facilities (and future supply).

For that reason, measures of the aggregate value of chemical sales greatly overstate the potential for losses to the economy. For example, the 1997 Economic Census, which uses the same industry categories that EPA uses for its Risk Management Program data, indicated total sales of more than $540 billion for all of the industries that used any of the regulated chemical processes. However, many of the establishments counted in that census do not maintain the chemicals of concern for homeland security. Also, the cost figures for any one establishment probably overstate the potential loss from attack because replacement supplies would be available from spare capacity throughout the industry, including supplies from inventory and imports. In some cases, altogether different chemicals and production processes could be substituted. The future cost to industry from a chemical attack would reflect only the increased cost of supplying those replacements or substitutes. (Considering the Exxon Valdez example, all of the lost oil was replaced from other sources, with only an imperceptible increase in world oil prices.)

In general, any increase in industry costs attributable to terrorist attacks is likely to be small, primarily because the chemical industry has already adapted to the prospect of disruptions from accidents, and terrorist incidents are likely to fall in the realm of its experience and planning. The same may not be true for the social costs. For a toxic release that spreads over a significant area, the social cost itself may expand to include the disruption of activity by local business and local populations not otherwise involved with chemicals. Also, there is no way to gauge the full economic consequences of an attack that involves a theft of toxic or flammable chemicals.

A further example in which the social costs may exceed the private costs involves the disruption of supplies of critical chemicals for which few alternative sources exist—such as chemicals that are key industrial ingredients or that have important medical uses. There may be only one or a few manufacturers of a number of medicines, such as vaccines. Without stockpiles of those items, a supply disruption could prove harmful.

Current Programs for Safety and Emergency Preparedness

Federal, state, and local programs already exist that—with varying degrees of effectiveness—encourage or require the operators of chemical facilities to boost their efforts to promote safety and security and to share information that can help local governments plan for emergencies.[10] Much of the overall government effort for chemical safety occurs at the state and local level and is oriented toward emergency preparedness. The federal effort includes worker-safety, environmental, and information programs that are intended to support local activities.

The Emergency Planning and Community Right-to-Know Act of 1986, passed largely in response to the Bhopal accident, represented the first federal initiative to promote safety specifically in chemical facilities. The law required operators of chemical facilities to participate in

9. For a summary of the settlement, see Environmental Protection Agency, "Exxon to Pay Record One Billion Dollars in Criminal Fines and Civil Damages in Connection with Alaskan Oil Spill" (press release, March 13, 1991), available at www.epa.gov/history/topics/valdez/02.htm. Additional background is available at www.newsaic.com/casecivil.html#exxon.

10. A discussion of the basic laws appears in Schierow, *Chemical Plant Security.*

community emergency planning to address the possibility of an accident, provide information to local planners on the chemicals they handle, and notify local officials of any sudden release. It also mandated the establishment of state and local commissions to coordinate planning and response for large releases of specified hazardous substances and required that local officials inform the general public about chemical hazards and emergency plans for them.

Additional requirements came in the Clean Air Act Amendments of 1990. The CAAA mandated a role for the Environmental Protection Agency in overseeing risk-management planning at facilities that handle threshold quantities of certain hazardous chemicals identified in the law and others to be identified by EPA. Operators are required to have programs for detecting, preventing, and minimizing the consequences of accidental releases of those chemicals. The CAAA also required the preparation of risk-management plans and offsite consequence analyses (for worst-case accidents).

Further federal support for chemical security comes from assistance grants to local governments for first-responder programs and from technical support and training programs, such as those of the Federal Emergency Management Agency. Among recent legislation, the Maritime Transportation Security Act of 2002 requires the preparation of vulnerability assessments for chemical facilities along the nation's waterways, and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 authorizes the creation of medical stockpiles to prepare for biological attacks.

Ideas for New Approaches to Chemical and Hazardous-Material Security

The gap between the private and social benefits of improved security for chemical facilities and transport is likely to be as large as for any of the critical industries considered in the aftermath of September 11. Although precise estimates are not available, information on accidents in the chemical industry, company assessments of what could happen in a severe release or explosion, and actual terrorist incidents involving chemicals suggest that the risk of attack is real and that losses could be significant. Any losses for society at large would probably be much more extensive than the immediate damage to the chemical facility that was targeted or whose chemicals were diverted as a weapon against others. Ideas for new approaches that would internalize the expected cost of an attack to chemical producers, socialize the cost of improved security, and address problems with incomplete information all deserve attention. In some cases, the intended change in behavior could be accomplished by more than one type of policy.

Internalizing the Costs of an Attack on the Chemical Industry

More-stringent regulations and enhanced enforcement of safe practices are options that would internalize the expected cost of a terrorist attack that used a chemical facility or chemicals in transit as a weapon to inflict mass casualties. Specifically, those options could include:

- Establishing fees or taxes on sales of certain hazardous chemicals to discourage their use.
- Establishing new regulations for tracking the ownership of hazardous chemicals that could be used as weapons.
- Establishing new regulations governing the safe transport of hazardous chemicals to route them away from population centers.
- Creating financial disincentives for businesses or residents to locate in danger zones (for example, by requiring higher insurance coverage or disallowing business tax incentives).
- Establishing enhanced incentives and protections for reporting on unsafe practices, conflicts with best-technology safety practices, or other sources of vulnerabilities.

Businesses may not face the full costs of damages from an attack because the full financial resources of the parent firm are not at stake or because the required limits for private insurance coverage are too low. Raising the stakes would increase private incentives to make chemicals and chemical production safer and could be accomplished by:

- Supporting industry efforts to pool financial resources to settle claims against any single business in the industry;
- Requiring chemical plants to purchase higher minimum coverage levels, regardless of cost; and

- Requiring private insurers to offer higher coverage levels.

The Congress has considered a number of measures that would cause the chemical industry to assume increased costs of security. For example, the Chemical Facilities Security Act of 2003 (S. 994) would have required DHS to develop regulations designed to increase security at facilities vulnerable to unauthorized releases of hazardous chemicals, in part by requiring owners and operators of those facilities to perform vulnerability assessments and to establish site security plans. (Although the Congressional Budget Office did not estimate the direct cost to industry of those measures, it estimated that the federal cost of implementing S. 994 would be $216 million over the first five years, assuming necessary appropriations.[11] Of that amount, DHS would use $126 million to develop the required regulations, maintain chemical facilities' site information, and enforce the bill's new requirements.)

Socializing the Costs of Improved Chemical Industry Security

The government may have a cost advantage in performing certain security services that are necessary to reduce the expected social costs of a terrorist attack on a chemical plant. For example, the government could directly provide for the perimeter security of chemical plants, as the Coast Guard already does to some extent for facilities located along navigable waterways.

Among the provisions of S. 994 were federal grants to improve security at agricultural businesses that produce or sell hazardous chemicals (such as fertilizer), which CBO estimated to have a federal cost of $90 million over five years.[12]

Other ways to spread the costs of improved security could include subsidizing the cost of private insurance or providing government insurance. Such insurance programs on their own might help pay for the damages from an attack, but they would not necessarily cause the industry to make actual security improvements unless the financial resources of the business or insurance underwriter were at stake as well. Only then would the insurer have an incentive to induce industry to improve its safety—for example, by making coverage or premiums contingent on specified safe practices.

Government funding for security improvements also could subsidize the sale of safer chemicals, subsidize expenditures on safer production materials and processes and safer transport methods, and provide assistance for people and businesses that wanted to move away from dangerous sites.

Improving Information

The general public, local emergency planners, and perhaps even the chemical industry lack a wide range of information about the potential scope of damages from a terrorist attack. To the extent that the potential cost is underestimated, spending to counter those damages will be too low. Another area in which information could be improved involves alternative technologies. Alternative chemicals or chemical processes may exist that would be inherently safer in some applications, but information on them is not widespread.

There are also dilemmas concerning information about all of the critical industries. One dilemma is how to balance the need for good information on potential vulnerability with the need to keep that information from people who could exploit it to launch a more effective attack. Another problem is how to disentangle industry's normal disincentive to make business information public from legitimate security concerns about disclosure. The Congress restricted access to offsite consequence analyses before September 11, and more recently, concerns about security prompted DHS to protect security-related data submitted voluntarily by critical-infrastructure companies from disclosure under the Freedom of Information Act. Problems related to incomplete information suggest several types of options to help boost security, including:

- Establishing emergency planning zones that reflect release scenarios consistent with the potential scope of a terrorist attack. (That measure could indicate more-extreme damages than in EPA's alternative-release scenarios, now used by many communities in emergency planning.)

- Better informing the public on where dangerous chemicals are, either by regulation or through public/private partnerships to disseminate information.

11. See Congressional Budget Office, Cost Estimate for S.994, *Chemical Facilities Security Act of 2003* (May 10, 2004).

12. Ibid.

- Establishing national property zoning (similar to FEMA's flood-zone mapping) to help inform new purchasers about local dangers; setting national restrictions on what activities can occur near dangerous chemicals (in particular, other critical industries); and dictating safe routes for transporting dangerous chemicals. (All of those responsibilities now lie with local governments.)
- Disseminating information to businesses on inherently safer chemicals and safer production processes (through public reports, demonstration projects, incentives such as research and development grants, and public/private partnerships such as EPA's product-labeling programs and information-sharing coalitions).

CHAPTER

4

Electricity Service

Electricity service is one element of critical infrastructure for which the post-September 11 benefits of improving security may not be very different from the pre-September 11 benefits. In general, the vulnerabilities that the nation's electricity supply currently face from terrorism are similar to those that the industry has long faced from extreme weather and other natural events, accidents, and equipment failures—occurrences that could disable any of the major physical components of the supply network or disrupt performance of the system's control centers. Potential losses from such disruptions would be limited and of relatively short duration because the industry and electricity customers are generally well prepared for such failures. However, greater losses could occur if attacks on key facilities were coordinated with the intent of causing a widespread and prolonged system failure. Concerns about terrorist attacks may give added impetus to proposals already under way to improve the reliability of power supplies.

Other concerns related to electricity service are the security of nuclear power facilities (discussed in Chapter 2) and the security of the nation's large dams and reservoirs. Many of the largest dams support hydropower production, although the vast majority serve other purposes. The Department of Homeland Security identifies large dams as critical infrastructure because of the potential downstream harm that the breaching of such a dam could cause (see Box 4-1). This paper does not explore options for improving the safety of dams.

Vulnerabilities from Disruption of Regional Transmission

The major vulnerabilities of electricity supplies are associated with regional transmission systems—the power grids that carry electricity at high voltage from power sources to communities. Transmission systems include the substations and high-voltage transformers that first "step up" the force of the current as it moves from generators onto the transmission lines and then "step down" that current as it moves onto the low-voltage lines necessary for local distribution. Generation facilities—other than nuclear power plants and hydropower dams, which present a different type of concern—are generally not a major source of vulnerability to electricity supplies because there are so many generators and so much excess generation capacity. Similarly, although highly exposed to attack, the distribution systems for carrying electricity at low voltage over the last few miles directly to homes and businesses would not make a good target, as a break in those lines would probably be well within the range of the industry's experience and capacity for making speedy repairs.

Assaults on Individual Components

Experiences with major outages involving bulk power (that is, generation and transmission) suggest ways in which a targeted attack on those systems could lead to widespread outages. Of particular concern for supply disruptions are assaults on selected individual components—or combinations of components—that could take advantage of system safeguards to produce a cascading sequence of failures and widespread service disruptions. For example, assaults on transmission lines at multiple points or at key nodes could cause failures that operators in control centers could not adjust to quickly; cyber attacks on the control centers themselves could also wreak havoc. But in general, such attacks would result in losses only for short periods.

A principal concern about supply losses for a longer period relates to attacks on the high-voltage transformers where the force of the current is stepped down from regional transmission lines to local distribution lines. The sudden loss of multiple substations could precipitate an imbalance between the amount of power being pushed

Box 4-1.

Vulnerabilities, Potential Losses, and Regulatory Regimes for Large Dams and Reservoirs

Compared with chemical facilities or nuclear plants, the largest dams are inherently secure structures by virtue of their massive design. Yet if a large dam upstream from a major population center was breached, large-scale loss of life and major economic damage could result. Dams are continuously vulnerable to extremes in weather, earthquakes, and failures because of age and inadequate maintenance. And with the increased threat of attacks since September 11, some preventive actions that may not have been cost-effective in the face of only natural events now may be worth undertaking.

The actual vulnerability of any dam to a terrorist attack that could release large volumes of water would depend on the uses of the dam, its basic design, and possibly its state of repair. Of greatest concern are those dams that are sited and designed to achieve maximum water storage—whether for recreation, flood control, or hydropower production. Among the different designs, earthen and rock-fill dams may be the most vulnerable to a concerted, small-scale effort to exploit weak spots. The two most notable dam failures in U.S. history—the Johnstown Flood of 1889 and the Teton Dam collapse of 1976—involved earthen structures. Age is a big concern because most federally constructed dams were completed by the mid-1900s, and two-thirds of the nonfederal dams that are licensed by the Federal Energy Regulatory Commission (FERC) are more than 50 years old.[1]

Historical experience with accidents gives some indication of the human losses that could result from an intentional breach of a dam. Total failures are very rare, but they have occurred with disastrous results. After Pearl Harbor and September 11, the event that caused the single greatest loss of life in this country was the Johnstown Flood of 1889, in which more than 2,200 people died. The failure of the newly built Teton Dam in Idaho in 1976 resulted in 11 deaths, 20,000 households evacuated, and perhaps $800 million in damages (beyond the cost of the dam itself).

Economic losses from flooding would come from damage to downstream properties and to the dam itself, reflecting the lost value of any services the structure had been providing (including power generation, municipal water, irrigation water, and recreation). Not all consequences need be negative; in fact, some environmental advocates would point to gains for some flora and fauna by letting rivers run free.

Recognition of private and public disincentives to build and operate dams in a way that provides the most cost-effective level of protection for downstream communities has led state governments and federal agencies to extensively regulate nonfederal dams. The security of federal dams, which include many of the nation's largest hydropower projects, is the responsibility of the federal agencies that build and operate them.

1. General Accounting Office, *Federal Power: Implications of Reduced Maintenance and Repairs of Federal Hydropower Plants*, GAO/RCED-99-63 (March 1999).

onto the wires from generation and the amount being pulled off for consumption (known as system load), which could threaten the regional grid as well as sever electricity to the targeted community.[1] (Power could be rerouted to compensate for the loss of only one or a few substations, depending on the load balance in the affected region.) Unlike with other equipment problems—such as damaged towers and downed lines—the industry does not have experience with emergency losses and subsequent replacement of multiple transformers. High-

1. The consequences of an attack on multiple substations are discussed in U.S. Congress, Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453 (June 1990), available at www.wws.princeton.edu/cgibin/byteserv.prl/~ota/disk2/1990/9034/9034.PDF.

Box 4-1.

Continued

The vast majority of the country's dams are small nonfederal structures that are not used to generate hydropower. They are regulated by the states and local governments, although the Federal Emergency Management Agency (FEMA) has an interest in those dams, too.[2] The National Dam Safety Program Act, passed in 1996, increased FEMA's authority to provide financial assistance to the states for strengthening their own dam safety programs. FEMA works with the states to promote dam safety legislation, establish emergency action planning for dams that present potential hazards, inspect dams regularly, and track dams in need of remediation. With federal assistance, the states reportedly inspected 14,000 dams in 2002.[3]

The Federal Energy Regulatory Commission regulates the construction, operation, and maintenance of nonfederal dams that are built for hydropower generation. In addition, most projects that affect navigable waters, occupy federal lands, or use water power from a government dam require a FERC license to operate. The commission is currently responsible for dam safety at more than 2,600 licensed and exempted dams and related water retention structures. FERC requires all operators to develop emergency action plans that indicate how to protect people and property in the event of a natural disaster or sabotage and how to quickly restore power.[4] In addition, for all larger projects, operators must provide a security plan that identifies protective measures and evaluates on-site security systems, as well as a vulnerability assessment that identifies vulnerable project features, threats, the consequences of an attack, and the likely effectiveness of security systems to counter an attack.

The security of federal dams is the direct responsibility of agencies such as the Bureau of Reclamation and the Corps of Engineers, which own and operate the largest federal dams and associated power-generating facilities. The Tennessee Valley Authority also owns the dams in its hydropower systems and sells that power. Some smaller dams are owned by the Bureau of Land Management, the Forest Service, and several other agencies. All of those federal operators are subject to federal guidelines on dam safety, although the guidelines do not establish technical standards that the agencies must meet. As the designated coordinator of the National Dam Safety Program, FEMA also monitors the progress of federal dam operators in implementing the federal guidelines for dam safety.

2. Information on state regulators is available from the Association of State Dam Safety Officials, an organization of state and federal regulators, dam operators, and others interested in dam safety, at www.damsafety.org.

3. See Federal Emergency Management Agency, *FEMA 466, Dam Safety and Security in the United States: A Progress Report on the National Dam Safety Program in Fiscal Years 2002 and 2003,* available at www.fema.gov/fima/damsafe.

4. See Federal Energy Regulatory Commission, *FERC Security Program for Hydropower Projects, Revision 1* (November 15, 2002), available at www.ferc.gov/industries/hydropower/safety/security/securitytext.pdf.

voltage transformers can take months to replace because relatively few are held in inventory, they generally are custom-made to reflect the load requirements of individual utilities, and they are very large (on the order of 400,000 pounds) and difficult to transport.[2]

Information on the number of generation- and transmission-related service losses gives some indication of the vulnerability of electricity supplies. The North American Electric Reliability Council (NERC) lists more than 500

2. For example, see news releases by APS, the investor-owned utility serving Phoenix: "APS Acquires Replacement Transformer from BPA," July 10, 2004, and "APS Brings Replacement Transformer into Service," August 9, 2004, available at www.aps.com/general_info/newsrelease/default.html?year=2004.

such outages in the period from 1984 to 2000.[3] Nearly three per year involved losses of at least 1,000 megawatts (comparable to the supply from any of the country's largest generation plants). And 19 from that list involved disruptions for more than 1 million customers (households and businesses). Of the 58 bulk power outages in 2000 alone, about half were attributable to natural events (26 to weather and two to wildfires). The rest were caused by human error and equipment failure (24) or by a contractual failure to provide enough supply to meet demand (six). Most of those outages were brief and affected relatively few people, with notable exceptions. A 1998 ice storm in southern Canada and New York left 1.6 million people without power for up to a month. The outage of August 2003, the largest to date, blacked out power for a day or more to perhaps 50 million people in the upper Midwest, eastern Canada, New York, and New England.

The Problem of Systemwide Failure

In the history of bulk power outages, single-component failures are the most common, but many of the largest outages—including the August 2003 blackout—involved cascading failures. In a cascading failure, problems with a key transmission link cause power to be rerouted over adjacent lines, which then become overloaded and automatically shut down. The effects cascade from the initial point of disturbance onto other lines and generators, successively tripping more protective devices and knocking out power over a broader area.

Two factors are at play in the inherent vulnerability of regional grids to cascading failures. One is the physical requirement that the amount of power going into the grid (from local generation or from neighboring grids) match the power that consumers are taking off the grid. When that balance is upset, system safeguards kick in to keep wires from overheating or consumer electrical equipment from being damaged. The other factor is the basic loop design of the regional grids, where power moves into the grid from multiple generators (and from neighboring networks) and then around to the multiple communities being served. (The simplest loop would directly connect a single generator with a single community.) Unlike the spoke-like design of distribution systems, in which only the customers down the line from a break would be affected, an assault on the transmission loop, transformer substations (especially those connecting transmission and distribution systems), or regional control centers could affect all users if system safeguards were not available to isolate problems and restore the balance between generation and consumer load.

Research on How Systems Could Fail

The equipment used in the production and transmission of electricity and the electronic monitoring devices and other controls on which operators rely would be vulnerable to physical attack because those targets are located outdoors and have little active protection. The National Research Council recently reported that an assault on any individual segment of the network would probably cause only a local disruption, but "a coordinated attack on a selected set of key points in the system could result in a long-term, multi-state blackout." In a war-game simulation carried out at the Naval War College, experts described an attack on regional power supplies that combined a physical attack on transmission towers at key points with a cyber attack on control systems in the same region.[4] Cyber attacks could take the form of a computer virus, introduced through Internet connections and the utilities' private networks, that would target supervisory control and data-acquisition systems that utilities use to manage power flows.[5]

Potential Losses from Disruption of Vital Services

Although there are indications that the total costs from losing power for a short time might not be great, even a

3. In the NERC data, "outages" reflect interruptions, unusual occurrences, demand and voltage reductions, and public appeals. Discussions of those data appear in Sarosh Talukdar and others, "Cascading Failures: Survival Versus Prevention," *Electric Journal*, vol. 16, no. 9 (November 2003); Jay Apt and others, "Electrical Blackouts: A Systemic Problem, *Issues in Science and Technology*, vol. 20, no. 4 (Summer 2004); and Alexander Farrel and others, "Bolstering the Security of the Electric Power System," *Issues in Science and Technology*, vol.18, no. 3 (Spring 2002).

4. The "Digital Pearl Harbor" war game, conducted in July 2002, was sponsored by the Gartner Group and the U.S. Naval War College. A description of the scenario for a regional power disruption appears in related research, "Utilities Should Upgrade the Security of Their Operations," October 3, 2002, available at www3.gartner.com/2_events/audioconferences/dph/dph.html.

5. For a general discussion of threats to control systems for electric power (and related network industries), see Congressional Research Service, *Critical Infrastructure: Control Systems and the Terrorist Threat*, CRS Report for Congress RL31534 (updated January 20, 2004).

temporary loss could impose some costs in terms of human lives, environmental damage, and the economy. Specific concerns about environmental consequences relate to power losses at water treatment and sewage plants. In the August 2003 blackout, concerns about potential contamination of local water supplies as a consequence of even a brief shutdown in treatment facilities prevented people from using their water service for many days after power was restored. Impaired operations at sewage treatment plants could have further environmental impacts if they caused raw sewage to be released into rivers or lakes.

Also at stake in a power loss are injuries that occur in darkened buildings, heart stress, consequences of limited emergency service (for example, from restricted access to high-rise buildings), and health problems caused by disrupted life-support apparatus and the loss of refrigeration for medication or food subject to spoilage. A power loss also may compromise government emergency services and telecommunications to the extent that emergency calls cannot be placed.

A loss of power also could impose economic costs related to disruptions in commercial, government, or residential activity as well as physical damages to electricity infrastructure. At a basic level, consumer costs arise from breaks in electricity service because utility customers have limited flexibility to switch to other sources of electricity or completely different sources of energy. Immediate costs for business customers could result from lost production and inventory, damaged equipment (including damage to computer systems and electronic storage systems), and restart costs. For residential customers, direct costs from the loss of lighting, refrigeration, heating and cooling, and the use of other appliances may be associated with threats to health and safety as well as diminished lifestyle. Some of those losses may be erased when power comes back on, but there may be capital losses, too—for example, from lost data on computer systems or appliances damaged by power surges—that have longer-lasting consequences.

Evidence from past blackouts demonstrates that the electricity transmission system has been designed so that line failures do not cause physical damage to the system beyond the initial breaks. As a result, if difficult-to-replace equipment, such as high-voltage transformers, is not directly targeted in the attack, power can be restored relatively quickly and economic losses can be minimal. The response of electric utilities to the September 11 attack on the World Trade Center shows how robust the electricity network is and how good utility service people are at restoring service. That attack destroyed two electric substations and severely damaged five subtransmission feeders, in addition to numerous other distribution facilities.[6] The damage cut off service to 13,000 customers, many of which were buildings serving key financial markets. The electricity supplier restored service to most of those customers within eight days and enabled major financial institutions to reopen after only six days.

An example of a much broader, regional disruption was the Northeast-Midwest blackout of August 14, 2003, which affected about 50 million people. In that case, it took five days to fully restore service throughout the region, although most customers had power within 24 hours. The Department of Energy estimated the total cost of the blackout at $6 billion, with the biggest cost coming from lost income and earnings.[7] However, data on actual electricity use in that region in August 2003 show no discernible, unseasonable change in total power consumption attributable to the blackout—that is, whatever drop in power use occurred over those days appears

6. North American Electric Reliability Council, *2001 System Disturbances* (Princeton, N.J.: NERC, April 2003).

7. See Department of Energy, U.S.-Canada Power System Outage Task Force, *Final Report on the August 14th Blackout in the United States and Canada: Causes and Recommendations* (April 2004). Other sources on the costs of the blackout are ICF Consulting, *The Economic Cost of the Blackout: An Issue Paper on the Northeastern Blackout* (Fairfax, Va.: ICF Consulting, August 15, 2003), available at www.icfconsulting.com/markets/energy/doc_files/blackout-economic-costs.pdf; and Patrick Anderson and Ilhan K. Geckil, *Northeast Blackout Likely to Reduce U.S. Earnings by $6.4 Billion*, Working Paper 2003-2 (Lansing, Mich.: Anderson Economic Group, August 19, 2003), available at www.anderson economicgroup.com/pubs/articles_pressreleases/aegreports/blackout_AEGWP2003-2pdf.

to have been made up after the lights came back on.[8] Economic activity after the disruption would have made up for most of the temporary losses that DOE referred to as well.

Individuals directly affected by a power loss may take a different view. The industry commonly describes consumers' concerns about supply interruptions in terms of "reliability" of service. Studies of the economic value of that reliability (or, equivalently, the costs of interruptions) indicate that many customers would have been willing to pay perhaps 100 times their normal electricity bill for a disrupted period to avoid that loss of power.[9]

Regulating for Reliable Electricity Service

Utility regulation and voluntary industry standards govern the reliability of electricity supplies. Regulatory bodies represent the interests of electric utility customers, working to ensure that the utilities maintain a level of reliability that reflects the social costs of service interruptions—not just the private costs to utilities from damaged equipment and lost sales. Under current standards, the utilities generally achieve the required level of reliability by maintaining sufficient excess capacity to overcome the loss of at least one important component at a time. The regulatory structure of the industry is changing, with large parts of the wholesale trade in electricity being priced at market rates, but most retail rates continue to reflect utilities' guaranteed recovery of expenditures on reliability. For the most part, rates for retail sales, transmission services, and some wholesale trade are approved by state public utility commissions (PUCs), the Federal Energy Regulatory Commission, and other government entities on the basis of prudent expenses by utilities plus a markup that allows them to earn a given rate of return on their capital investments.[10]

Because utilities interact with other utilities and, increasingly, with independent generators to move power over large regional networks, they are interdependent in providing their respective customers with reliable supply. The industry has adopted voluntary standards to help prevent outages to customers that result from disruptions by other suppliers. In response to the nation's first large blackout, in New York in 1965, the electric power industry established the North American Electric Reliability Council to oversee the overall reliability of wholesale electricity supplies in North America. Utilities' participation in the NERC is voluntary, but the organization exercises significant influence over reliability planning and coordination because utilities recognize their high degree of interdependence.

Under NERC's voluntary standards, utilities operate the network with a contingency for the failure of network components that is known as "N minus one." That means the transmission network is operated so that it could continue to serve customers fully if a single critical network component failed. (Critical equipment includes generators, segments of the transmission grid, and high-voltage transformers.) In the event of such a failure, operators are supposed to quickly adjust the network to a new N-minus-one status in which the system can withstand the failure of an additional component. If operators cannot restore the network to that status, they are supposed to take other actions to ensure that any effects are isolated to the local area so that neighboring systems cannot be affected. (Under existing standards, all power systems have protective devices such as fuses to ensure that any disruption in power quality cannot physically damage the equipment. In the event of a power surge that could not be controlled by those automatic fail-safes, operators would need to shut down all affected equipment to avoid

8. For example, see monthly data on retail electricity sales from Department of Energy, Energy Information Administration, *Electric Power Monthly*, DOE/EIA-0226 (various issues), which indicate no relative drop in sales from July 2003 to August 2003 compared with those months in 2002 and 2004.

9. Estimates of the value of service reliability vary widely depending on many factors, such as the type of customer and the time and length of the outage. For a detailed review of estimates, see Lawrence Berkeley Laboratory, *Scoping Study on Trends in the Economic Value of Electricity Reliability in the U.S. Economy* (Berkeley, Calif.: Lawrence Berkeley Laboratory, June 2001).

10. With the introduction of competition in wholesale markets—largely because of federal policy initiatives—new merchant generators have emerged that are not subject to rate-of-return regulations, and utilities have had strong incentives to divest generation capacity to avoid rate-of-return regulations, too. In some states, utilities have sold off additional generation capacity as a part of local initiatives to restructure retail markets. However, utilities that still own generation facilities as part of their vertically integrated systems and all of the federal power agencies continue to base their wholesale prices on operating costs plus a return on capital. For transmission services, the federal government ensures that all utilities receive their costs and a fair rate of return, but individual purchasers of transmission services may pay more than that cost, depending on local congestion.

damage.) The NERC also has developed detailed guidelines that may help protect the electric power sector from physical and electronic attacks.[11]

Ideas for New Approaches to Reliable Electricity Service

A terrorist attack (or another, more common cause of power loss) that disrupted electricity supplies would be likely to impose social costs on the public in addition to those faced by the providers and direct purchases of that power. Private costs would be borne by the owners of the generators, transmission lines, or control centers that were the immediate target of such an attack and by their electricity customers who lost power for any period of time. Those private costs include the value of equipment damaged in the attack and lost sales from the interruption of power. Society's costs would encompass other power suppliers (and their customers) affected by cascading system problems but not directly doing business with the targeted utility. Total costs would include the inconvenience or threats to safety for everyone dependent on the goods and services that the direct electricity customers provide—for example, residents of high-rise buildings, customers of retail gasoline outlets, or communities that rely on water treatment systems and certain emergency services.

In general, electricity suppliers do not see the full social benefits from spending to increase reliability or are not able to fully profit from their efforts. For that reason, there is general recognition that government has an important role to play in promoting efforts to make electricity service more reliable and increase consumers' ability to endure interruptions. Many of the options described here have been considered as a part of several comprehensive energy bills introduced in past Congresses—independent of any concerns about homeland security. For example, the Energy Policy Act of 2003 would have required the Federal Energy Regulatory Commission to establish several new rules for managing the nation's electricity system and governing the electricity industry's business practices.[12] Such rules would affect transmission services, construction and siting permits for new transmission lines and the reliability of the nation's electricity transmission infrastructure.[13]

Internalizing the Costs of Power Losses

Policies that would lead the electricity industry to internalize more of the social costs of potential attacks could include fiscal incentives and regulatory changes that caused utilities to further improve their response to a loss of key facilities or that helped reduce general economic losses by making utilities and power consumers less reliant on particular sources of supply.

For example, to improve preparations for the threat of an attack on any one critical piece of equipment, such as a high-voltage transformer, utilities could be required to hold larger inventories of those critical spare parts (or perhaps establish a national stockpile). Another option would be to standardize the design of critical spare parts to increase the use of existing local inventories in responding to attacks elsewhere in the country. Also, although the costs of hardening defenses for the nation's transmission system may far exceed the benefits of avoiding an attack on any part of the system, opportunities may exist to physically protect certain key pieces of equipment.[14] For instance, because there are relatively few high-voltage transformers that step down power to serve the nation's largest cities, protecting those important substations against light attacks may be cost-effective.

Introducing Competition. Introducing competition into both wholesale and retail markets for electricity has been a goal of federal law and regulation for almost 30 years. Competition has occurred to some extent in the wholesale markets, and security concerns may reinforce the case for continuing on that path. Specifically, introducing competition from additional power sources could further reduce losses from a successful attack by making it easier

11. See North American Electric Reliability Council, *Security Guidelines for the Electric Sector* (June 14, 2002), available at www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricity Sector-Version1.pdf.

12. S. 14, 108th Cong. (2003). See Congressional Budget Office, Cost Estimate for S. 14, *Energy Policy Act of 2003* (May 7, 2003).

13. For a discussion of some options directly relevant to the vulnerability of electric power control systems, see Congressional Research Service, *Critical Infrastructure.*

14. For a discussion of why hardening the transmission system's defenses may not be the best strategy to pursue, see Alexander E. Farrell, Lester B. Lave, and Granger Morgan, "Bolstering the Security of the Electric Power System," *Issues in Science and Technology* (Spring 2002), available at www.issues.org/issues/18.3/farrell.html.

for utilities to replace lost power and by giving regional systems more flexibility in achieving a balance of generation and load. In addition, customers would be better able to choose suppliers on the basis of reliability or to switch to other power sources during a disruption. Further, increased competition could better align electricity prices with scarcity, giving consumers and businesses greater incentives and capabilities to switch to less costly sources of supply.[15] Competition could also allow customers who placed a particularly high value on reliability to invest in their own backup generation or contract with local, off-grid suppliers—thus enabling them to switch to other power sources during a disruption of the main supply.

More sources of supply would mean greater reliability in the face of disruptions to any one of those sources. But competing sources of electricity supply—such as neighboring utilities, merchant generators, and industrial cogenerators—may need federal legislation to overcome regulatory impediments to expanding their markets. Such impediments come from regulations that establish who can buy and sell power at competitive rates, restrict the addition of transmission lines and regional planning in general, restrict connection of new suppliers to local grids, and limit consumers' ability to add generation capacity. Adding transmission capacity may be especially important to increasing competition—whether by adding new lines or improving the management of existing systems.

Local Versus Regional Regulation. Regulatory obstacles to protecting the supply of electricity are complex. Because of the network design of the regional grid and the interdependence of local supply systems, new spending on transmission links or activities to directly protect equipment in one local system would help protect supplies regionwide. But local regulators might be reluctant to approve rate hikes to cover spending that did not exclusively benefit their local consumers. And more immediately, local utilities might be reluctant to take actions that could protect regional supplies—such as shedding load to help preserve system balance—if they did not receive compensation for lost sales. One possible solution to those problems is to transfer authority for approving new transmission lines or other changes related to regional reliability from local regulators to regional authorities that would focus more on systemwide effects.

Other restrictions on competition make it difficult for local customers to choose suppliers on the basis of reliability or to develop capacity to switch to other power sources during a disruption. Consumers continue to face obstacles to installing their own generating devices, although such home- and business-based power would be likely to enhance regional reliability.[16]

Despite the difficulty of devising fully competitive markets for wholesale and retail power, several options related to market restructuring exist that might help internalize social costs that could otherwise result from service disruptions. Those options include:

- Establishing a structure for wholesale markets for electricity (and for ancillary services) that would reduce barriers to entry for new suppliers and help improve incentives for regional coordination in areas of the country where such markets do not exist.
- Requiring planning over broader regions (whether by private entities independent of the utilities or by government agencies) for generation and transmission capacity to reduce system vulnerability, funded by fees on all regional suppliers. (Such planning organizations would have authority over local public utility commissions and publicly owned utilities and merchant generators that are not subject to PUC jurisdiction.)
- Requiring all suppliers (utilities and nonutilities) to build greater redundancy into regional systems by constructing whatever generating and transmission capacity is called for in the regional plans.
- Improving real-time management of regional power grids to further increase the system's flexibility to manage disruptions (either by placing more decisionmaking authority about generation and load-shedding with operators of the regional transmission systems or by improving the availability of information on emerging supply constraints to help local utilities make decisions).

15. A discussion of problems in implementing increased competition appears in Paul L. Joskow, *The Difficult Transition to Competitive Electricity Markets in the U.S.* (Washington, D.C.: AEI-Brookings Joint Center for Regulatory Studies, July 2003), available at www.aei.brookings.org/admin/authorpdfs/page.php?id=271.

16. For a discussion of regulatory obstacles to distributed generation, see Congressional Budget Office, *Prospects for Distributed Electricity Generation* (September 2003).

Concerning the options for regional planning and real-time management, one approach could be to give the North American Electric Reliability Council regulatory authority to establish and enforce clear standards for utilities on available reserves. Another approach could be to give regional operators the ability to issue orders to temporarily reduce the supply to some consumers (or shed load) as a precondition for connection to regional power grids. And the Federal Energy Regulatory Commission could be given authority to direct the construction of additional transmission lines and to set conditions for wholesale markets that would enable more suppliers to participate.

Increasing Customers' Flexibility. One option to increase electricity customers' flexibility to respond to disruptions would be to require retail utilities to promote diversity of energy and power sources for their customers (including providing a choice of suppliers). To be most effective, such diversity would need to reflect an addition to the generating capacity anywhere it might be needed (to overcome constraints on transmission), an increase in the number of different suppliers (to overcome constraints on individual suppliers), or an increase in the types of energy sources for generating power (to overcome constraints on supplies of individual fuels for generating power). One approach to help achieve that diversity would be to remove technical, contractual, and pricing impediments that discourage consumers from investing in distributed power (for homes and businesses) and cogeneration (especially for critical industries).

In addition, the current system of average-cost pricing can undermine consumers' incentives to reduce power use at critical times, thus weakening system reliability. One possible response would be to implement real-time, marginal-cost pricing at the retail level, with consumers free to choose providers. The resulting prices would more fully reflect the scarcity of supply, so that any power disruptions would lead to higher prices—which in turn would lead some consumers not affected by shortages to reduce their use. For disruptions that lasted long enough for the price signals to reach consumers, the reduction in power use by some would make additional power available where it was needed most.

Need for Backup Generators. One problem for the market is that many of the people who rely on electricity are not the direct purchasers—for instance, people who live in high-rise buildings, take the subway, or depend on community and business services that require reliable electricity. Many critical services, such as hospitals, already maintain their own generators as a backup source of electricity. And under local building codes, most high-rises are required to have them, too. But the August 2003 blackout demonstrated that many high-rises in New York City had no working backup systems. Traffic gridlock ensued because traffic lights did not work; people ran out of gas in idling cars, and service stations were unable to refill gas tanks. In several cities, the absence of backup power at water and sanitation facilities for even a brief period jeopardized the safety of drinking water for weeks. That scenario suggests the establishment of national building codes to require the presence of emergency backup generators for high-rise buildings, electricity-powered subways, traffic lights, gasoline stations, and critical public functions such as water treatment.

Socializing the Costs of Power Losses

It may be cost-effective to federalize some supply activities, such as transmission, or to make regional planning a government activity. Options that would socialize the costs of power losses attributable to terrorism (or other causes) include:

- Establishing fiscal incentives for utilities to remove constraints on regional power systems—for example, by supporting construction of additional generating units (possibly driven by different fuels) or new transmission lines in markets that have little diversity of supply.

- Compensating local utilities for their stranded costs attributable to new competition. (Stranded costs are investments by the utilities that cannot be paid off because of regulatory changes that undermine the utilities' revenue base.)

- Establishing fiscal incentives for new investments in distributed power (in homes and businesses) and cogeneration (in critical industries), especially in markets where there is no choice among electricity suppliers.

Improving Information

Security efforts can be enhanced if suppliers and customers have more-complete information on the extent of a current power loss or their vulnerability to future losses. With changes in the structure of electricity markets, transmission systems must now move power for more generators and to more communities than they originally

were designed for.[17] And the communities that purchase bulk power do not always know where their power is coming from or by what routes. Several options to address that information gap include:

- Requiring utilities or transmission-system operators to prepare vulnerability assessments that would indicate facilities where the need for additional capacity or a hardening of defenses was greatest.
- Establishing market-based, real-time prices in the wholesale markets for electricity to help convey better information about the potential for losses.
- Requiring operators to install additional sensors and telemetry to provide detailed, real-time information on power flows at all points within the regional grids and between grids.
- Collecting and disseminating additional national information indicating potential supply constraints and system weaknesses and improving the display of power-flow information.

17. For a discussion of information needs in the transmission sector, see Department of Energy, Energy Information Administration, *Electricity Transmission in a Restructured Industry: Data Needs for Public Policy Analysis,* DOE/EIA-0639 (December 2004).

CHAPTER

5

Food and Agriculture

Reports of terrorist groups' interests, as well as the history of events involving food contamination and the use of biological agents, support concerns about the prospect of terrorist attacks on the food and agriculture industry.[1] The industry would be vulnerable to attack because of the large numbers of food items and the many points of access. However, many of those vulnerabilities are already addressed through extensive regulation put in place before September 11 in response to the nation's continuing concerns about food safety. That regulation and the organization of the nation's public health system would help limit the losses from any attacks on food supplies involving a range of known agents. The greatest concern would be threats that could escape or exceed the nation's current detection capabilities or for which an effective response would require an increased level of coordination among agencies and different levels of government.

Vulnerabilities from Contamination, Loss of Food Sources, and Use of Agricultural Resources as Weapons

The use of natural agents in attacks on agriculture or directly on people is commonly described as bioterrorism. That term would include biological attacks—such as with Bacillus anthracis (anthrax) and smallpox—that might not involve farms and food but would require some of the same protective measures and emergency responses. The security of drugs and drinking water supplies is a particularly important, related concern. And although the main focus of attention in the event of a biological attack would be on the immediate safety of the food supply, much of the value of the industry's output is in areas such as forest products, fibers, and other products that are not related to food—and those nonfood resources could be threatened as well.

Types of Attacks

The food and agriculture industry is vulnerable to four types of assaults:

- Contamination of food with natural biological agents, such as Clostridium botulism toxin (botulism) and Escherichia coli bacteria (E. coli);
- Contamination of food with man-made contaminants, such as poisonous minerals or chemicals and foreign objects;
- Attacks to disrupt food supplies, including the use of fires, floods, or biological agents such as foot-and-mouth disease or insects; and
- Use of agricultural resources as weapons for attacks on other targets, such as wildfires that spread to residential areas, nitrate fertilizer for use in explosives, pesticides for poisoning, crop dusters to spread toxins, or radioactive materials used in food irradiation.

The Food and Drug Administration (FDA) has identified several specific hazards to the safety of food supplies.[2] Among the biological hazards, the deadly pathogens anthrax and botulism are considered the greatest dangers. Next are salmonella, pathogenic strains of E. coli, and ri-

1. For a discussion of the threat to food supplies, see Food and Drug Administration, *Risk Assessment for Food Terrorism and Other Food Safety Concerns (*October 13, 2003), available at www.cfsan.fda.gov/~dms/rabtact.html. For a discussion of the threat to crops and livestock, the economic implications, and some policy ideas for countering that threat, see Congressional Research Service, *Agroterrorism: Threats and Preparedness*, CRS Report for Congress RL32521 (August 13, 2004).

2. Food and Drug Administration, *Risk Assessment for Food Terrorism and Other Food Safety Concerns* (October 13, 2003), available at www.cfsan.fda.gov/~dms/rabtact.html.

cin. Among the man-made contaminants that present a threat, FDA has noted concerns about heavy metals (such as lead and mercury), pesticides, dioxins, and other substances that could be introduced into the food supply.

Potential Weaknesses in Defenses

The vulnerability to extensive losses would be relatively small if a disease or contaminant maliciously introduced into the food supply was one with which the industry had experience. The government tests for the most common diseases and requires that outbreaks of many diseases (whether in plants and animals or in the human population) be reported. As a result, it is likely that an attack would be detected early, traced to its source, treated, and contained.

Losses could be significantly higher if the attacks involve substances that can enter the supply chain at a point before or after which their origins cannot be traced, substances that are not tested for, and pathogens or contaminants with which government inspectors or health professionals have little experience. Tests may not be available to detect certain agents within foods, and people's exposure to such substances may not be recognized or reported to appropriate state or national organizations to discern a pattern of assault or initiate a response. Further, detection of and response to new modes of attack may require an increased level of coordination among different federal agencies and between different levels of government.

For example, the Department of Agriculture (USDA) tests many meat products for E. coli and salmonella, but it does not routinely test food supplies for contamination from anthrax or ricin. Records are kept on animals, poultry, and eggs that enable USDA to trace the source of contaminants back through much of the supply chain. But after meats are delivered to meat processing centers, for example, there is no way to distinguish what herds (or animals from specific regions or countries) went into what batches of meat products for subsequent delivery to stores. The Food and Drug Administration also requires random testing of many food products (in processing and packing facilities and in transit) for certain contaminants. However, for food products, FDA currently requires only that lot numbers (for tracking purposes) be placed on infant formula and low-acid canned food.

Terrorists' Intent and Past Incidents

Terrorist groups reportedly have shown interest in exploiting weaknesses in the nation's food and agriculture industry, although little information on that threat is publicly available. The al Qaeda terrorist group is known to have considered using crop duster aircraft, apparently with the intent of distributing toxins or pathogens over crops and populated areas. Members of a related group were arrested in London for trying to manufacture the deadly poison ricin—a product of castor beans.

The number of publicly documented crimes intended to harm people or disrupt supplies is small. However, many of those assaults confirm the potential for serious health and economic consequences. For example, efforts by a religious cult in Oregon to contaminate local salad bars with salmonella in 1984 affected 750 people. Other incidents of food sabotage are more commonly perpetrated by disgruntled employees and affect only a few people. But the consequences can be more widespread than the direct numbers harmed, as illustrated in the 1982 case of cyanide-tainted Tylenol capsules. The immediate effect was seven deaths, but the resulting publicity caused a near-total collapse in national demand for that product and led to at least five imitation attacks in subsequent years, all involving fatalities.[3]

Potential Losses from Threats to Health or Consumers' Aversion to Contaminated Products

The immediate consequences of a terrorist attack on food and agriculture may be illness or the loss of life, depending on the nature of the attack and how quickly it is detected. With the important exception of several foodborne outbreaks affecting many thousands, the numbers of people seriously harmed by individual incidents (whether by accident or intent) have been small, at least in part because of current regulations and the success of the nation's public health system in containing outbreaks and limiting losses. As a result, the costs of a terrorist attack may be related more to business losses than human losses. Much of the economic cost would result from the increased costs of replacing lost supplies. That cost might

3. Those acts were the poisonings of Lipton Cup-A-Soup in 1986, Excedrin in 1986, Tylenol again in 1986, Sudafed in 1991, and Goody's Headache Powder in 1992.

be small for the nation but could differ among regional economies.

Losses from Accidental Contaminations

Past incidents involving accidental contaminations of the food supply indicate the potential health consequences of an attack and underscore the importance of current food safety regulations and public health institutions. Researchers at the Centers for Disease Control and Prevention estimate that 76 million illnesses, 325,000 hospitalizations, and 5,000 deaths occur every year because of contaminated food.[4] Specific incidents point to how widespread a contamination can become if not detected quickly. About 170,000 people were sickened by salmonella typhimurium in milk from a U.S. dairy plant, and 224,000 people were sickened by salmonella enteritidis linked to ice cream.[5]

Economic costs associated with those threats to health and safety can be significant. For example, USDA estimates that the annual cost to the nation—in terms of medical costs, productivity losses, and costs of premature deaths—from five major foodborne pathogens totals $6.9 billion.[6]

Why Economic Consequences Might Be Small

Retail sales by food and beverage stores (including groceries) were more than $505 billion in 2003, and agricultural exports were valued at more than $59 billion.[7] However, those types of aggregate measures of the value of annual sales or output are likely to overstate the potential economic cost to the nation of disrupting the industry. It is difficult to imagine how all food supplies could be affected or even how the total supply of any basic food source could be affected for a significant amount of time. Replacement supplies (from storage or from unaffected regions) and very close substitutes (from the perspective of consumer welfare) are readily available for virtually every type of food product. People could draw on current inventories of the targeted item (in home and stores), stop consuming any particular food item altogether, stay away from food from a particular agricultural region, or not frequent a given grocery chain or fast-food outlet. For the nation as a whole, the sales lost by products or establishments that were directly affected by an attack would be made up in increased sales elsewhere.

The cost to the national economy would, for the most part, be the increase in the cost of supplying those replacements or substitutes (and the loss in consumer satisfaction). For a number of reasons, even that residual cost should be small. First, the food and agriculture industry is well adapted to the prospect of disruptions from weather and occasional health incidents. For example, in anticipation of periodic crop losses, the most vulnerable crops are often grown in multiple regions, and individual farmers diversify their plantings and purchase crop insurance. Similarly, food distributors and grocers already have experience with identifying and recalling contaminated lots. Second, government programs are in place to ensure food safety (and limit the health consequences of an attack) and to sustain the income of some agricultural producers (and, indirectly, the businesses and regions that depend on them). As a result, the economic effects of a terrorist incident might well fall within the realm of industry experience and current public plans for detection and response.

Cases in Which Economic and Societal Costs Would Be Highest

Circumstances could exist, however, in which the cost of replacement would be high or the cost to society would be greater than the immediate loss associated with any replacement or substitution for lost supplies. For example, replacement costs could be greater than otherwise if there was a high market concentration in the targeted food or agriculture industry. Where only one or a few businesses account for a large share of sales, the opportunities for drawing on inventories or switching to other suppliers may be limited. Also, in some cases of contamination, the costs of replacing lost supplies may entail more than sim-

4. Paul S. Mead and others, "Food-Related Illness and Death in the United States: Reply to Dr. Halberg," *Emerging Infectious Diseases,* vol. 5, no. 6 (November-December 1999).

5. Food and Drug Administration, *Risk Assessment for Food Terrorism and Other Food Safety Concerns*. Other examples of foodborne outbreaks, intentional and unintentional, appear in FDA, Notice of Proposed Rulemaking, *Federal Register,* vol. 68, no. 90 (May 9, 2003), p. 25187.

6. Department of Agriculture, Economic Research Service, "Economics of Foodborne Disease," available at www.ers.usda.gov/briefing/FoodborneDisease/features.htm.

7. Sales data for 2003 are from Bureau of the Census, *Annual Benchmark Report for Retail Trade and Food Services: January 1992 Through February 2004* (March 2004), Table 2, available at www.census.gov/prod/2004pubs/br03-a.pdf. Export data for 2003 are from Department of Agriculture,*Outlook for U.S. Agricultural Trade, AES-4* (November 22, 2004), available at usda.mannlib.cornell.edu/reports/erssor/trade/aes-bb/2004aes44.pdf.

ply ramping up production. For some diseases, there may be few options to eliminate the risk of further contamination other than burning facilities, plants, and livestock.

The cost to society would be greater than the direct losses associated with replacement and substitution if there were noneconomic losses to consider. For example, if the attack resulted in a major forest fire, costs could include the loss of recreational benefits, erosion from damaged watersheds, and loss of wildlife—values that can be difficult to express in dollar terms. And attacks involving pesticides or other toxins could cause environmental damage.

Regardless of the economic cost to the nation, the potential loss for the particular producers or regional economies could be significant. For example, in seven states, farm employment accounts for more than 5 percent of the total state work force.[8] The nature of many agricultural commodities is that they are produced in discrete growing seasons: once the current supply is lost, the domestic market has to wait through a new cycle.

Other Long-Term Effects on Businesses

Broad consumer concerns about the safety of food supplies can have other adverse economic effects. Any public demonstration of vulnerability to attack can lead to costly, long-term (if not permanent) changes in product handling and consumer demand. The Tylenol case, for instance, led to requirements for tamper-resistant packaging. The situation with mad cow disease, although not deriving from terrorism, has led to new costs, too—from having to discard certain animal parts, restrict the contents of animal feed, and inspect slaughtered animals. Based on the costs to beef producers in Japan for inspecting slaughtered animals, that requirement alone could entail $1.2 billion in expenses for the much larger U.S. beef industry if applied here.[9] (Japan spends $40.9 million a year inspecting only about 1.3 million slaughtered cattle. The United States slaughters about 37 million cattle annually.)

8. Percentages for 2002 are from Bureau of Economic Analysis data on farm employment, available at www.bea.doc.gov/bea/regional/reis/drill.cfm?table=CA25N&lc=70&years=2002,2001&format=htm&areatype=00000.

9. "Japan Is Strict Model for Cow Testing," *Wall Street Journal*, December 29, 2003.

Current Programs for Food Safety

The U.S. food and agriculture industry is highly regulated.[10] Virtually all products at all points in the supply chain are regulated to some degree to ensure the ultimate safety of the food supply and protect the agricultural economy. The principal federal regulatory agencies responsible for providing consumer protection are FDA (part of the Department of Health and Human Services), USDA's Food Safety and Inspection Service and Animal and Plant Health Inspection Service, and the Environmental Protection Agency. Inspectors from the Department of Homeland Security's Bureau of Customs and Border Protection assist other agencies by checking imports. (Further controls come from state and local regulations. All states conduct safety inspections of food processing plants. Some states, such as California, have programs that restrict certain agricultural imports or that call for inspections of agricultural shipments.)

Federal Programs

FDA is charged with protecting consumers against impure, unsafe, and fraudulently labeled foods. It has regulatory authority over about 80 percent of the nation's food supply, including seafood, canned goods, and other products that are defined as "food" in the Federal Food, Drug, and Cosmetic Act. Many substances come under FDA jurisdiction as "food" because of the presence of substances or chemicals in food containers or other food-contact surfaces that can leech into food products.

Generally, only meat, poultry, and egg products fall under the direct responsibility of other agencies. The Food Safety and Inspection Service regulates the safety, quality, and labeling of most meats, as well as poultry and egg

10. For an overview of federal regulation, see the interagency paper by the Department of Agriculture and the Food and Drug Administration, *A Description of the U.S. Food Safety System* (March 3, 2000), available at www.fsis.usda.gov/OA/codex/system.htm. For a specific discussion of FDA and USDA regulation at food-processing plants, see General Accounting Office, *Food-Processing Security,* GAO-03-342 (January 2003). For a discussion of bioterrorism security efforts by the Department of Health and Human Services, see General Accounting Office, *HHS Bioterrorism Preparedness Programs,* GAO-04–360R (February 10, 2004).

products.[11] EPA's mission includes protecting public health and the environment from risks posed by pesticides and promoting safer means of pest management. No food or feed item may be marketed legally in the United States if it contains a food additive or drug residue not permitted by FDA or a pesticide residue exceeding tolerance level established by EPA. The role of the Animal and Plant Health Inspection Service is to protect against the introduction and spread of plant and animal pests and diseases, in part by monitoring countries experiencing outbreaks of foot-and-mouth disease, mad cow disease, and other diseases. Those agencies also use existing food safety and environmental laws to regulate plants, animals, and foods that are the products of biotechnology.

Many other agencies have food safety missions within their research, education, prevention, surveillance, standard-setting, and outbreak-response activities. Within FDA are the Center for Food Safety and Applied Nutrition and the Center for Veterinary Medicine. Other agencies at the Department of Health and Human Services are the Centers for Disease Control and Prevention and the National Institutes of Health (which identify sources and cures for food-related illnesses), and other offices of the Public Health Service (which help prepare hospitals and health professionals for responding to a bioterrorist attack).[12] Other USDA agencies with some stake in food safety are the Agricultural Research Service; the Cooperative State Research, Education, and Extension Service; the Agricultural Marketing Service; the Economic Research Service; the Grain Inspection, Packers, and Stockyard Administration; and the Food and Nutrition Service. At the Department of Commerce, the National Marine Fisheries Service inspects fish processing plants for compliance with FDA and USDA safety regulations under a voluntary industry program.

New Policies Since September 11

The federal policy for defending the food and agriculture system against terrorism, disasters, and emergencies was laid out in January 2004 in Homeland Security Presidential Directive–9.[13] The Department of Health and Human Services, USDA, and EPA were directed to increase their efforts in the areas of prevention, surveillance, emergency response, and recovery. Much of USDA's effort is grouped in its Food and Agriculture Defense Initiative, including its program to direct research and share information through the Food Emergency Response Network —a joint effort with FDA and participating state laboratories.[14] In addition, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 provided the authority for new regulations to improve FDA's ability to identify domestic and foreign facilities that provide food, monitor and target inspections of food imports, and notify food processors and other establishments that may have been or become involved in the contamination of food supplies.[15] Regulations recently promulgated under the authority of that law require all businesses in the chain of supply to maintain records that would identify the immediate previous sources and immediate subsequent recipients of food and its packaging.[16] Finally, the Project BioShield Act of 2004 required new measures to expand and expedite the availability of vaccines and treatments to combat potential bioterrorism agents.

Ideas for New Approaches to Food and Agriculture Security

Two basic problems can cause the social losses from an attack on food supplies to be greater than the private losses to suppliers. One problem is that most food products, by the time they reach the market, cannot be distinguished by their source, so the supplier of a harmful product may bear little responsibility for, or suffer serious economic loss from, its adverse effects. That situation also applies to sellers of hazardous agricultural supplies, such as nitrates or pesticides, that can be used in attacks elsewhere. The other problem is that consumers may not be able to assess the safety of their food and suppliers may not know if they are starting with a contaminated product.

11. Products subject to regulation are defined in the Federal Meat Inspection Act, the Poultry Products Inspection Act, and the Egg Products Inspection Act.

12. The Centers for Disease Control and Prevention provides an overview of documents and activities related to public health preparedness at www.bt.cdc.gov/planning/index.asp.

13. Available at www.whitehouse.gov/news/releases/2004/02/20040203-2.html.

14. Information on the budget and activities of the Food and Agriculture Defense Initiative is available at www.usda.gov/agency/obpa/Budget-Summary/2005/05.FoodandAgDefense.htm.

15. See Food and Drug Administration, *The Bioterrorism Act of 2002*, available at www.fda.gov/oc/bioterrorism/bioact.html.

16. *Federal Register,* vol. 69, no. 236 (December 9, 2004), p. 71561.

Internalizing the Costs of Food and Agriculture Security

Specific options that could cause the food and agriculture industry to internalize more of the costs of increasing their security efforts are:

- Establishing more-extensive labeling and tracking systems for food products. Such systems also could include the tracking of animals and animal products, with the goal of helping health officials more quickly pinpoint and isolate the source of contamination. Other requirements could include regular sampling at different stages of food processing and delivery to detect a wider range of dangerous contaminants.[17]

- Short of complete labeling, indicating the country or region of origin for some foods—if that could help health officials more quickly pinpoint the sources of contamination. (Otherwise, reports of contamination might lead to discarding more food than was necessary.)

- Establishing full tracking of ownership for the most hazardous materials in the agriculture industry that could be used as weapons (including nitrates and certain pesticides).

- Establishing enhanced incentives and protections for reporting new incidents of food contamination, improper sales of hazardous materials, unsafe processing and handling procedures, or incomplete inspections that might increase consumers' vulnerability.

Socializing the Costs of Food and Agriculture Security

In some cases, government efforts to conduct or fund safety programs may be more cost-effective than private efforts. For example, it may be worth considering expanding the food and agricultural inspection system by adding inspectors and increasing the frequency of sampling where there already is a federal role, as well as introducing federal inspectors in other vulnerable markets.

Improving Information

Suppliers may have little information about the technologies for or costs of making their products safer. Further, they may not know about threats to safety that are introduced somewhere farther along in the supply chain. That last point is especially relevant for individual food businesses that do not have full control over their production, distribution, and retail activities—because they lack either direct ownership of that full chain of activities or long-standing arrangements with their suppliers and customers.

Expanding programs to provide early warning of contaminations—without creating a major new regulatory system—could help improve information. One such option would be the creation of new public/private partnerships to help quickly disseminate information on specific threats to the general public—for example, on assaults in progress—or on general threats and potential corrective actions. Those partnerships could help move critical information to individuals, businesses, and local governments that must take action. A related option would be to create new information clearinghouses to address the difficulty of pulling together isolated pieces of information on outbreaks of certain illnesses or instances of contamination that are not widely monitored—in much the same way that certain communicable diseases must now be reported to the Centers for Disease Control and Prevention. That option could help move information upward toward central agencies that could look for broad patterns and provide early warning of an assault under way.

17. Congressional Research Service, *Animal Identification and Meat Traceability*, CRS Report for Congress RL32012 (updated July 2, 2004), and *Country-of-Origin Labeling for Food*, CRS Report for Congress 97-508 ENR (updated August 3, 2004).