DEPARTMENT OF JUSTICE
ASSESSMENT OF THE INCREASED RISK OF TERRORIST OR OTHER CRIMINAL ACTIVITY ASSOCIATED WITH POSTING OFF-SITE CONSEQUENCE ANALYSIS INFORMATION ON THE INTERNET

April 18, 2000

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

I. BACKGROUND 6
- A. The Chemical Safety Information, Site Security and Fuels Regulatory Relief Act 6
- B. RMPs and OCA Data 8
- C. EPA's Current Internet Website 11

II. NATIONAL SECURITY ISSUES 11
- A. The Threat from International Terrorism 13
- B. The Threat from Domestic Terrorism 14
- C. Trends in Terrorism involving Weapons of Mass Destruction 15
- D. The Growth of the Internet and Threats to Our National Security 19
- E. The United States' Response to These Threats 20

III. THE POTENTIAL DANGERS AND THE LIKELIHOOD OF A CHEMICAL RELEASE CAUSED BY A CRIMINAL OR TERRORIST 22
- A. The Likelihood that Someone Could Cause a Toxic Industrial Chemical Release 22
  - 1. Terrorists and Other Criminals Have Considered Using Chemical Releases from Industrial Facilities as Weapons 22
  - 2. The Feasibility of a Criminal or Terrorist Causing a Release of Toxic or Flammable Industrial Chemicals 25
- B. Industrial Facilities Are Attractive Targets to Terrorists and Criminals 27

IV. EXPLOITATION OF PUBLICLY AVAILABLE INFORMATION BY TERRORISTS, CRIMINALS, AND HOSTILE GOVERNMENTS 31
- A. Publicly Available Information Used in Criminal Acts 32
- B. Public Information Disseminated Through the Internet Used in Criminal Acts 33

V. EVALUATING THE RISKS OF MAKING OCA DATA AVAILABLE TO THE PUBLIC 34
- A. OCA Data that Provides Information Important to Causing, Targeting, or Maximizing the Effects of an Industrial Chemical Release 34
- B. Pieces of OCA Data that Would Be Salient to a Terrorist Attack that Are Currently Publicly Available 39
  - 1. Information Currently Disseminated by EPA 39
  - 2. Analysis of the Current Availability of OCA-Type Data 40
- C. Public Dissemination of OCA Data Consistent with National Security and Law Enforcement Concerns 43
  - 1. Security of Data Disseminated Using the Internet 43
  - 2. Problems with the Breadth of Access of Internet Information 45
  - 3. Access to Paper Copies of OCA Data and the Internet 46

DEPARTMENT OF JUSTICE
ASSESSMENT OF THE INCREASED RISK OF TERRORIST OR OTHER CRIMINAL ACTIVITY ASSOCIATED WITH POSTING OFF-SITE CONSEQUENCE ANALYSIS INFORMATION ON THE INTERNET

EXECUTIVE SUMMARY

On August 5, 1999 the President signed into law the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRA). This legislation requires the President to promulgate on or before August 5, 2000, regulations to address public access to information describing the worst possible impact that a release of toxic or flammable chemicals from a facility could have on the nearby populace and environment. This data, called off-site consequence analysis (OCA) information, is contained in documents known as Risk Management Plans (RMPs). Approximately 15,000 chemical facilities throughout the United States have submitted RMPs to the EPA.

The statute requires that the regulations be based on an assessment of whether release of OCA information over the Internet would increase the risk of terrorism or other criminal acts directed at the chemical facilities submitting such data, and an assessment of whether such release of OCA information would reduce the risk of accidental releases of chemicals from the facilities. The statute further requires that the regulations balance, to the extent possible, the potential risks and the potential benefits, thereby minimizing the overall risk to public health. On January 27, 2000 the President delegated the drafting of the assessments to the Environmental Protection Agency (EPA) (to describe the benefits of release of the OCA data) and to the Department of Justice (DOJ) (to describe the risks associated with the release of such information). The President also delegated jointly to EPA and DOJ the task of drafting the regulation.

For purposes of this risk assessment, we posed three questions: (1) what is the likelihood that a terrorist or other criminal would attempt to use an industrial chemical release as a weapon for purposes of causing casualties among the public and/or damaging property and the environment; (2) what effect would the public release of OCA data have on the possibility of a terrorist or other criminal attempting to cause such a chemical release; and (3) how would release of OCA data specifically over the Internet affect the likelihood of such a chemical release being attempted by a terrorist or other criminal. Our analysis concludes that posting most pieces of OCA information on the Internet would increase the risk of a chemical release caused by a terrorist or other criminal.

I. The Likelihood that a Terrorist or Other Criminal Would Attempt to Use an Industrial Chemical Release as a Weapon

Based upon our analysis of trends in international and domestic terrorism and upon the burgeoning interest in weapons of mass destruction (WMD) among criminals and other terrorists, we have concluded that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible. Increasingly, terrorists engineer their attacks to cause mass casualties to the populace and/or large-scale damage to property. Terrorists or other criminals are likely to view the potential of a chemical release from an industrial facility as a relatively attractive means of achieving these goals. In recent years, criminals have with increasing frequency attempted to obtain or produce WMD precisely because such weapons are engineered to cause wide-scale damage to life and property. However, traditional means of creating or obtaining WMD are generally difficult to execute. In contrast, breaching a containment vessel of an industrial facility with an explosive or otherwise causing a chemical release may appear relatively simple to such a terrorist. Therefore, someone seeking to cause the damage associated with WMD may instead seek to cause a chemical release from an industrial facility.

It is particularly noteworthy that there have been successful efforts by foreign militaries and certain terrorist groups indigenous to other countries to cause releases from industrial facilities using bombs. These efforts have in effect converted the facilities into makeshift WMD. Some of these releases have inflicted damage on surrounding communities. Moreover, the evacuations that were triggered by the attempted and successful releases of industrial chemicals produced panic and disruption among the targeted population. These are precisely the goals of a terrorist.

It is also important to recognize that certain types of facilities that are required to submit OCA information are preferred terrorist targets. For example, international and domestic terrorists have most frequently attacked U.S. military, federal and infrastructure facilities in the U.S. and abroad. Consequently, releasing information that could be used for targeting purposes about such facilities may render them more attractive to a terrorist. While security at some of these sites may ameliorate the concern that they will be targeted, no security is foolproof and not everyone intent on terrorist activity–especially those motivated by religious or ideological zealotry–will be dissuaded by security measures. The ubiquitousness of industrial facilities possessing toxic chemicals and their proximity to population centers also make them attractive targets for those interested in causing mass casualties or large scale property damage. Many industrial facilities that are required to submit OCA information are located in high-population areas and, therefore, are likely targets for terrorist activity. Of the nearly 15,000 facilities that have submitted OCA data, almost half report that over 1,000 people live in zones that could be affected by the release of toxic chemicals from those facilities. While not all of the individuals who live in such zones would likely be killed or injured by a chemical release, one of the worst terrorist incidents that the U.S. has experienced could result if even a fraction of them were; by comparison, 168 people were killed and 500 injured in the Oklahoma City bombing.

Our analysis recognizes the fact that the United States has in recent years become the prime target for international terrorists. In 1998, forty percent of all terrorist attacks that occurred

throughout the world were directed against the United States. During the past decade, international terrorists have not been content to attack U.S. interests abroad. The 1993 World Trade Center bombing, the subsequent conspiracy to bomb New York landmarks and transit ways, and the December 1999 interception of bombmaking material being carried across the Canadian border into the United States are vivid reminders that international terrorists are active on United States soil.

The concerns about the exploitation of OCA data for illicit purposes are further compounded by the prospect that domestic terrorists will use the data with disastrous consequences. The1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City illustrated with tragic clarity that the threat from domestic terrorists seeking to cause widespread damage and casualties cannot be discounted. Moreover, in regard specifically to attacks on industrial facilities, in the last two years alone there have been two incidents involving domestic terrorist groups planning to cause industrial chemical releases for terroristic purposes. In both cases, law enforcement intervened before the plans were implemented. Although such events are not common–and in years past may not even have been contemplated–we cannot discount the possibility that they may continue to occur, and perhaps occur with greater frequency than in the past.

Contemporaneous with the contemplated release of OCA data are the ongoing efforts by the federal, state and local governments to implement extensive and costly efforts to plan for, prevent, and respond to criminal, terrorist and WMD incidents. In recent years Congress has appropriated billions of dollars to guard against terrorist activities targeting United States citizens and interests. This Administration has also directed extensive and intense efforts in this area and to protect United States' interests against the increasing globalization of crime. The President has issued Presidential Decision Directives 62 and 63, focusing specifically on international crimes and the nation's infrastructure facilities, committing the government to protect such facilities because their disruption could cripple a city or an entire region of the country. Notably, infrastructure facilities comprise approximately 15% of the total number of facilities for which OCA data may be released. In the face of all of these and other efforts to protect against the threats posed by the modern era of crime, an unintended consequence of releasing OCA data may be to undermine the counter-terrorism measures being funded by Congress and being implemented at great cost and effort by federal agencies.

II. The Risk Associated with Public Dissemination of OCA Data

Having determined that there is a legitimate terrorist threat related to the use of industrial chemical releases as weapons, we have also concluded that public dissemination of certain portions of OCA data would create an increased risk that terrorists or other criminals will attempt to cause an industrial chemical release. OCA data would be helpful to someone seeking to cause such a chemical release because OCA data would provide "one-stop shopping" for refined targeting information, allowing terrorists or other criminals to select the best targets from among the 15,000 chemical facilities that have submitted OCA data. Such perpetrators would be able to assess the relative attractiveness of targeting particular facilities for attack based upon OCA data elements that would provide salient information. The distance that a toxic cloud of chemicals might travel, the numbers of people who might be harmed, and the environmental or public receptors (such as national parks, hospitals and schools) that could be affected are precisely the types of factors that a terrorist weighs when planning an attack.

We do not conclude that the release of all pieces of OCA data creates an increased risk. Rather, we find that the release of different OCA data elements pose varying degrees of risk. The release of OCA data pertaining to the distance to endpoint, the population within the distance to endpoint, the public and environmental receptors within the distance to endpoint, and the optional map or graphic illustrating a worst case or alternative release scenario (category one information) poses the greatest risk, because those data elements provide information that could be construed to estimate the precise body count and environmental harm that would be caused by a chemical release. Such information is increasingly central to the planning of terrorist attacks. The release of OCA data pertaining to the scenario information, the release rate and duration of release, the amount of chemical involved, and the endpoint for flammables (category two information) poses less risk than the data elements in category 1, but would nonetheless pose a risk because these data elements would be helpful to planning an industrial release. They would provide a rough sketch of the elements of a large-scale industrial release, like a worst case or alternative release scenario. Information about a facility's active and passive mitigation systems (category three information) would be of limited use to planning an industrial release but would likely be exploited by only relatively sophisticated terrorists. Lastly, the remaining pieces of OCA information pose practically no risk, because they are apt to be of no assistance to planning a chemical release.

Some of the pieces of OCA information identified above as helpful to planning a chemical release are already publicly available. For example, the information in category three is comparable to information that is available in portions of the RMPs that have been publicly released. Moreover, certain pieces of information in category two are also publicly available. However, none of the pieces of information in category one, which are the data elements that would be the most helpful for purposes of targeting or maximizing the potential harm of a chemical release, are currently available in as readily accessible and user-friendly form as OCA data. The information that is publicly available could only be assembled into comparable targeting information by someone possessing at least some degree of technical proficiency and background in the meaning and use of such information. Furthermore, the following category two data elements are not currently publicly available: the amount of chemical involved, scenario information, the release rate and duration of release for alternative release scenarios, and the endpoint for flammables for alternative scenarios.

III. Public Dissemination of OCA Data via the Internet

The method of dissemination and the degree to which OCA data are disseminated are of paramount concern to evaluating the risk posed by the release of OCA data. We conclude that among the methods of providing access to OCA data, Internet access poses the greatest risk that OCA data will be used in relation to an attempted industrial chemical release. The degree of risk varies depending upon which pieces of OCA data would be posted. If the OCA data that fall within category one, which represent refined targeting information, were posted on the Internet, it would be accessible to anyone anywhere in the world who has access to the Internet, including agents of hostile foreign countries. Such unmonitored dissemination of this data in a manner that permits users to obtain it anonymously greatly increases the risk of its misuse.

Providing OCA data in a manner that does not permit anonymity would reduce the risk that individuals interested in obtaining OCA data for illicit purposes would attempt to do so. However,

the Internet is incompatible with monitored dissemination. Various technological devices permit users of the Internet to browse the World Wide Web anonymously or under a pseudonym.

To the extent that posting OCA information on the Internet poses an increased risk of chemical releases caused by terrorists or other criminals, dissemination of OCA information in a manner that would permit it to be easily converted into an electronic format for posting on the Internet would raise similar concerns. Paper copies of OCA data could easily be converted into electronic format, possibly using a scanner and optical character recognition software, both of which are widely available and quite affordable. OCA information could then be easily posted on the Internet, where it would pose the risk discussed above.

I. BACKGROUND

We begin this assessment by providing an overview of the statute and regulations governing the development of RMPs and the dissemination of OCA data. Next, we present a discussion of national security and law enforcement issues, including the general vulnerability of the United States to terrorist attack. Third, we describe the potential dangers associated with a chemical release, and discuss the likelihood of such a release by a criminal or terrorist. Fourth, we analyze the ways in which criminals, terrorists and hostile governments have in past instances obtained and misused publicly available information. Fifth, we evaluate the risks of making OCA data available, including assessing what information is already publicly available and attempting to identify to what extent release of OCA data would increase the risk of criminal or terrorist activity toward chemical facilities. In short, this assessment evaluates the motive that criminals and terrorists would have to commit the crime; the means by which they could commit the crime (using a combination of publicly available data and, if available, OCA data), and the potential consequences of the crime. Given the motive and the means, we conclude that the risk will generally increase if OCA data are released, and will increase sharply if OCA data are released over the Internet.

A. The Chemical Safety Information, Site Security and Fuels Regulatory Relief Act

The 1990 amendments to the Clean Air Act (CAA) directed EPA to promulgate regulations that would require facilities possessing and handling more than a threshold amount of toxic chemicals and other regulated substances implement a Risk Management Program to reduce the likelihood and severity of chemical releases. The Risk Management Program is intended to reach the most hazardous toxic industrial chemicals and flammable substances. As part of the Risk Management Program, facilities are required to provide the EPA, states and local emergency planners with a risk management plan (RMP).

The RMPs that are mandated under EPA regulations must include the following information:

- an executive summary outlining the facility's RMP;
- identifying information about the facility, including its location, address and contact information;
- information about the chemical accidents that have occurred at the facility in the last five years;
- an accident prevention program;
- an emergency response plan; and
- an off-site consequence analysis (OCA).

OCA data consists of projections about hypothetical circumstances in which the most hazardous regulated toxic and flammable substances on premises are accidentally released into the

environment. In short, these data described the worst possible impact that a chemical release could have on the public and the environment around each facility. (OCA data are discussed more completely infra at 8.)

The CAA required that RMPs, including OCA data contained therein, be made publicly available. Furthermore, the Freedom of Information Act (FOIA) required that RMPs be made available in electronic format, if a citizen requested the OCA data in that form.[1] In 1997, the prospect of the OCA data being released to the public raised concerns among members of the national security community since OCA data could be used by terrorists or criminals to identify facilities from which to cause a chemical release that would result in the most harm to humans, property, and the environment. In response to such concerns, proponents of releasing the OCA data emphasized the benefits that would inure to the public from the release of OCA data. For example, EPA asserted that public release of information about chemical releases has prompted industry to adopt safer and more efficient practices.

Different segments of the federal government and various parties involved in the regulation of chemical facilities disagreed about the dissemination of OCA data. Some believed that posting OCA data on the Internet was the appropriate way to afford the widest possible public dissemination. Others objected to posting OCA data on the Internet because of concern that such unfettered dissemination would increase the risk of terrorists or saboteurs misusing OCA data.

Initially, the OCA data were to be made publicly available in June 1999. However, in early 1999, Congress held hearings on the issue and subsequently passed the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRA). Among other things, this statute exempted OCA data from FOIA for one year, thereby forestalling the public release of OCA data for a year from the date of enactment.[2] The President signed CSISSFRRA into law on August 5, 1999.

---

1 Availability of the information in electronic format was required by the Electronic Freedom of Information Act of 1996, codified as amended in various sections of 5 U.S.C. §552(f).

2 The amendment to the CAA also restricted dissemination of OCA data to only enumerated categories of individuals and limited their dissemination of OCA data. Currently, pursuant to CSISSFRRA "covered persons" may obtain "OCA information" for "official use." Covered persons include federal government officers and employees and their contractors; state government officers and employees and their contractors; local government officers and employees and their contractors; SERC and LEPC members and their contractors; police; paid and volunteer firefighters; and other emergency responders. In addition, CSISSFRRA will require that "qualified researchers" also obtain access to the OCA information. Furthermore, members of the public will also receive access to paper copies of OCA information.

The statute requires that the President, during the year following enactment of CSISSFRRA assess the increased risk of terrorism and other criminal activity associated with posting OCA data on the Internet, as well as the incentives created for the reduction in the risk of accidental releases by public disclosure of OCA data. By the end of that year (i.e., by August 5, 2000), the President must promulgate regulations governing the distribution of OCA data that to the extent possible minimize the risk of terrorism and other criminal activity while also achieving the benefits of reducing the likelihood of accidental chemical releases. Arriving at an appropriate balance of the risks and benefits associated with release of OCA data are the central goal of the regulations. If the regulations are promulgated within the one year period, OCA data will continue to remain exempt from disclosure under FOIA. Otherwise the OCA data must be disclosed in electronic form upon request and will likely end up posted on the Internet.

On January 27, 2000, the President delegated to the Attorney General the task of assessing the increased risk of terrorist and other criminal activity associated with posting OCA data on the Internet, and to the Administrator of the EPA the task of assessing the incentives created by public disclosure of OCA data. The President also delegated to the Attorney General and to the Administrator jointly the drafting of the regulations based on those assessments.

B. RMPs and OCA Data

Facilities handling more than a certain threshold of regulated toxic and flammable substances must submit an RMP to outline the facility's compliance with CAA regulations and to summarize the facility's hazard assessment, prevention program, and emergency response program. The RMP must include enough data to allow the EPA to determine through review of the RMP whether the source is in compliance with the CAA.

An RMP is comprised of nine parts. The first part is registration information for the facility that provides identification information such as the facility's location, the name of its owner, its parent company, and the regulated substances that are on site. Parts two through five of the RMP consist of OCA data, the substance of which is discussed below. Part six of the RMP is the facility's five-year accident history. Parts seven and eight contain descriptions of the facility's accident prevention program. Lastly, part nine has information on the facility's emergency response program.

The format of the RMP submission forms was designed to gather basic data from the facilities without requiring detailed documentation. Almost all responses on the RMP submission form are in the form of check-off boxes, "yes" or "no" answers, or numerical entries. The format was intended in part to enable the data to be assembled and easily downloaded or searched. EPA originally anticipated that States, communities, trade associations and public interest groups, among others, would have access to all RMP submissions, including OCA data, in searchable format.

OCA data, which comprise parts two through five of the RMP, consist of two categories of information, worst-case and alternative release scenario information. In addition, facilities must provide worst case and alternative release scenario information for two classes of substances, toxic chemicals and flammable substances. The worst-case scenario describes the results of a catastrophic release of the largest quantity of a regulated substance on site as a result of a vessel or process piping

failure. The worst-case scenario assumes that all active mitigation systems (such as sprinklers, scrubbers, and emergency shutdown systems) fail and only passive mitigation systems (such as dikes, berms, drains, sumps and enclosures) work to contain the release. Based upon such a scenario and a statistical model, the facility calculates the probable effects of such a release. These calculations reflect the size of the area and the number of people who would potentially be affected by a chemical release. They are also used to determine whether certain public buildings and/or environmental sites are within the affected area. It is generally agreed that the worst-case scenario is an unrealistic situation that is highly unlikely to occur, because some of the conditions assumed by the statistical model cannot occur.[3] Nevertheless, even damage far less than that projected by the worst case and alternative scenarios could be severe.

In contrast, the alternative release scenario represents a more realistic situation related to a chemical release. Under the alternative release scenario, the facility is allowed to take into account more likely circumstances that may arise during a chemical release. The alternative release scenario, by most accounts, represents a far more realistic assessment of the results of a chemical release.

Facilities must provide worst-case and alternative release scenario information for two classes of substances, toxic chemicals and flammable substances. In general, OCA data for flammable substances will not produce consequences that are as far reaching as those for toxic substances, since a plume of flammable substances will typically disperse to safe levels before traveling beyond the site of release. However, a flammable substance release may produce an explosion or fire that could cause extensive localized damage, although such explosions are reportedly rare.

The information that must be provided for the OCA portion of the RMP related to a toxic chemical worst-case scenario is as follows:

- the chemical involved in the worst-case scenario and the concentration of that chemical;
- the physical state (gas or liquid) of the chemical;
- the model used for the worst-case scenario projection;
- the scenario that produces the worst-case scenario (gas release or liquid spill and vaporization);
- the projected quantity of chemical released in the worst-case scenario, the release rate, and the duration of the release;

---

[3] For example, the area identified as potentially affected (the distance to endpoint) is based upon the assumption that the chemical plume would radiate equally in all directions at once. This is virtually impossible because of meteorological factors.

- the atmospheric stability during the worst-case scenario;[4]
- the topography of the surrounding area (urban or rural);[5]
- distance to end-point, or the distance that the chemical release will extend;
- the residential population within the affected area;
- the types of public receptors within the affected area (schools, residences, hospitals, prison/correctional facilities, recreation areas, or commercial/industrial areas);
- the types of environmental receptors within the affected area (national or state parks, forests, or monuments; officially designated wildlife sanctuaries, preserves, or refuges; federal wilderness area); and
- the types of passive mitigation systems considered.

The worst-case scenario differs slightly for flammable substances: it only includes one scenario describing the release and includes a flammable endpoint data element, which describes the type of damage that would result. The required alternative release scenario information for toxic and flammable substances also varies from the worst-case scenario information, principally in that it includes consideration of active mitigation systems as well as passive mitigation systems (sprinkler systems, deluge systems, water curtain, neutralization, excess flow valve, flares, scrubbers, and emergency shutdown systems), and the facilities have the option of altering the assumptions surrounding the alternative release.

Because the EPA believed that the RMPs should also provide the public with comprehensible information that would encourage discussion about issues related to accident prevention and preparedness, the RMP also includes an executive summary in plain-text that is intended to provide information to the public in a format that is more easily understood than the raw RMP data. EPA instructs facilities submitting RMP data to include a discussion of OCA data in its executive summary. However, EPA does not specify what elements of OCA data or the amount of detail that should be provided in the executive summary. A random search of fifty RMP submissions suggests

---

4 This data element concerns atmospheric conditions that affect the distance that a chemical plume will travel without dispersing. The greater the atmospheric stability the further the plume will carry with a high concentration.

5 Note that "urban" and "rural" are not used here as they are typically understood. They refer to whether there are any outcroppings in the surrounding topography. If there are objects such as buildings, structures, or trees in the surrounding area, the area is deemed "urban." In contrast, a flat, unobstructed landscape is considered to be "rural." This information is collected because the shape of the topography will affect the dispersion rate of a gaseous chemical.

that there is substantial variance in the amount of OCA information that is provided in the executive summaries that have been submitted to EPA. (See infra at 44).

In addition, CSISSFRRA requires that EPA make OCA information available to "covered persons" for official use and to "qualified researchers." However, these individuals are expressly restricted by CSISSFRRA from disseminating OCA data to the public except as provided by the statute. OCA data has been available to "covered persons" since the enactment of the statute. However, access by "qualified researchers" has not been permitted pending a determination by EPA as to the process by which such access should be permitted.

C. EPA's Current Internet Website

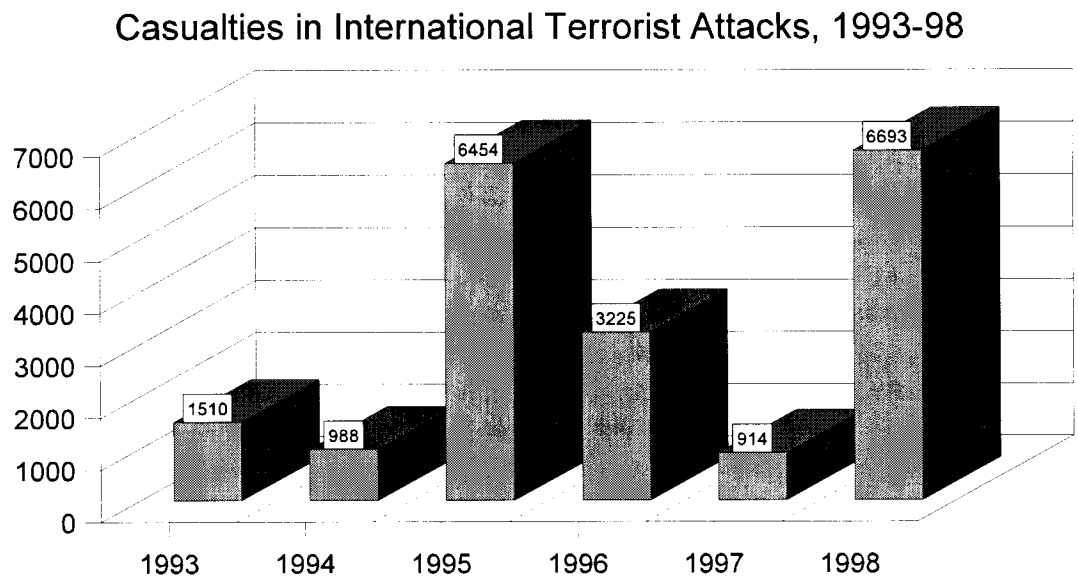
To date, nearly 15,000 RMPs have been submitted. EPA estimates that these 15,000 RMPs may constitute about 80 percent of the expected submissions.[6] Registration and identification information for each facility, the facility's five-year accident history, the facility's accident prevention program, its emergency response program, and the executive summaries, which include OCA data, are currently posted on the EPA website. That information is available to the public and fully searchable by various data elements, including location of the facility, regulated chemicals on site, and the five-year accident history. However, none of the OCA portions of the RMPs are currently posted. As discussed more fully infra at 47, the General Accounting Office (GAO) recently issued a report raising concerns about the vulnerability of EPA's computer network, including its website, to cyber-terrorism and other hacker attacks.

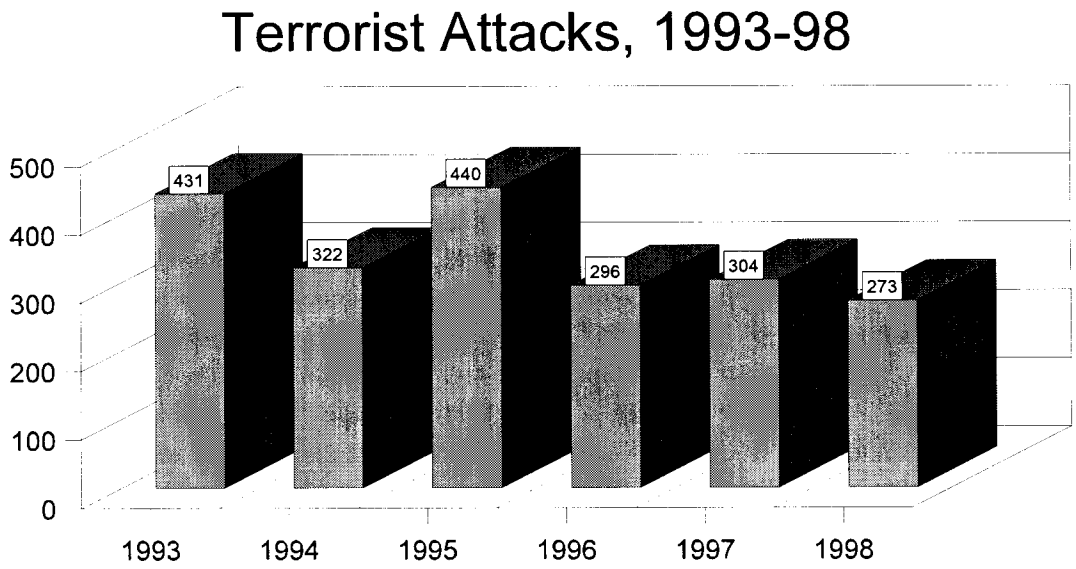
II. NATIONAL SECURITY ISSUES

An assessment of the increased risk of terrorist activity associated with disseminating OCA data must take into account the general vulnerability of the United States to terrorist attack. The concern about terrorism being directed against the United States or the United States' interests has escalated during the last several years. Even as the number of terrorist acts have declined in the world, the lethality of terrorist attacks has escalated. The State Department reports that the number of international terrorist attacks have generally declined since 1991. However, during the same period, the number of casualties from those attacks each year has fluctuated, peaking in 1998. Over a longer span of time, the trend in greater lethality is evident. According to a chronology of terrorist events compiled by the RAND Corporation and the University of St. Andrews, at least one person was killed in 29 percent of terrorist incidents in 1995. By comparison, only 17 percent and just 19 percent of terrorist incidents resulted in a single death during the 1970's and 1980's respectively.

---

6 Initially, the EPA estimated that approximately 30,000 RMPs would be filed. However, subsequent examination suggests that the original estimates may have been too high. EPA's discussions with its regional offices suggest that some facilities that would have been required to submit RMPs have opted instead to reduce the amount of regulated chemicals that they keep on site so that they no longer were subject to the CAA.





Terrorism experts attribute the increase in the lethality of terrorism to various factors. They include the terrorist's increased quest for attention, developments in terrorist weaponry, and the dramatic proliferation of terrorist groups motivated by religious zealotry.[7] Unfortunately, experts believe that the threat of terrorism is likely to increase in the foreseeable future. A report released in September 1999 by a federal advisory commission headed by former Senators Gary Hart and Warren B.

---

[7] See, e.g., Hoffman, Bruce, Inside Terrorism, Columbia University Press, 1999.

Rudman found that the threats from terrorism in the next 25 years is likely to increase and that the country "will be vulnerable to an increasing range of threats against American forces and citizens overseas, as well as at home."

It is also necessary to put the potentially catastrophic nature of a chemical release in perspective with terrorist attacks. As illustrated by the chart on page 29, almost half of the worst case scenarios for toxic chemicals (over 7,000) project that over 1,000 people live within the distance to endpoint. The potential consequences of the more conservative estimates based upon the alternative release scenarios still indicate that over a tenth of the submitted RMP facilities (1,669) project populations of over 1,000 people within the distance to endpoint. While not everyone within the distance to endpoint would be killed, injured, or even affected by a worst case or alternative release, injury to even a small proportion of those individuals would constitute one of the worst terrorist incidents in U.S. history. In contrast, the bombing of the Murray building in Oklahoma City killed 168 people and injured 500.

In the context of terrorist attacks that could be executed with the intent of causing maximum harm, the United States must be wary of making information available to terrorists or other criminals that would provide them with an increased ability to consummate their criminal intentions. Public dissemination of OCA information for the 15,000 chemical facilities located throughout the United States that have submitted RMPs could enable terrorists and other criminals to focus their efforts on specific U.S. targets and hone their destructive intent to maximum effect. Thus, in crafting any regulation permitting public disclosure, we must carefully assess the extent to which the potential risk of harm weighs against the benefits to be derived from providing this information.

A. The Threat from International Terrorism

In the post-Cold war era, the United States' unique position on the world stage as a military and economic leader has increasingly made it a primary target of international terrorists. In 1998 alone, forty percent of all terrorist attacks (111 attacks) throughout the world were directed against the United States.[8] The FBI's International Terrorism Operations Section currently tracks an average of ten threats per week against U.S. interests emanating from abroad.

A chilling reminder of the depth and intensity of terrorists' animosity toward the United States appeared only recently in the "fatwa" or Muslim religious decree that the terrorist Usama bin Laden and allied groups issued on February 23, 1998 (and reaffirmed in May 1998) calling for all Muslims to wage a holy war on U.S. citizens and interests.[9] The threat of attack represented by this

---

[8] Patterns, page 1.

[9] The fatwa was signed by such terrorist groups as al-Jihad and al-Gama' at al-Islamiyya. Several militant groups have also vowed revenge against the U.S. for the missile strikes on terrorist training camps in Afghanistan. 1998 Patterns of Global Terrorism, United States Department of State, page 10 (hereinafter "Patterns").

"fatwa" is real, as recent events show. Based on the fatwa, bin Laden's agents committed simultaneous bombings of U.S. embassies located in Kenya and Tanzania in August 1998, resulting in over 300 fatalities and over 5,000 injured. In the wake of the embassy bombings, the United States launched the most extensive overseas criminal investigation in U.S. history, and, as a result, indicted Usama bin Laden and 14 of his associates. Currently, Usama bin Laden remains free, under the shelter of the Taliban regime in Afghanistan. The threat posed by UBL to the United States is particularly relevant to this assessment given his reported attempts to obtain chemical and biological weapons for use in his "jihad," or holy war, against the United States.

Acts of terrorism perpetrated by international terrorist groups have also taken place in the United States. In February 1993, international terrorists demonstrated their ability to reach inside United States borders when they bombed the World Trade Center office building in New York City, killing five people and injuring more than 600. Investigation revealed that these bombings were only one piece of the war of urban terrorism against the United States that Sheik Omar Abdel Rahman and his co-conspirators were plotting to wage in 1993. These terrorists had also taken steps to plan and carry out the bombing of numerous other New York City landmarks and public facilities, including the U.N. building, the Holland and Lincoln tunnels, and a Manhattan bridge. Only the arrests of the conspirators prevented the scores of additional casualties and widespread destruction that would have resulted from their plans. Law enforcement intervention also prevented bombings in July 1997 that would have targeted the subway system in Brooklyn, New York. Two Palestinian men were arrested in an explosives-laden apartment. They were believed to have been planning to bomb the busy Atlantic Avenue transit station, which adjoins a Long Island Rail Road terminal in Brooklyn.

More recently, just before the past New Years, an individual with links to terrorist organizations was intercepted by U.S. Border Control entering the U.S. with materials that could be used to construct a large bomb. He was charged in federal court with commission of an act of terrorism transcending national boundaries.

As we enter the next millennium, the United States and other countries face a new era of increased globalization and technological advances. Already these advances have strengthened our connection with other countries through transnational agreements and international travel; at the same time, they have exposed the United States to unprecedented vulnerabilities. Moreover, the extensive U.S. cultural, political, economic and military presence abroad, in conjunction with opposition by certain foreign groups and governments to United States policies and actions, continues to make U.S. citizens and interests prime targets for international terrorists.

B. The Threat from Domestic Terrorism

The threat posed by domestic terrorists against the United States government's interests and citizens is comparable to that posed by international terrorism. On average, the FBI responds to five threats each week emanating from domestic terrorists, or two hundred and sixty per year. During fiscal year 1998, FBI investigative actions successfully thwarted twelve full plots involving the commission of terrorist attacks within the United States.

The April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City–the most deadly act of terrorism in U.S. history–revealed the United States' vulnerability to attack from domestic terrorists. Equally as disturbing as the destructive force of the Murrah building attack was its indiscriminate nature. The 168 killed and over 500 injured included not just members of the military and other government workers, but also scores of children in the daycare center located at the site. The realization that such vast destructiveness could be caused merely by the actions of one or two individuals, acting alone, with relatively rudimentary bombing tools at their disposal was disquieting.

Subsequent bombings, such as the 1996 bombing at the Atlanta Summer Olympics, numerous abortion clinic bombings, and the 1997 planned bombing attack by North American Militia members on federal buildings and a highway interchange have also thrust a spotlight on terrorism perpetrated by the home grown terrorist. These troubling events are hardly anomalous. Numerous other attacks have been perpetrated by domestic terrorists against government facilities in recent years. For example, in December 1995, in Reno, Nevada, two construction workers attempted to bomb the Reno, Nevada, office of the Internal Revenue Service (IRS) using a bomb made of about 100 pounds of fertilizer and kerosene. Fortunately, the triggering mechanism failed and the bomb did not ignite. According to authorities on the scene, many deaths and injuries would have occurred had it gone off. A year later, in January 1996, a bomb exploded outside of a U.S. Forest Service headquarters in Espanola, New Mexico, causing $25,000 damage to the offices but no injuries. A Forest Service employee in Nevada has been targeted twice. Further, in August 1996, in Austin, Texas, a defendant was sentenced to more than 20 years in prison for plotting to bomb the office of the IRS in Austin. The defendant was convicted on six counts of explosives and firearms violations. Evidence presented at the trial showed that he had planned to plant more than a thousand pounds of explosives in the IRS service center.

The organizations and other terrorist interests responsible for these bombings or similar bombings and attempted bombings have demonstrated an interest in obtaining chemical and biological agents. For instance, in March 1995, two members of the anti-tax Minnesota militia known as the Patriots Council, were convicted of making an illegal batch of ricin, a toxic derivative of the castor bean. The evidence at the trial showed that they planned to use the ricin against law-enforcement officers who had served legal papers on members of the group. In August 1989 indictments were returned against two additional alleged conspirators. According to trial testimony, members of the group planned to poison U.S. agents by placing ricin on doorknobs of their building and to blow up a federal building.

Domestic terrorist groups have also sought to attack the U.S. infrastructure. In December 1999, federal agents in Florida and Georgia arrested two men in connection with a plan to steal explosives from National Guard armories and blow up energy facilities in the Southeast. One of the defendants was the leader of a state militia group located in the Southeast, formed to launch "violent acts of retaliation" against government facilities and personnel.

C. Trends in Terrorism involving Weapons of Mass Destruction

In addition to the generally elevated level of the terrorist threat confronting the United States, as the Oklahoma City and African Embassy bombings so grimly demonstrated, there is an increased willingness of terrorists to carry out more large-scale incidents designed for maximum destruction."[10] That willingness is evidenced by the increased interest of terrorist groups, both domestically and abroad, in acquiring chemical, biological and nuclear WMD.[11]

Intelligence agencies have predicted that terrorist use of chemical or biological materials will increase over the next decade.[12] FBI Director Louis Freeh has stated that "the most potentially devastating threat facing the United States as we enter the next century is the terrorist use of weapons of mass destruction (large conventional explosive, chemical, biological, radiological or nuclear devices)."[13]

WMD are particularly attractive to terrorist organizations.[14] WMD's ability to harm a significant number of individuals and create panic renders their use, or mere threatened use, by terrorists ideal for purposes of intimidating, influencing, or coercing a government or civilian population.

---

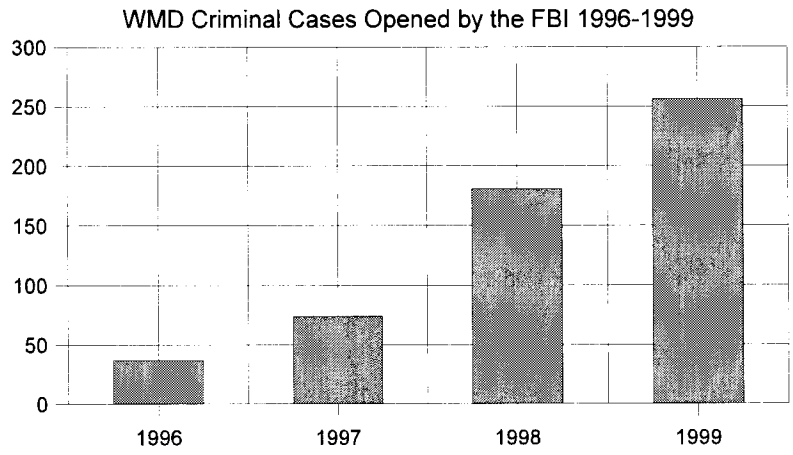
10 Statement for the record of Louis J. Freeh, Director, Federal Bureau of Investigation, before the United States Committee on Appropriations, Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, February 4, 1999, (hereinafter "Freeh Congressional Statement, Feb. 4, 1999), page 6.

11 Federal law and the Department of Justice define a WMD as any destructive device as defined in 18 U.S.C. 921, which includes, inter alia, explosive, incendiary, or gas devices; any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; any weapon involving a disease organism; or any weapons that is designed to release radiation or radioactivity at a level dangerous to human life.

12 GAO Report,"Combating Terrorism: Need for Comprehensive Threat and Risk Assessments Focused on Chemical and Biological Attacks," (GAO/NSIAD-99-163, September 7, 1999)(hereinafter "GAO Report on Terrorism"), page 17.

13 Freeh Congressional Testimony, Feb. 4, 1999, page 18.

14 While there is no universally accepted definition of "terrorism," federal law and the FBI define "terrorism" as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." In the same vein, the FBI defines "domestic terrorism" as the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction and whose acts are directed at elements of the U.S. Government or its population, in furtherance of political or social goals.



Domestically, the FBI has seen a marked increase in the number of cases involving WMD, primarily in cases involving the threatened use or procurement of chemical and biological materials with intent to harm. Internationally, as the State Department notes, terrorist groups are "known to be interested in utilizing (or in some cases have actually employed) chemical, biological, radiological or nuclear materials in their anti-U.S. operations for the specific purpose of creating mass casualties and inflicting long-term damage."[15] Since Aum Shinrikyo, a Japanese doomsday cult, released sarin nerve gas on the Tokyo subway in March 1995, killing 12 people, terrorist incidents involving chemical or biological agents have increased. Before the late 1990s, the FBI investigated roughly a dozen cases per year involving chemical, biological, radiologic, or nuclear materials. In contrast, the FBI opened 74 such investigations in 1997 and 181 in 1998. The trend continued in 1999, during which the FBI investigated over 280 such cases. Although 80 percent of the incidents in 1997 and 1998 were hoaxes involving only the threatened use of such agents, some of remaining incidents were in fact unsuccessful attacks. In any event, the use of toxic chemical and biological agents in criminal incidents is on the rise. Intelligence agencies believe that the possibility that terrorists will use chemical or biological materials may increase over the next decade. The CIA also asserts that interest among non-state actors, including terrorists, in both biological and chemical materials is real and growing.

The FBI has ranked groups of agents according to the likelihood that they would be used. Currently, the FBI assesses chemical and biological threats as follows:

1. Biological Toxins: Any substance of natural origin produced by an animal or plant.

---

[15] Letter dated November 12, 1999 of Ambassador Michael Sheehan, Coordinator for Counterterrorism, Department of State.

2. Toxic Industrial Chemicals:[16] Chemicals developed or manufactured for use in industrial operations such as manufacturing solvents, pesticides, and dyes.

3. Biological pathogens: Any organism such as a bacteria or virus capable of causing serious injury or death.

4. Chemical agents:[17] A chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate people.

According to a recent General Accounting Office report, Combatting Terrorism: Need for Comprehensive Threat and Risk Assessment of Chemical and Biological Attacks, GAONSIAD-99-163 (September 1996), toxic industrial chemicals are considered by experts from the scientific, intelligence, and law enforcement communities to be an attractive instrument for those who would seek intentionally to do considerable harm to the public. In contrast to many chemical or biological agents, industrial chemicals can cause mass casualties while requiring little if any expertise or sophisticated methods to obtain and adapt to terrorist use, in contrast to many chemical or biological agents. In regard to the threat of chemical and biological terrorism, Henry L. Hinton, Assistant Comptroller General, National Security and International Affairs Division, provided the following testimony to Congress in regard to GAO's report:

> According to the experts we consulted, in most cases terrorists would have to overcome significant technical and operational challenges to successfully make and release chemical or biological agents of sufficient quality and quantity to kill or injure large numbers of people without substantial assistance from a state sponsor. With the exception of toxic industrial chemicals such as chlorine, specialized knowledge is required in the manufacturing process and in improvising an effective delivery device for most chemical and nearly all biological agents that could be used in terrorist attacks.
>
> * * *
>
> Some chemical agents are commercially available and require little sophistication or expertise to obtain or use, but other chemical agents are technically more challenging to make and deliver. Toxic industrial chemicals such as chlorine, phosgene, and

---

[16] An "industrial chemical" is a chemical developed and manufactured for use in industrial operations or research by industry, government, or academia. Industrial chemicals are not manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by humans.

[17] The term "chemical agent" means a chemical substance that is intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects.

hydrogen cyanide are used in commercial manufacturing and could easily be acquired and adapted as terrorist weapons. (Emphasis added)

Testimony of Henry L. Hinton, Jr., October 20, 1999 before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives.

Some industrial chemicals, like chlorine and phosgene, are considered by chemical, intelligence, and law enforcement experts to be particularly dangerous because they are "choking agents" similar to ones used in modern chemical warfare.[18] Some choking agents are readily available because they are commonly used in manufacturing processes, making them convenient components of a makeshift WMD. Chlorine was the second most reported chemical in the RMPs that have thus far been received by EPA. Over 5,000 facilities reported that they used it. Further, chlorine was the second most mentioned chemical in relation to worst-case scenarios, accounting for 30% of the total worst case scenarios.

D. The Growth of the Internet and Threats to Our National Security

The far-reaching and ever more rapid advances in computer and software technology over the last ten years have combined with the explosive growth of the Internet to dramatically alter the manner in which we communicate and interact. As the Attorney General recently noted, "[w]ith breathtaking speed the Internet has nearly doubled in size every year since 1990. By 2003, the number of Internet users worldwide is projected to be five hundred and two million people."[19] The Attorney General also observed that although the Internet has brought us "splendid tools of wonder," it has also brought a dark side, including the vulnerability of our nation's infrastructure to cyber-terrorism: "Our nation's infrastructure, including the banking system, the stock market, the electricity and water supply, telecommunications network, and critical government services such as emergency and national defense services, all rely on computer networks."[20] Today, our national policy on how best to protect our national security from threats via the Internet (e.g., attacks on our critical infrastructures), is still evolving.

During the last several years, the threat against these critical infrastructures has become increasingly apparent. For example, in December 1999, the FBI arrested a militia leader plotting to

---

[18] A "choking agent" is a substance that causes physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is "choked."

[19] Remarks of the Honorable Janet Reno, Attorney General of the United States, to the National Association of the Attorneys General, Jan. 10, 2000 (hereinafter "NAAG Speech, , Jan. 10, 2000") pages 1-2.

[20] Id.

destroy a power installation in Florida using explosives stolen from National Guard armories. Other efforts by domestic terrorists have also targeted infrastructure facilities.

As discussed more fully at pages 29 infra, approximately 15 percent of the infrastructure facilities across the country are among the group submitting OCA data, including water supply and irrigation facilities; military installations; utility companies; natural gas distribution, and facilities related to the generation, transmission or control of electrical power. Disruption of even one of these facilities could wreak havoc on an entire region or locality. But the risk to national security is greatly heightened by the nature of the chemicals at use in the facilities that submit RMPs–not only could a criminal or terrorist accomplish the kind of disruption of a region or locality usually feared in the case of attacks on critical infrastructure, but he or she could also potentially compound the terroristic effect by causing the deaths of and injuries to people in the surrounding area.

E. The United States' Response to These Threats

The increased vulnerability of the United States to terrorist attacks in the post-Cold War era has prompted extraordinary efforts by the federal government to prepare for and prevent such attacks. The federal government's efforts to address the vulnerability of the nation's infrastructures intensified in 1995 under Presidential Decision Directive (PDD) 39, when the Attorney General chaired a Cabinet Committee to assess and recommend measures to protect these infrastructures. Based on this Committee's recommendations, the President's Commission on Critical Infrastructure Protection also known as the Marsh Commission, working under the direction of the Steering Group chaired by the Attorney General, addressed this issue. On May 22, 1998, following the Marsh Commission report, the President announced the signing of PDD 62 and 63 on combating terrorism and protecting critical infrastructure. These provisions built upon U.S. counter-terrorism policy and measures outlined in PDD 39. PDD-62 created a new and more systematic approach to fighting the terrorist threat of the next century by reinforcing the mission of the many U.S. agencies charged with roles in defeating terrorism; it also codified and clarified their activities in the wide range of U.S. counter-terrorism programs, from apprehension and prosecution of terrorists to increasing transportation security, enhancing response capabilities and protecting the computer-based systems that lie at the heart of America's economy.

PDD-63 generated an unprecedented effort to protect our nation's critical infrastructure. This included the establishment in 1998 of the inter-agency National Infrastructure Protection Center (NIPC) at the FBI and the creation of specially-trained computer squads in 16 field offices, as well as a host of other FBI teams dedicated to the counter-terrorism effort. Moreover, each of the 97 U.S. Attorneys Offices around the country are staffed with specially trained "Computer and Telecommunications Coordinators" (CTCs), as well as specially trained "Crisis Management Coordinators" (CMCs) to respond to cyber and terrorism attacks. These federal efforts are augmented by similarly extensive efforts in other federal agencies, and by state and local agencies and departments.

The magnitude of the federal, state, and local government's effort to prevent and prepare for terrorist attacks, including those that use chemical weapons, is illustrated by the number and breadth of initiatives undertaken for that purpose, including: the ongoing development in 120 cities of rapid

terrorism response teams for WMD incidents; the development by the Department of Health and Human Services (HHS) of Metropolitan Medical Response Systems (MMRS) in local jurisdictions across the United States; the development by the Federal Emergency Management Agency (FEMA) and the Office of Justice Programs (OJP) of training programs for emergency first responders to WMD incidents; the establishment of national training centers for emergency responders; and the creation of the National Domestic Preparedness Office (NDPO) to coordinate the numerous federal programs providing weapons of mass destruction-related domestic preparedness assistance to state and local jurisdictions.

As even the partial listing of the above-described WMD initiatives indicates, the federal government has expended billions of dollars in recent years on efforts to prepare for the possibility of terrorist attacks in the areas of weapons of mass destruction and on critical infrastructure protection. GAO figures indicate that the President has proposed $10 billion for counter-terrorism programs for fiscal year 2000, an increase of more than $3 billion over the $6.7 billion requested for fiscal year 1999. Of the $10 billion, $8.6 billion is for combating terrorism, including defending against WMD, and $1.4 billion is for critical infrastructure protection.[21] Moreover, for fiscal year 2001, the Justice Department has again requested budget increases to augment its fight against terrorism and to address hostile intelligence activities.

The federal government has been no less active in its efforts to address the potential increase in crime that may arise from the advent of the Internet. Through efforts like the creation of the FBI's NIPC and the interagency efforts of law enforcement agencies, the Department of Defense, the Intelligence Community, and federal agencies with infrastructure-focused responsibility such as the Departments of Energy and Transportation, there has been a consolidated effort to protect the nation's infrastructure from the potential perils of cybercrime.

These efforts are reflected in the Department's budget priorities. In fiscal year 2000, Congress is providing a total of $106 million in funding for cybercrime efforts underway in the Department's Criminal Division, the FBI, DEA, U.S. Attorneys Offices, and the Office of Justice Programs. The Department has sought an increase for fiscal year 2001 of an additional $37 million to continue the fight against cybercrime. These enhancements will increase the Department of Justice's funding base for computer crime by 28 percent, for a total of $138 million.

To put it simply, the government's counter-terrorism policy initiatives and extensive efforts to protect itself from the threat of terrorism and cybercrime could be seriously undermined by the dissemination of OCA data over the Internet. Given the terrorist threat facing the United States both here and abroad, the U.S. should exercise extreme caution in releasing information that would assist those with terrorist intent. Similar concerns prompted Congress to enact legislation in 1999 that

---

[21] GAO Report on Terrorism, page 1. For the FBI alone, the annual funding for the Counterterrorism program has increased from $78.5 million in 1993 to $301.2 million in 1999. Freeh Congressional Testimony, Feb. 4, 1999, page 1.

would render it illegal for someone to provide information on the manufacture of destructive devices or WMD with the intent to further a crime.

III. THE POTENTIAL DANGERS AND THE LIKELIHOOD OF A CHEMICAL RELEASE CAUSED BY A CRIMINAL OR TERRORIST

Both the EPA and the Department of Justice agree that a release of toxic industrial chemicals–whether as a result of accidental or criminal activity–could have dire consequences. The intentional release of methyl isocynate gas from a chemical plant in Bhopal, India, in 1984 was reportedly responsible for nearly 2,500 deaths and thousands of injuries. The explosion of a storage tank in Qingdao City, China, in 1997 released a cloud of chlorine gas that injured over 1,000 workers. While there has been no chemical release in the United States that has resulted in comparable injury to life or property, smaller incidents have occurred that have resulted in fatalities and have underscored the dangers of industrial chemical accidents and toxic releases: in 1990, an explosion at a chemical plant in Texas killed 17 people; in 1998, an explosion at a chemical plant in Reno, Nevada, killed four and injured six; and in July 1999, an explosion at a chemical plant near New Orleans injured 15 workers.

While there has been no confirmed terrorist or criminal act responsible for such loss of life, an intentional act that targets a facility and results in a chemical release could prove catastrophic.[20] The fact that chemical releases have occurred with deadly results because of accident or negligence affirms that such consequences could possibly result from intentional criminal acts. We believe that it is possible that large chemical releases could be triggered by criminal activity. Further, we found that an attempt to cause an industrial chemical release would be consistent with both the tactics and the goals of terrorist organizations.

A. The Likelihood that Someone Could Cause a Toxic Industrial Chemical Release

1. Terrorists and Other Criminals Have Considered Using Chemical Releases from Industrial Facilities as Weapons

Although unlikely to deter someone from actually attempting to use an industrial chemical release as a weapon, we recognize that there are several factors that may undercut the effectiveness of using a chemical release as a weapon. Some chemicals will ignite if released by an explosion; some burning chemicals are robbed of their lethality. In fact, igniting toxic chemicals escaping from a container, like a tank car or a holding tank, is a method of containment called "vent and burn" used

---

[20] We are not including in our assessment one incident that resulted in a terrorist claim of credit. On July 5, 1990, 17 workers were killed during an explosion at the ARCO chemical plant in Texas. The fatalities were the result of a tank containing waste water materials that exploded, causing physical devastation in a one block area. Initially, an Islamic extremist group claimed responsibility for the explosion. However, the ensuing investigation was inconclusive as to the cause of the explosion.

by emergency responders to stanch a leak of hazardous chemicals. Further, some containment containers have safety features intended to prevent accidental releases. Moreover, directing an industrial chemical release toward a particular site that is not in close proximity to the emitting facility would be difficult, if not impossible; there are multiple uncontrollable variables that would affect the dispersal of a toxic plume, such as wind and humidity.

Our conclusion that such disincentives do not sufficiently deter is born out by the fact that individuals have indeed attempted to use chemical releases from industrial facilities as makeshift WMD both domestically and abroad. Some of these events have involved countries or factions hostile to the United States.

Internationally, there have been several incidents involving the attempted release of toxic industrial chemicals. During the recent war in Croatia, Serbian forces attempted to use releases from chemical facilities in conjunction with "ethnic cleansing" efforts. One of the most noteworthy examples was the repeated attacks by Serbian forces on the Petrochemia plant in the town of Kutina, located in the western Slavonia sector of Croatia. The Petrochemia plant produced fertilizer, carbon black, and light fraction petroleum products. Hazardous substances produced or stored at the plant included ammonia; sulfur; nitric, sulfuric, and phosphoric acids; heavy oil; and formaldehyde. The town of Kutina was less than 1 kilometer from the plant and atmospheric contaminant modeling conducted by the Croatian government indicated that a massive fire at Petrochemia would pose a danger to public health across a 100-kilometer radius, extending into Bosnia, Hungary, Slovenia, and Italy. Serbian forces attacked the plant on six occasions during 1993-1995. In response to the attacks on the chemical plant, Petrochemia prepared a detailed report to the United Nations Security Council recommending that the definition of chemical warfare be changed to include attacks on chemical industries. On another occasion, a natural gas refinery in the city of Ivanic, in eastern Slavonia, which produces ethane, propane, and butane and was located 1 kilometer from the center of the city was attacked with rockets containing cluster bombs. Attacks were also launched against pesticide plants in Croatia's industrial center at Sisak and a pharmaceutical factory that used ammonia, chlorine, and other hazardous chemicals located in Zagreb, the capital of Croatia. Again, these facilities were in close proximity to population centers and appeared to have been chosen for that reason. In yet another incident, according to 1995 press accounts, terrorists linked to Chechen rebels had planned to blow up the Polymer Material Works in Budennovsk, Russia, to cause an ecological disaster in the region.

In the United States, we have been fortunate not to have suffered any casualties from the intentional release of industrial chemicals for purposes of causing mass casualties. However, it is indisputable that individuals bent on causing large scale damage have considered using chemical releases from industrial facilities. There have been two instances in just the past two years in which individuals have plotted to use industrial releases from facilities to cause widespread harm. Most recently, in Sacramento, California, the FBI Joint Terrorism Task Force arrested two anti-government militia members in an alleged plot to blow up a large propane storage facility. The facility stored approximately 24 million gallons of liquefied propane fuel and was located about a

mile from a residential subdivision. Had the defendants' plan been implemented, it could have resulted in extensive damage and loss of life.

In a separate event that took place in early 1997, three men and a woman conspired to blow up a gas refinery in Bridgeport, Texas, releasing what they thought would be a lethal cloud of hydrogen sulfide gas in an effort to kill police officers who would come to investigate a telephone bomb threat. During the commotion caused by the chemical release, they hoped to rob an armored car in the nearby town of Chico of $2 million and use the money to finance other terrorist activities. Fortunately, an informant provided the authorities with information about the group and they were arrested before acting on their plan.

The difficulty inherent in predicting the path of a chemical release may hinder its use as a weapon. However, such considerations may only limit the purpose for which a chemical release is caused rather than dissuading someone altogether from using a chemical release for malevolent purposes. For example, an industrial chemical release is not likely to be used as a means of attacking a particular site, unless that site were in close enough proximity to the facility to assure that it would be affected by the release. It is more probable that a chemical release would be used for the broader terroristic purposes of indiscriminately killing, harming, or threatening people in the surrounding community and damaging their property (i.e., a chemical release is more likely to be used as a blunt tool rather than as a surgical instrument). Moreover, the fact that industrial facilities are numerous may compensate for the difficulty of directing a chemical plume in a particular direction. The number of facilities from which a terrorist or criminal may choose to cause a release of toxic chemicals or flammable substances provides for numerous sites of release.

Even if not ultimately lethal, a chemical release would still cause widespread disruption, panic, and fear. Eliciting fear among the general public is exactly the type of assault on the public psyche that is consistent with terrorism. This may offset a terrorist's concerns over limitations related to the inability to direct a chemical release. As the Advisory Panel to Assess the Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction recently stated in its first report to Congress:

> Terrorism, in essence, is a form of psychological warfare. The ultimate objective is to destroy the structural supports that give society its strength by both showing that the government is unable to fulfill its primary security function and, thereby, eliminating solidarity, cooperation, and interdependence on which social cohesion and functioning depend. Viewed in this context, even a "limited" terrorist attack involving [WMD] would have disproportionately large psychological consequences, generating unprecedented fear and alarm throughout society. (Footnotes omitted)

First Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, at p. 22 (December 1999).

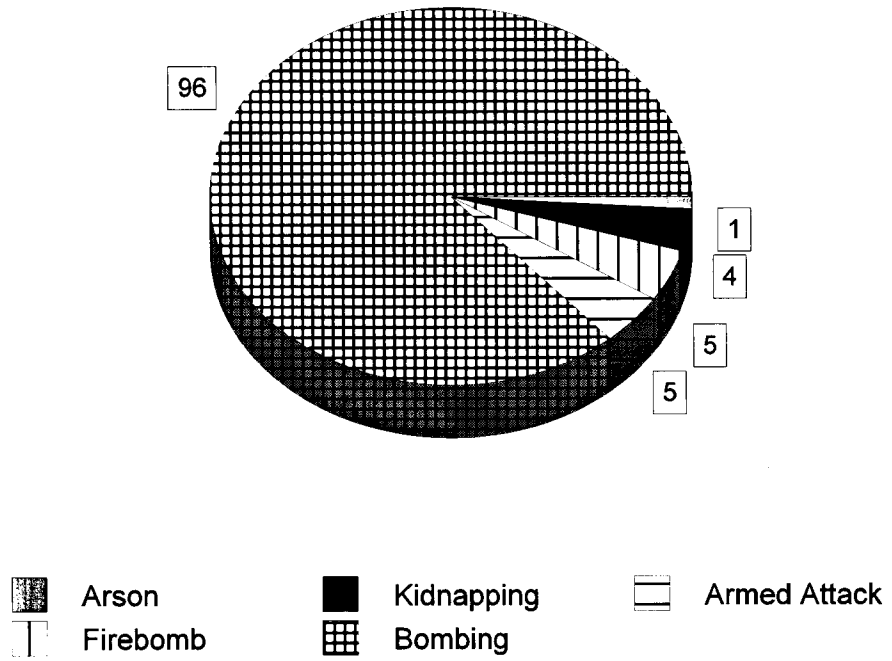
2. The Feasibility of a Criminal or Terrorist Causing a Release of Toxic or Flammable Industrial Chemicals[21]

Our discussions with experts in container breaches have suggested that breaching a hazardous material container using conventional explosives is feasible. While there are multiple methods of possibly breaching a containment vessel (one scenario considered by EPA in a 1995 study involved a plane crashing into a tank), explosives are the most likely means to be employed by terrorists. Among terrorist attacks committed in 1998 against U.S. citizens or facilities, explosives were by far the preferred method of attack. It is also one of the most obvious means of attempting to rupture a large metal vessel. Furthermore, use of a conventional explosive for purposes of causing an industrial release that would harm the public would be a force-multiplier–the scale of the damage and the amount of disruption that could be caused by an explosive that causes a chemical release in a public place could surpass the effects of the same conventional explosive alone.

---

[21] This assessment does not limit itself to considering whether a criminal or terrorist attack produces a chemical release identical to that projected by the worst case or alternative release scenarios. The likelihood of human casualties on a par with the projected population within the distance to endpoint in the worst case or alternative scenario projections is slim. Those figures are based upon the total number of individuals who live within the distance to endpoint rather than a projection of the number who would be affected by a chemical release. EPA has suggested that approximately one-sixth to one-tenth of the area within the distance to endpoint would likely be affected by a chemical plume projected under the worst-case or alternative release scenarios. Nonetheless, even if a fraction of those who live or work in a distance to endpoint were affected, that discounted figure could constitute a terrorist event of unprecedented scale in the United States. As noted above, almost half of the RMP facilities reported that over 1,000 people live within their distance to endpoints. This assessment also takes into consideration the collateral disruption and long term damage that could be caused by a chemical leak. Such leaks may trigger large scale evacuation that would provoke exactly the sort of panic and fear intended by terrorists. Further, release of some chemicals could have long-term health and environmental ramifications.

Type of Terrorist Attacks in 1998



It is noteworthy that chemical tanks have been intentionally ruptured during attacks involving explosives and have resulted in chemical releases, some of which have produced grave damage. Serbian attacks on some industrial facilities attacks did result in the release of toxic chemicals. Fortunately, large evacuations took place in advance. An attack upon a chemical plant in Jovan resulted in the release of 72 tons of anhydrous ammonia. Thankfully, that plant was located 30 km from the town and local public safety officials had time to evacuate its 32,000 residents.[22] Successful chemical releases have also occurred in other countries. In December 1995, members of the Revolutionary Armed Force of Colombia (FARC), Colombia's largest guerrilla group, blew up a pesticides warehouse in Une, Colombia, resulting in large volumes of toxic materials being released into the air. Approximately 9,000 people living in the vicinity of the warehouse were evacuated in order to prevent mass poisoning from the toxic emissions. It is noteworthy that FARC has sympathizers in the United States and the FARC in Colombia has threatened U.S. air carriers.

---

[22] Examples of the Serbian military's efforts to create chemical releases are particularly troubling because terrorist organizations sympathetic to Serbian causes are currently operating in the United States.

Components of the U.S. government have also considered the possibility of a release of toxic chemicals from an industrial facility to be a credible threat in U.S. interests. In 1995, EPA and an LEPC (Local Emergency Planning Committee) recognized the potential dangers of chemical releases resulting from terrorist activity and factored the possibility of a terrorist threat into their assessment of safety at facilities storing anhydrous ammonia in the Tampa Bay area.[23] In addition, the Agency for Toxic Substances and Disease Registry (ATSDR), a branch of the Centers for Disease Control and Prevention, has recognized the threat posed by attacks on chemical facilities and, in response, devised a ten-step procedure for analyzing, mitigating, and preventing public health hazards resulting from terrorism involving industrial chemicals. It is noteworthy that among the "soft targets" that the ATSDR identified as potential terrorist sites were chemical manufacturing plants (chlorine, peroxides, other industrial gases, plastics, and pesticides); compressed gases in tanks, pipelines, and pumping stations; and pesticide manufacturing and supply distributors. OCA data contains information about many such "soft targets." For example, there are 68 pesticide and other agricultural chemical manufacturing facilities that have submitted RMPs.

There has yet to be a toxic chemical release from a facility in the U.S. as a result of terrorist or criminal activity. The predictive value of this fact is limited, however. First, in contrast to the lack of terrorist incidents aimed at industrial chemical releases during the entire history of the United States, in the last two years alone law enforcement thwarted two attempts to cause such a chemical release. These recent events suggest that there may be a change in trends relating to such crimes and that the past may not be the most reliable barometer of future events in regard to criminal and terrorist efforts to cause mass damage and casualties through means that may include toxic industrial chemical releases.

B. Industrial Facilities Are Attractive Targets to Terrorists and Criminals

Industrial facilities such as those that have submitted RMPs may be attractive targets for criminal and terrorists intent on causing massive damage. First, many such facilities exist in well-populated areas, where a chemical release could result in mass casualties and would result in widespread disruption. Many of the facilities that submitted RMPs reported significant populations living within their distance to endpoints, i.e., the zone that would be affected by a chemical release under the worst case or alternative case scenarios.

---

[23] In 1995, EPA conducted a study of storage facilities for anhydrous ammonia in the Tampa Bay area. The study was prompted by concerns about the huge ammonia facilities located in the Tampa Bay area situated in close proximity to the approximately half a million people who live there. The study took into consideration the possible results of several scenarios in which ammonia was released. Among the scenarios under consideration was an "absolute worst case scenario" resulting in the release of ammonia from a tank, perhaps as the result of a plane crash, and a "nightmare scenario" resulting from the simultaneous release of the contents of all storage tanks, perhaps by earthquake or terrorist action. Ultimately, the report raised concerns about the lack of security at the Tampa Bay facilities.

Number of facilities reporting populations within the area that might be affected by a worst case or alternative release scenario					
	Population within Area that Might be Affected by Worst Case and Alternative Case Scenarios				
	0-199	200-499	500-999	1000 and up	# of facilities
Toxic Worst Case	2604	1543	1356	7308	12,811
Toxic Alternative Release	8489	1443	906	1669	12,507
Flammable Worst Case	1928	308	173	279	2688
Flammable Alternative Release	2153	69	37	37	2296

The RMP data above illustrates that over 7,000 facilities, or nearly half of the total number of facilities, have over 1,000 people within the distance to endpoint.

Second, as illustrated in the chart below, most facilities reported that there was more than one public or environmental receptor within the distance to endpoint. Accordingly, a chemical release at an industrial facility might prove attractive because it would both harm a large number of people and public and environmental receptors (for instance, a national park or landmark).

Number of facilities reporting OCA data affecting 1 or more public or environmental receptor					
	1 Public Receptor	Multiple Public Receptors	1 Enviro Receptor	Multiple Enviro Receptors	Total Facilities
Toxic Worst Case	1648	10,842	2055	750	12,811
Toxic Alternative Release	4450	6483	873	102	12,507
Flammable Worst Case	798	1386	198	18	2688
Flammable Alternative Release	950	561	104	5	2296

Third, many facilities submitting RMP data are also the types of facilities that terrorists are apt to target. Military installations, federal facilities, and utility companies are among the facilities that are required to submit RMP data. Such facilities have been the preferred targets of terrorist attacks. Terrorists often select a target because of its symbolic value both to the terrorist and to the victims. International targets of terrorism include entities that represent United States interests abroad, such as the military. The bombings in Riyadh, Beirut, and at Khobar Towers are vivid examples of the targeting of the military by international terrorists that produced devastating results. There are an estimated 80 Defense Department facilities included among the RMP submissions. Among these submissions is one for Fort George G. Meade, where an intelligence agency is located. Moreover, federal facilities have been prime targets among domestic terrorists. The rationale for such attacks have varied. For example, individuals aligned with militia organizations often attack IRS offices because of the IRS' role in collecting funds from citizens of the United States, which some view as an unlawful act. Forest Service facilities have been bombed by those who believe in the absolute sovereignty of the states or in a divine right to unregulated ownership of property. These individuals assert that the federal government has illegitimately usurped states' or individual property owners' rights.

Infrastructure facilities have also been targeted by terrorists. The U.S. infrastructure consists of a broad array of components: telecommunications systems, electrical power systems, gas and oil storage and transportation facilities, banking and finance institutions, transportation facilities, water supply systems, emergency services, and continuity of government entities. Approximately 15 percent of infrastructure facilities across the country are required to submit RMP data. For example, 1,903 of the facilities that submitted RMPs are water supply and irrigation facilities across the country; 56 facilities are involved in the generation, transmission, or control of electrical power; and

14 are involved in natural gas distribution. Infrastructure facilities are apt to be targeted because their disruption can cripple a city or an entire region of the country. For these reasons, hostile countries would be particularly interested in damaging or disrupting such facilities if hostilities broke out between the U.S. and those countries. These underlying concerns are exactly what prompted the extensive efforts and expenditures under PDDs 62 and 63.

In regard especially to military and infrastructure facilities, it is important to recognize that an attempted release of toxic chemicals may be directed at on-site consequences, as well as off-site consequences. A chemical release would be particularly effective at disrupting the operations of strategic sites, even if no off-site consequences resulted. A chemical release may be more effective than a bomb in causing such disruption, since a leak of toxic chemicals may necessitate large-scale evacuation.

Lastly, RMP facilities may also be choice targets because security at many industrial facilities is generally not as substantial as the security at other comparable potential terrorist targets that could cause a harmful release. For example, the security at nuclear facilities is tested and assessed by a Nuclear Regulatory Commission anti-terrorism unit that identifies security weaknesses at commercial nuclear power plants. No comparable effort exists industry-wide for chemical manufacturers.[24]

---

24 CSISSFRRA states that the Department of Justice shall, in consultation with relevant federal, state and local agencies, as well as members of the industry and the public, submit to Congress a report examining issues relating to site security at RMP facilities and to security of transportation of regulated substances.

Category of Facilities Submitting RMPs	Examples of Regulated Entities within these Categories of Facilities
Chemical Manufacturers	Industrial organics and inorganics, paints, pharmaceuticals, adhesives, sealants, fibers
Petrochemical	Refineries, industrial gases, plastics and resins, synthetic rubber
Other Manufacturing	Electronics, semiconductors, paper, fabricated metals, industrial machinery, furniture, textiles
Public Sources	Drinking and waste water treatment works
Utilities	Electric and gas utilities
Others	Food and cold storage, propane retail, warehousing and wholesalers
Federal Sources	Military and energy installations

IV. EXPLOITATION OF PUBLICLY AVAILABLE INFORMATION BY TERRORISTS, CRIMINALS, AND HOSTILE GOVERNMENTS

It is practically axiomatic that increased availability of information creates an increase in the risk that such information will be misused.[25] As a dean of the School of Criminal Justice at Rutgers has state in connection with the circulation of a book providing instructions, inter alia, on committing murder, "Research has found that if you show people how to commit a crime, they are more likely to do it ... Spreading the knowledge is spreading the opportunity for crime."[26] There are numerous examples of publicly available information being misused for criminal purposes. Such examples relate to information that is made public in a variety of forms: books, other publicly disseminated documents, and Internet postings.

The examples below demonstrate that when information that could be used for criminal purposes is publicly circulated, some members of the public will exploit it for illicit purposes. Some of the following examples also underscore the fact that terrorist groups, both domestic and

---

[25] We recognize that it is also axiomatic that increased access to information has attendant benefits. However, this assessment focuses, as required by CSISSFRRA, only upon risk of terrorist or other criminal activity.

[26] "Terror by Mail: Books and Products with Violent Content," Good Housekeeping, 1/1/97, at 76.

international, are exploiting the Internet, both to communicate with each other and, more to the point, to collect information for purposes of committing crimes.

A. Publicly Available Information Used in Criminal Acts

Domestic terrorist groups share information within their respective communities obtained from a variety of sources. Some of that information is used for the commission of crimes. For example, the Turner Diaries is a popular book among Christian Identity adherents. It describes a racist revolutionary movement within the United States that eventually leads to the overthrow of the government and the execution of minorities and government officials. The book also describes, in detail, an attack against the FBI Headquarters in Washington, D.C. The Turner Diaries was considered the "blue print" for Timothy McVeigh's bombing of the Alfred Murrah Building in Oklahoma City, Oklahoma, in April 1993.

The Army of God Manual is another document that has been in circulation among members of the radical fringe. It has been re-printed and updated several times by an anonymous author. The Army of God Manual contains advice on how to disrupt operations at clinics where abortions are performed and includes advice on how to build and deploy bombs. These bombmaking instructions were derived from information that was available through other sources, such as the Anarchist Cookbook. The Army of God Manual also includes instructions on the use of isobutyric acid, a caustic, noxious smelling chemical with an odor so pervasive that when it is introduced into a wall of a building, the wall often will have to be demolished and removed.

The Army of God Manual has been tied to several anti-abortion terrorists. Rachelle Shannon, who was convicted of burning eight clinics, conducting two isobutyric acid attacks, and shooting a doctor in Kansas, was tied to the Army of God Manual. Shannon committed several isobutyric acid attacks using the instructions provided in the manual. Similar attacks involving isobutyric acid have continued to occur across the United States following Shannon's incarceration. Clinic arsons have also been committed using the modus operandi outlined in the Army of God Manual. The Army of God Manual has continued to circulate underground.

The Anarchist Cookbook is another example of a published book that has been used by readers for purposes of committing crimes. The Anarchist Cookbook is a collection of information about "revolutionary activities," such as bombmaking. It has been linked to the manufacture of explosive devices and the illegal possession of weapons in several FBI investigations. In one instance, an individual who possessed the book was also found in possession of black powder, fertilizer, detonation cord, caps and pipes. Most recently, a copy was found in the possession of an individual who was indicted by a federal grand jury in November 1999, on charges of threatening to injure a woman and sending a threatening letter to a Court of Appeals Judge. Reportedly, that individual claimed in his letter that he could kill 10,000 people with a chemical called ricin. He had a makeshift lab containing material that could be used to manufacture a deadly biological poison. One of two individuals who were arrested in connection with the November 1999 plot to detonate storage tanks at a northern California propane facility was also found in possession of the

Anarchist's Cookbook, as well as a book entitled The Poor Man's James Bond, which also provides tips on bombmaking activities.

Obviously, the information in the Army of God Manual, the Anarchist Cookbook, and the Poor Man's James Bond are distinct from OCA data, which have primarily legitimate purposes. Nonetheless, these examples illustrate that when information that is susceptible to misuse is made publicly available, it is sought by individuals who would use it to cause harm. It also demonstrates that there are networks of potentially violent criminals who obtain information that is susceptible to being exploited for bad purposes and who circulate it within their communities. In such circles, it is only a manner of time before someone uses that information to do harm.

B. Public Information Disseminated Through the Internet Used in Criminal Acts

The Internet is a tremendous source of information. While it is primarily being used by law-abiding individuals every day, it is also being exploited by individuals who use it to assist in criminal activity. The last two years have produced a precipitous rise in Internet usage in households. But violent extremist groups are also part of the burgeoning use of the Internet. The Southern Poverty Law Center reported in 1999 that there was a 60 percent increase in hate group and extremist web sites in 1998; the number of such sites grew from 163 in 1997 to 254 in 1998. There can be little doubt that terrorists are Internet-savvy.

In many regards, the characteristics that make the Internet attractive to the average user also attract extremist groups to its use. The relative ease of access, the amount of content that is available, and the breadth of its use by members of the public make the Internet a valuable new tool. However, the additional fact that information can be obtained from the Internet with virtual anonymity also makes it attractive to those who would use that information for illicit purposes.

The growth of the Internet -- in particular, the explosion of cyber-crime just in the past year alone -- has introduced a new variable into the assessment of the risk involved in making OCA data publicly available. The Internet has been used for two purposes by individuals intent on causing harm: 1) to obtain information that facilitates criminal acts, and 2) to disseminate information to others for purposes of committing criminal acts. In regard to gathering information, there have been many instances in which information gathered online was used in the commission of a crime. The Army of God Manual, discussed above, has been passed via the Internet. In addition, there are numerous examples of bombmaking information that was gathered on the Internet being used during the commission of crimes. In 1997, the Department of Justice released a report discussing use of the Internet to find bombmaking instructions that could be used to commit crimes. That report found that, according to statistics from the Bureau of Alcohol, Tobacco, and Firearms, between 1985 and 1996, the investigations of at least 30 bombings and four attempted bombings resulted in the recovery of bombmaking literature that the suspects had obtained from the Internet. Furthermore, there have been numerous instances of individuals, usually minors, building explosive devices using

instructions that were found on the Internet.

Furthermore, the Animal Liberation Front (ALF), an extremist animal rights organization, has a website providing information on the construction of explosive devices and the names and locations of ALF enemies. One instance under investigation by the FBI entails information that was downloaded from the ALF website and used as an operational hit list.

Crimes committed in the past would likely have been aided by information posted on the Internet. For example, in 1974 the "Alphabet Bomber" was arrested for numerous crimes, including threatening to unleash nerve agents upon populated areas. Upon searching his apartment, local police found live pipe bombs, explosive materials, two gas masks that were stamped "U.S. Army," catalogues for purchasing chemicals and laboratory equipment, and several newly declassified military manuals about poisons and WMD. The Alphabet Bomber had collected a broad array of information about chemical warfare agents from publicly available books from the library and other sources. What took the Alphabet Bomber considerable time and effort to obtain through the library and other sources could have been obtained in a matter of hours on the Internet.

V. EVALUATING THE RISKS OF MAKING OCA DATA AVAILABLE TO THE PUBLIC

Having concluded that there is a legitimate threat that a terrorist or other criminal might seek to use an industrial chemical release as a weapon, we next evaluate whether OCA data would assist someone seeking to cause a chemical release. Further, we also examine whether there is already publicly available information similar to OCA data that reduces concern over the release of OCA data.

A. OCA Data that Provides Information Important to Causing, Targeting, or Maximizing the Effects of an Industrial Chemical Release

OCA data do not include all of the information that would be helpful to someone seeking deliberately to trigger a chemical release. For example, the OCA information does not include information about the site staffing, physical security arrangements, or the layout of the plant. However, certain OCA data represents information that would provide a would-be perpetrator with refined targeting information, making it possible for him or her to select a facility from which a chemical release would cause the greatest damage, both to humans and to the surrounding environment and community.

Not all of the pieces of OCA data pose a risk. As discussed supra at 10-11, OCA data consist of the following constitutive data elements:

- the name of the chemical involved;
- the concentration of the chemical involved;
- the physical state (gas or liquid) of the chemical involved;
- the statistical model used;
- the scenario that produces the worst-case scenario;
- the projected quantity of chemical released;
- the release rate;
- the duration of the release;
- the atmospheric stability;
- wind speed;
- the topography of the surrounding area;
- distance to end-point or the distance that the chemical release will extend;
- the endpoint for flammables;
- the residential population within the affected area;
- the public receptors within the affected area;
- environmental receptors within the affected area;
- passive mitigation systems considered in the worst-case scenario and the active and passive mitigation systems considered in the alternative release scenario; and
- map or other graphic that illustrates a worst case or alternative release scenario.

While it is difficult precisely to predict the pieces of information that would be critical to a terrorist, saboteur, or other criminal seeking to cause an industrial chemical release, we have concluded that the following subset of OCA data would assist a would-be perpetrator in planning a chemical release:

- the name of the chemical involved;
- the scenario that produces the worst-case scenario;
- the projected quantity of chemical released;
- the release rate;
- the duration of the release;
- distance to end-point or the distance that the chemical release will extend;
- the endpoint for flammables;
- the residential population within the affected area;
- the public receptors within the affected area;
- environmental receptors within the affected area;
- active mitigation measures;
- passive mitigation measures; and
- map or other graphic that illustrates a worst case or alternative release scenario.

We believe that the pieces of OCA data that do not fall into the list above would not be particularly helpful to someone seeking to cause a chemical release.

The pieces of OCA data whose public release poses some degree of risk can be placed into three categories. The first category provides a general account of the consequences of a chemical

release in terms of the damage that it might inflict on the community. It consists of the distance to endpoint, residential population within the distance to endpoint, the public receptors, the environmental receptors, and the map or graphic of the worst case or alternative release scenario. These pieces of OCA data would allow someone to compare the relative damage that could be caused by chemical releases from different sites and decide the best target from which to attempt to cause a release. In this regard, the terrorist would use the OCA data in much the same way that it is intended to be used by the public for purposes of assessing the relative risk posed by various facilities. Terrorists' mounting interest in causing the maximum damage would make this information highly valuable to a terrorist seeking to maximize the consequences of a release. We believe that this category of OCA data would be of the greatest value to a terrorist.

The second category of OCA data that would be potentially useful to a terrorist consists of information about the elements of a large scale chemical release and basic information about how to cause a release. The pieces of OCA data that fall within this category are: the name of the chemical involved in the worst or alternative case scenario; the projected quantity of chemical released, the release rate, and the duration of the chemical release; the endpoint for flammables, and the scenario that results in the chemical release. Since different chemicals have different degrees of lethality, knowing just the distance to endpoint may not be enough for purposes of planning a release. It would also be important to know exactly what chemical will be released before assessing a chemical release's potential for harm. In addition, OCA data about the amount of chemical released and the interval of release provides some basic notion of the type of release that would have to be achieved to bring about something approaching the worst or alternative case scenarios. The endpoint for flammables supplies information about the type of damage (radiant heat or a blast wave) that would result from a release of flammable chemicals. Lastly, the scenario information in the RMPs provides rudimentary information about how to cause a release. For example, in regard to scenario information, the facility must identify whether the alternative scenario that is projected by the facility resulted from a transfer hose failure, a pipe leak, a vessel leak, overfilling, rupture disk/relief valve failure, or excess flow device failure. While neither the OCA data nor the RMP provides information about the location of the particular pipe or vessel that would have to be ruptured to cause the alternative release scenario, the means of causing a release have been winnowed down for a would-be perpetrator, providing him or her with a broad notion of where, for example, to place a bomb. All of this information together provides a rough sketch of the elements involved in triggering a serious release from the RMP facilities. This information is less sensitive than the first category of information above, but would nonetheless provide valuable assistance for purposes of planning a chemical release. Further, as discussed <u>infra</u> at 44, some of this information is already publicly available.

The third category, which is the least likely to be exploited by a terrorist but would nonetheless be relevant to an attempt to cause a chemical release, concerns the facilities' safety measures. An ambitious perpetrator could also use OCA data to prioritize the best targets on the basis of their lack of mitigation measures that might thwart or hamper a chemical release. This category is reflected by the OCA data about passive and active mitigation measures. Of the three

categories of information, we assess this to be the least important to a terrorist. In addition, this information is already publicly available, as discussed infra at 44.

OCA DATA THAT WOULD BE SALIENT TO A TERRORIST FOR PURPOSES OF CAUSING A CHEMICAL RELEASE	
Category 1: OCA data about the consequences of a chemical release	- distance to endpoint - residential population within the distance to endpoint - public receptors - environmental receptors - optional map or graphic of the worst case or alternative release scenario
Category 2: OCA data providing the elements of a large scale chemical release and basic information about how to cause a release	- name of chemical involved - projected quantity of chemical released - the release rate - duration of the chemical release - endpoint for flammables - scenario that results in the chemical release[27]
Category 3: OCA data on facility safety measures	- active mitigation measures - passive mitigation measures

We compared our analysis of pieces of OCA data that would be helpful to a terrorist to a model derived from the intelligence and operations planning/targeting criteria used by the Defense Department's U.S. Special Operations Command (USSOC). That military force's approach to target selection is reportedly similar to that used by a terrorist organization or similar entity. The USSOC-based model included nine pieces of information that it deemed critical to someone seeking to cause an industrial chemical release. The nine pieces of information were identified as:

1) knowledge that the facility existed;
2) knowledge of which chemicals were present at the facility;
3) knowledge that there were offsite consequences to a chemical release from the facility;

---

[27] Although we would normally include information like the scenario data element, which is a description of the worst case or alternative release scenarios, in category one, our concern about this information is somewhat diminished because the scenario information in the RMP forms is general and summary in nature. It provides only in broad terms the conditions under which the worst case or alternative case release is presumed to occur (e.g., transfer hose failure or overfilling of tank).

4) knowledge of security at the facility;
5) knowledge of the facility layout;
6) knowledge of where the chemicals were stored;
7) knowledge of the mitigation measures to be employed to limit damage used by the site;
8) knowledge of the facility's emergency response plan; and
9) knowledge of the community emergency response plan.

Seven of the pieces of OCA data that we identify as important to a terrorist (the name of the chemical involved, the distance to endpoint, the residential population within the distance to endpoint, the public receptors, the environmental receptors, the active mitigation measures, and the passive mitigation measures) correspond to the salient items that a terrorist would seek to learn according to the USSOC-derived rubric.

B. Pieces of OCA Data that Would Be Salient to a Terrorist Attack that Are Currently Publicly Available

The risk inherent in releasing OCA data may be reduced to the extent that the pieces of OCA data that we have identified as helpful to planning a chemical release are already publicly available in a comparable form. We find that some of the pieces of OCA data that are cause for concern are indeed currently publicly available in a comparable form. However, we have determined that the data that are the most useful to a terrorist are not, or would otherwise require technical proficiency to assemble.

1. Information Currently Disseminated by EPA

Consistent with its regulatory mission, EPA collects and disseminates a wide variety of information concerning chemicals used and stored at facilities across the country.[28] EPA collects and disseminates information concerning the release and transfer of chemicals and compounds pursuant to Section 313 of the Emergency Planning and Community Right-to-Know Act (EPCRA). Furthermore, facilities that manufacture, process, or use a designated toxic chemical must annually report information to the EPA regarding any chemical releases at the facility. If no reported release

---

[28] Our assessment focuses primarily upon publicly available information that is provided by the government. We focus upon such information because there is a qualitative difference between information collected by a member of the public or a non-governmental organization and information that is collected by the government pursuant to federal regulations. The latter information, which has the government's imprimatur, carries a greater presumption of accuracy and is more likely to be considered credible and reliable.

of a chemical has occurred at a site, no report is made to the EPA. Other sources of information provide data about the dangers of potentially hazardous chemicals that are used by manufacturers. Such sources are intended to be used for purposes of worker safety.

In addition to these sources, there are various software programs available through EPA that chart information about potential or actual environmental contamination obtained from certain EPA databases onto a map. Another program takes information from various databases containing environmental information and displays it in a geographic format. Yet another program provides dispersion models that allow users to estimate the dispersion of chemical vapors based on characteristics of a released chemical.

Pursuant to CSISSFRRA, EPA has released the executive summaries of all the RMPs, many of which contain some OCA data. According to EPA guidance, each executive summary had to mention worst case scenario and alternative release scenario information. However, as the chart infra at 44 demonstrates, while the executive summaries contain some OCA data, they do not contain all OCA information. Furthermore, many do not include the most sensitive OCA data.

2. Analysis of the Current Availability of OCA-Type Data

The public availability of OCA data in the three categories of information identified supra at 40 varies greatly. Some of those pieces of OCA data are posted on the Internet, while others are available through programs that must be downloaded and installed on a computer. In other instances, SERCs (State Emergency Response Committee) and LEPCs make such information available, which means it is available mostly on a local level and on a limited scale. Other pieces of the OCA data that poses national security and law enforcement concerns are only available if someone with sufficient expertise compiled information from disparate sources and analyzed it. Lastly, some pieces of OCA data are not available at all.

The four pieces of information in category 1 related to the consequences of industrial chemical releases at facilities (i.e., distance to endpoint, residential population within the distance to endpoint, environmental receptors, and public receptors) are not generally available. We judge this category of information to be vital to many of the potential perpetrators who would seek to cause a chemical release, since maximizing the death toll or damage from a release would be one of the principal goals of a terrorist. Its release poses the greatest national security and law enforcement risk.

Certain websites supply information concerning the consequences of toxic emissions from facilities; however, information from those websites is far less complete than OCA information. For example, there currently are maps posted on some websites annotated with radiating circles to indicate the zone that would be affected by a chemical release from a particular facility. But there

are only a handful of such websites and maps, and the information they contain pertains only to several cities in the country. Moreover, because these websites use data that is not as accurate as the data the federal government gathered through the RMPs, their calculations of consequences are less precise than those represented by OCA data.

Other information about off-site consequences of chemical releases is also currently inaccessible. Neither the numerical estimates of the residential populations, nor the public and environmental receptors that would be affected by chemical releases from facilities is currently available through any public source. This information could be calculated using information available from several different public sources. However, it would take time, familiarity with those sources, and an understanding of how to manipulate them to arrive at figures for the population and receptors that would be affected by a chemical release; a limited pool of people possess all three.

The publicly available information that is most comparable to the distance to endpoint, residential population within the distance to endpoint, and environmental and public receptor data are available through the RMP executive summaries that have been released on the Internet. The EPA's guidelines for submission of RMP data require that the executive summaries include OCA information. However, the guidelines do not specify how detailed the information in the executive summaries should be.[29] Indeed, based upon a random sample of a geographically diverse selection of 50 executive summaries, it appears that they vary greatly in the amount of OCA data they contain, as the chart below indicates. While over half of the sample of executive summaries provided the the distance to endpoint, few gave the residential population within the distance to endpoint. Further, while almost half identified that public or environmental receptors would be affected, only seven identified exactly what receptors would be affected. Such information is provided in the complete OCA data.

---

[29] It is noteworthy that we believe the fact that some OCA data has been released in RMP executive summaries poses law enforcement and national security concerns. We recommend that EPA change its guidelines so that OCA data that raises such concerns not be included in the executive summaries in the future.

Worst Case Scenario Data Contained in a Random Sample of 50 Executive Summaries			
Environmental Receptors	Public Receptors	Distance to Endpoint	Residential Population w/in Endpoint
20/50	22/50	35/50	12/50

In sum, the data likely to be used for purposes of targeting a facility from which to cause an industrial chemical release–which falls within our category 1–are not currently available to the public in a format that would be easily used by someone lacking technical sophistication and familiarity with environmental issues.

In regard to the information in category 2, (i.e., OCA data providing the elements of a large scale chemical release and basic information about how to cause a release) portions of these pieces of information are available to the public and are fixed values. The duration of release for the worst case scenarios (Section 2.7) is a fixed numbers selected by EPA. The fixed values are readily accessible in documents that define the worst case scenario. Similarly, the endpoint used for flammables in the worst case scenario (Section 4.5 of the RMP) is also a set value that is readily accessible in the documents that define the worst case scenario. For this reason, we have less concern about the release of these data elements. The alternative release scenario duration of release and endpoint of flammables data elements are not fixed and not generally available. Consequently, their release poses the same degree of risk as the rest of the category 2 data elements.

Lastly, the information in category 3 (OCA data on facility safety measures) is generally currently available in the released portions of the RMPs. Section eight of the RMPs provides information about the facility's prevention program. As part of the information provided in that section, the mitigation measures at each facility are discussed.

In sum, the information in category 1, which is the information that poses the greatest law enforcement and national security concerns, is the information that is currently least available to the public in a form that is comparable to the OCA data. Further, while some portions of category 2 information have been released to the public, others have not. Specifically, the duration of release and the flammables endpoint for the worst case scenario are fixed values that are publicly available. Lastly, all of the category 3 information is currently available to the public. Based upon this analysis, dissemination of category 1 information will increase the risk of a chemical release being used by a terrorist, because it will disclose heretofore unavailable information that would be useful to a terrorist for purposes of maximizing a chemical release. In addition, release of the following pieces of information that we rank as category 2 information would also have the effect of increasing risk of a chemical release caused by criminal activity, because such information would be helpful to planning a release and is not currently available to the public: the name of the chemical involved,

the projected quantity of chemical released, the scenario, the release rate, the duration of the chemical release for the alternative release scenario, and the endpoint for flammables for the alternative release scenario. Lastly, the information in category three has already been released to the public in the RMPs and, therefore, its release would only negligibly increase the national security or law enforcement risk.

C. Public Dissemination of OCA Data Consistent with National Security and Law Enforcement Concerns

CSISSFRRA requires that the government make all OCA data available in some form to any member of the general public, as well as to covered persons and qualified researchers. Consequently, the only vehicle by which national security or law enforcement concerns described above can be taken into account is in the manner of providing access to the OCA data. From a national security perspective it seems apparent that if all OCA data– including the data elements that pose the greatest risk to national security–must be released to the general public, significant steps must be taken to ensure that the manner in which the data is released poses the least risk to national security. This is particularly true of the information in categories 1 and 2, as enumerated supra at 38, that pose the greatest law enforcement and national security concern.

Not all information that is released to the public is equally accessible. For example, information posted on a website is generally more accessible than information obtained through the mail, which in turn is typically more accessible than information provided in a reading room. Nevertheless, dissemination of information through each of these methods is considered public dissemination. The more personal contact that is required to obtain information, the less likely it is that someone seeking to misuse the information will attempt to obtain it.[30]

1. Security of Data Disseminated Using the Internet

The Internet has revolutionized and will continue to revolutionize how we obtain and share information. The Internet has grown from 65 million users in 1998 to over 100 million users in the U.S. in 1999, or half the country's adult population; the number of Internet users in the U.S. is projected to reach 177 million by the end of 2003; and the number of Internet users worldwide is estimated to reach 502 million by 2003. The Internet, like most new technologies, is an inherently value-neutral tool: It can be used in ways that are socially beneficial or socially harmful. Individuals who wish to use a computer as a tool to facilitate criminal activity may find the Internet as appealing,

---

[30] We recognize that the corollary concern is that methods that require more effort might also be a disincentive to individuals who would make appropriate use of the information would also be less likely to obtain it.

if not more so, as they did the telephone decades ago or the telegraph before that. Similar to the technologies that have preceded it, the Internet provides a new tool for wrongdoers to commit crimes.

There is little doubt that terrorist organizations spanning the ideological spectrum are aware of and using the Internet for a variety of purposes. The Liberation Tigers of Tamil Eelam, a separatist group banned by the government of Sri Lanka, and Peru's Shining Path each have websites. In fact, at least 12 of the 30 groups on the State Department's list of designated terrorist organizations maintain web sites. Most use the Internet to advance their political or ideological agenda. Terrorist groups in Latin America have used websites to spread propaganda and Islamic militant organizations have provided their charters through Internet posting. Some reportedly even field press inquiries through electronic mail. Regardless of their purpose, it is clear that many terrorist organizations are Internet-savvy.

We have yet to appreciate all of the ways in which data made available on the Internet may be subject to interception or unauthorized access. Just in February 2000, Internet security experts have identified a "potentially huge" and heretofore unnoticed problem that would allow someone to inject malicious scripts into Internet pages that are generated dynamically by Web servers.[31] A host of data security issues are presented by computers that are linked to the Internet. An Internet security expert at AT&T Labs Research was recently quoted saying that despite a substantial effort by security experts to secure computers, "the attackers have the edge."[32]

One obvious way in which a computer can be involved in unlawful conduct is when the confidentiality, integrity, or availability of a computer's information or services is attacked. This form of crime targets a computer system, generally to acquire information stored on that computer system without authorization (i.e., "hacking" into it). A recent survey of Fortune 500 companies conducted by the FBI and the Computer Security Institute found that 62 percent of respondents had computer security breaches in the last year. There are apparently a variety of methods for obtaining information off of the hard drive of a computer connected to the Internet. For example, it is possible to create a program attached to a piece of e-mail that will read all of the information off of a hard drive and send it to someone as e-mail or post it to a news group.

Offenses involving theft of information may take a variety of forms, depending on the nature of the system attacked. Sensitive information stored on law enforcement and military computers

---

[31] This problem, called "cross-site scripting," is being addressed by computer security officials who are providing detailed information to the public about how it works in a concerted effort to inform and ultimately rid the Internet of the problem.

[32] "PC's Vulnerable to Security Breaches, Experts Say," N.Y. Times, 2/04/00.

offers a tempting target to many parties, including subjects of criminal investigations, terrorist organizations, and foreign intelligence operatives.

In regard to the OCA data, we have reservations about making the sensitive pieces of such data available via the Internet because of the difficulty safeguarding Internet-available information from unauthorized access. These concerns are increased given the difficulty that government agencies, including the EPA, have experienced protecting their computer systems to computer attack.

A General Accounting Office (GAO) report entitled "Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk" prepared in anticipation of a February 17, 2000 hearing before the Subcommittee on Oversight and Investigations, House Committee on Commerce, found that EPA suffered "serious and pervasive problems that essentially render EPA's agency-wide information security program ineffective." The report concluded that "EPA's computer systems and the operations that rely on these systems are highly vulnerable to tampering, disruption, and misuse." The GAO findings related specifically to the computer systems through which EPA makes information, like OCA data, available to the public via its website. The report further claimed that GAO identified two dozen instances during 1998 and 1999 in which EPA's systems were in fact compromised or misused and that "EPA['s computer system] was the subject of repeated systematic probes <u>from a variety of domestic and foreign sources</u>." (Emphasis added.)

EPA has reportedly taken steps to remedy the problems cited in the GAO report. Nevertheless, making the sensitive pieces of OCA data available to the public via its Internet website, or any website, raises data security concerns.

2. <u>Problems with the Breadth of Access of Internet Information</u>

Setting aside the issue of vulnerability to unauthorized access of OCA data, the potential availability of OCA data to the general public–which includes terrorists, as well as law abiding citizens– obviously poses potential hazards, depending on precisely what portions of OCA data are made available. If the sort of targeting information we have identified as posing the greatest security risk among all the OCA data were made available through a website, anyone would have unfettered use of that data. While members of the public with legitimate reasons for seeking such information would have access to such information, individuals with sinister motives would as well.

The risks attendant in disseminating OCA information on the Internet also relate to the likelihood that groups hostile to the United States will seek such information for purposes inimical to U.S. interests. In light of intelligence and other information regarding the extensive use of computers and the Internet by terrorist groups, it should be assumed that in making the OCA data available on the Internet, international terrorist groups will seek, scrutinize, and use that information to the extent it advances their ends. Such ends could include causing chemical releases.

Not surprisingly, in recent years terrorist groups have proven to be as adept as legitimate organizations in taking advantage of and incorporating high technology into their operations and activities. Classified information indicates that a terrorist group which had used chemical agents as a terrorist weapon in the past had also used computer techniques to produce nerve gas and acquired computer-controlled precision machine tools for its abortive effort to produce a nuclear weapon.

Intelligence indicates that, as a general matter, terrorist organizations are increasingly using computers and the Internet for support activities such as recruitment, fundraising, propaganda and communications.[33] Even more significantly for purposes of this assessment, there is intelligence reporting that terrorists have used computer applications, such as the Internet, CD-ROM-based databases, or engineering and research programs, in order to research and analyze target vulnerabilities.

The Internet affords a user access to information virtually anonymously in an unmonitored environment. Even though certain electronic "footprints" may be left by a user, these can be easily disguised through the use of "anonymizers," which are Internet websites that strips all identifying information from a user's Internet transactions, allowing anonymous e-mailing, Web browsing, and newsgroup posting.

3. Access to Paper Copies of OCA Data and the Internet

An offshoot of the concern about the risks inherent in providing OCA data to the public via the Internet is the issue of how to effectuate the requirement under CSISSFRRA that members of the public receive "access to paper copies" of OCA data. The core consideration from a risk point of view is that the dissemination to the public of OCA data in paper form will significantly increase the risk that OCA data will ultimately be posted on the Internet. Technological advances have had a great impact upon document handling. Improvements in optical character recognition software programs and affordable computer scanners have vastly simplified the task of converting data contained on paper into electronic data. Creating a reliable and accurate electronic version of a paper document is practically as simple as making a photocopy. Further, these technological advances have vastly simplified the task of converting large quantities of paper documents into electronic data. Once in electronic format, uploading it and posting such information on the Internet is simple.

Accordingly, if paper copies were distributed to members of the public as a means of giving the public access to OCA information, there is a substantial chance that the security interests would be undermined. A coordinated effort of a handful of individuals could fairly easily assemble a large

---

[33] Hizballah, for example, maintains several Web sites and claims to have recorded some 65,000 views or "hits" since January 1997.

quantity of submissions regarding different facilities. Depending upon the number of stationary facilities about which someone was entitled to receive OCA data, a group of individuals could possibly even amass OCA data for the entire database. If someone were intent on posting this information on the Internet, little, if anything, could be done to prevent them from accomplishing this objective once the paper copies were in his or her possession. In light of the fact that certain organizations have already taken the OCA Executive Summaries and made them more accessible by posting them on the Internet, it is likely that individuals or organizations will embark on a similar effort with regard to OCA data. Thus, to minimize the risk to national security and law enforcement interests, we recommend that in light of the concerns about certain portions of OCA data being posted on the Internet, the public should be provided access to paper copies of OCA data in the means that will least likely result in members of the public posting OCA data on the Internet.