# SUMMARY REPORT ON CRITICAL INFRASTRUCTURE INTERVIEWS

Report to the
President's Commission
on Critical Infrastructure Protection
1997

## CONTENTS


**SECTION** **PAGE**

EXECUTIVE SUMMARY ..... viii

1 INTRODUCTION ..... 1

1.1 Background ..... 1
1.2 Interviews ..... 1
1.3 Report Organization ..... 2

2 INTERVIEW PROCESS ..... 3

2.1 Background ..... 3
2.2 Identifying Interviewees ..... 3
2.3 Conducting Interviews ..... 3
2.4 Individual Interview Summaries ..... 3

3 OVERALL FINDINGS ..... 4

3.1 General Findings ..... 4
3.2 Information and Communications ..... 4
3.3 Electrical Power Systems ..... 4
3.4 Gas and Oil Production, Storage and Transportation ..... 4
3.5 Banking and Finance ..... 5
3.6 Transportation ..... 5
3.7 Water Supply Systems ..... 5
3.8 Emergency Services ..... 6
3.9 Continuity of Government Services ..... 6

4 INFORMATION AND COMMUNICATIONS ..... 8

4.1 General Information ..... 8
4.1.1 Background ..... 8
4.1.2 Organization ..... 8
4.2 Threats and Vulnerabilities ..... 8
4.2.1 Types of Threats ..... 8
4.2.2 Types of Vulnerabilities ..... 8
4.2.2.1 New Technology and Trends ..... 9
4.2.2.2 Hackers and Security Technology ..... 10
4.2.2.3 Interconnectivity ..... 10
4.2.2.4 Foreign Threats ..... 10
4.2.2.5 Operating Systems ..... 11
4.2.2.6 Internet ..... 11
4.2.2.7 Insider Threats ..... 11

4.2.2.8 Virus Protection ..... 11
4.2.2.9 Natural and Human-Caused Disasters ..... 11
4.2.2.10 Year 2000 Problem ..... 12
4.2.3 Security Tool Developments and Analysis ..... 12
4.3 Requirements and Standards ..... 12
4.4 Emergency Plans ..... 13
4.5 Information Exchange ..... 13
4.5.1 General Information ..... 13
4.5.2 Threat Information ..... 13
4.6 Research Needs ..... 14
4.7 Government Role ..... 15
4.8 Other Areas of Interest or Concern ..... 15

5 ELECTRICAL POWER SYSTEMS ..... 17

5.1 General Information ..... 17
5.1.1 Background ..... 17
5.1.2 Organization ..... 17
5.1.3 Infrastructure Involved ..... 18
5.2 Threats and Vulnerabilities ..... 18
5.2.1 Types of Threat ..... 18
5.2.2 Vulnerability Assessments ..... 19
5.2.2.1 Assessment Methods ..... 19
5.2.2.2 Areas of Vulnerability ..... 20
5.2.2.3 Levels of Risk ..... 21
5.2.2.4 Impact on Other Infrastructures ..... 21
5.2.3 Vulnerability Reduction Actions ..... 21
5.3 Requirements and Standards ..... 22
5.4 Emergency Plans ..... 22
5.4.1 Response Plans ..... 22
5.4.2 Exercises/Drills ..... 22
5.4.3 Communications/Command ..... 23
5.5. Information Exchange ..... 23
5.6. Research Needs ..... 23
5.7. Other Areas of Interest/Concern ..... 23

6 GAS AND OIL PRODUCTION, STORAGE, AND TRANSPORTATION ..... 24

6.1 General Information ..... 24
6.1.1 Background ..... 24
6.1.2 Organizations ..... 24
6.1.3 Infrastructures Involved ..... 24
6.2 Threats and Vulnerabilities ..... 24
6.2.1 Threats ..... 24
6.2.2 Vulnerabilities ..... 24

6.2.2.1 Assessment Methods ..... 25
6.2.2.2 Vulnerability Reduction Actions ..... 26
6.3 Requirements and Standards ..... 26
6.3.1 Existing ..... 26
6.3.2 Suggested Changes
6.4 Emergency Plans ..... 27
6.4.1 Response Plans ..... 27
6.4.2 Recovery Plans ..... 27
6.5 Information Exchange ..... 27
6.6 Research and Development ..... 28
6.6.1 Needs ..... 28
6.6.2 Schedule ..... 28
6.6.3 Role of Government ..... 28
6.7 Other Issues ..... 28

7 BANKING AND FINANCE ..... 29

7.1 General Information ..... 29
7.1.1 Background ..... 29
7.1.2 Organizations ..... 29
7.1.3 Infrastructures Involved ..... 29
7.1.4 Industry Trends Related to Infrastructure Protection ..... 29
7.2 Threats and Vulnerabilities ..... 30
7.2.1 Types of Threats ..... 30
7.2.2 Vulnerabilities ..... 30
7.2.3 Externalities Affecting Threats and Vulnerabilities ..... 31
7.3 Requirements and Standards ..... 32
7.4 Emergency and Disaster Recovery Plans ..... 32
7.5 Research and Technology Needs ..... 32
7.6 Government Role ..... 33

8 TRANSPORTATION ..... 35

8.1 General Information ..... 35
8.1.1 Background ..... 35
8.1.2 Organizations ..... 35
8.1.3 Infrastructure Involved ..... 36
8.1.3.1 Mass Transit ..... 36
8.1.3.2 Ports and Harbors ..... 36
8.1.3.3 Bridges and Tunnels ..... 36
8.1.3.4 Airports ..... 37
8.2 Threats and Vulnerabilities ..... 37
8.2.1 Types of Threats ..... 37
8.2.1.1 Mass Transit ..... 37
8.2.1.2 Ports and Harbors ..... 38

8.2.1.3 Bridges and Tunnels ..... 38
8.2.1.4 Airports ..... 38
8.2.2 Vulnerability Assessments ..... 38
8.2.2.1 Assessment Methods ..... 38
8.2.2.2 Areas of Vulnerability ..... 39
8.2.2.3 Level of Risk ..... 39
8.2.2.4 Impact on Other Infrastructures ..... 39
8.2.3 Vulnerability Reduction Actions ..... 39
8.2.3.1 Operational Practices ..... 39
8.2.3.2 Technologies ..... 40
8.2.3.3 Investment Considerations ..... 40
8.3 Requirements and Standards ..... 41
8.3.1 Existing or Planned ..... 41
8.3.2 Suggested Change ..... 41
8.4 Emergency Plans ..... 41
8.4.1 Response Plans ..... 41
8.4.1.1 Exercises/Drills ..... 42
8.4.1.2 Communications/Command ..... 42
8.5 Information Exchange ..... 42
8.5.1 Current Methods ..... 42
8.5.2 Areas of Deficiency ..... 43
8.5.3 Suggested Improvements ..... 43
8.6 Research Needs ..... 43
8.6.1 Unmet/Inefficiently-met Needs ..... 43
8.6.2 Government Role ..... 43

9 WATER SUPPLY SYSTEMS

9.1 General Information ..... 45
9.1.1 Background ..... 45
9.1.2 Organizations ..... 45
9.2 Threats and Vulnerabilities ..... 45
9.2.1 Threats ..... 45
9.2.2 Vulnerabilities ..... 45
9.2.3 Vulnerability Reduction Actions ..... 46
9.3 Requirements and Standards ..... 46
9.4 Emergency and Disaster Recovery Plans ..... 46
9.5 Information Exchange ..... 46
9.6 Research and Development
9.6.1 Infrastructure Needs ..... 47
9.6.2 Funded Research ..... 47
9.6.3 Role of Government ..... 48
9.7 Other Considerations ..... 48

10 EMERGENCY SERVICES ..... 49

10.1 General Information ..... 49
10.1.1 Background ..... 49
10.1.2 Organizations ..... 49
10.1.3 Infrastructure Involved ..... 49
10.2 Threats and Vulnerabilities ..... 50
10.2.1 Types of Threats ..... 50
10.2.2 Vulnerability Assessments ..... 50
10.2.3 Vulnerability Reduction Actions ..... 51
10.2.3.1 Operational Practices ..... 51
10.2.3.2 Technologies ..... 51
10.3 Requirements and Standards ..... 52
10.4 Emergency Plans ..... 52
10.4.1 Response Plans ..... 52
10.4.1.1 Exercises/Drills ..... 52
10.4.2 Recovery Plans ..... 53
10.4.3 Communications/Command ..... 53
10.5 Information Exchange ..... 54
10.6 Research and Development ..... 54
10.6.1 Unmet or Partially-Met Needs ..... 54
10.6.2 Role of Government ..... 55

11 CONTINUITY OF GOVERNMENT SERVICES ..... 57

11.1 General Information ..... 57
11.1.1 Background ..... 57
11.1.2 Organizations ..... 57
11.1.3 Infrastructure Involved ..... 57
11.2 Threats and Vulnerabilities ..... 57
11.2.1 Types of Threats ..... 57
11.2.2 Vulnerability Assessments ..... 58
11.2.3 Vulnerability Reduction Actions ..... 59
11.2.4 Investment Considerations ..... 59

11.3 Requirements and Standards ..... 59
11.4 Emergency Plans ..... 60
11.4.1 Response Plans ..... 60
11.4.2 Recovery Plans ..... 60
11.5 Information Exchange ..... 60
11.6 Research Needs ..... 61

Appendix A – Interview Question Template ..... 62

Appendix B – Water Supply Stakeholder's Questionnaire ..... 65

## EXECUTIVE SUMMARY

More than 40 interviews of knowledgeable people in the eight critical infrastructures were conducted to ascertain industry perspectives on their threats, vulnerabilities, research needs, and ideas on the appropriate role of government in addressing infrastructure protection. These interviews were conducted by Argonne National Laboratory on behalf of the President's Commission on Critical Infrastructure Protection. More than 100 individuals from over 50 organizations participated in these interviews.

Detailed summaries of these interviews are found in subsequent chapters of this report. However, some of the more generally applicable findings are noted here.

**Threats:** Each of the eight critical infrastructures has some level of physical threat which they must potentially address. Such threats include those of terrorist activities although most interviewees expressed the opinion that terrorist activities were not as much of a concern as other physical threats, e.g., natural disasters. An exception to this general consensus on terrorism is the Oil and Gas infrastructure which, because of its multi-faceted and multi-national nature, is more potentially subject to, and concerned about, terrorist activities, including kidnapping.

A common area of concern among the infrastructures is that of the insider threat. It was generally felt that knowledgeable insiders could cause considerable damage to existing systems.

In the transportation infrastructure, and in particular the public transit area, the largest threat is that of crime, e.g., theft, assault, rape, etc. The great majority of expenditures in reducing threats in this infrastructure currently goes to crime-fighting activities such as additional lighting in parking lots, police officers riding busses and trains, or monitoring with closed-circuit TV cameras.

**Vulnerabilities:** Most of the vulnerabilities discussed during these interviews dealt with specific issues pertinent to the individual infrastructures. There are however, some areas of vulnerability common to a number of the infrastructures. These are:

- Competitiveness within the industry or general shortage of funding often results in a disproportionate reduction in the level of security or protection;
- Many infrastructures have only limited testing of their emergency response plans and response plans generally deal with natural disasters and not terrorist activities;
- There is little training or equipment to respond to an NBC threat.

**Research Needs:** Specific research needs for each of the critical infrastructures are noted in the appropriate chapter of this report. Commonly expressed needs include the following:

- Methods and tools for vulnerability analysis, particularly as applied to terrorism;

- Proper emergency response actions for terrorist events, particularly those involving NBC agents; and

- Improved monitoring and detection devices, particularly for remote locations;

**Government Role**: Many interviewees expressed opinions regarding the role of government in assisting in critical infrastructure protection. Among the more frequently expressed thoughts are:

- Support research and development activities as the industries are not likely to do so;

- Provide tougher enforcement and stiffer penalties for laws dealing with infrastructure protection;

- Develop and provide guidance on infrastructure protection but do not mandate any specific actions;

- Provide funds for training and for implementing security/protection actions, (e.g., equipment and communication systems); and

- Share intelligence information on terrorism with the appropriate industries.

# SUMMARY REPORT ON CRITICAL INFRASTRUCTURE INTERVIEWS

prepared for
The President's Commission on Critical Infrastructure Protection

## 1 INTRODUCTION

### 1.1 Background

The President's Commission on Critical Infrastructure Protection (Commission) was established through Executive Order 13010 and has been tasked to bring together the combined forces of the government and private sector to develop a strategy for protecting and assuring the continued operation of this nation's critical infrastructures. The critical infrastructures as identified in the Executive Order are:

1. Information and Communications (originally referred to as Telecommunications)
2. Electrical Power Systems
3. Gas and Oil Production, Storage and Transportation
4. Banking and Finance
5. Transportation
6. Water Supply Systems
7. Emergency Services
8. Continuity of Government Services

In fulfilling its mission, the Commission has undertaken several activities including:

- Determining and characterizing the range of threats;
- Identifying vulnerabilities within and among the critical infrastructures;
- Finding and assessing options for protecting infrastructures, assuring continuation and restoration of service;
- Developing a strategy for protecting critical infrastructures; and
- Recommending an implementation plan for protective and assurance measures, including the policy, legislative and other changes required.

Private-sector participation in Commission activities was accomplished in several ways. From the beginning of the Commission, representation of the private sector on the Commission itself was established as a goal. Information on threats, vulnerabilities, needs, strategies, and other issues was received from the private sector.

### 1.2 Interviews

One means of obtaining private-sector input to the Commission was to conduct a set of interviews with representatives of each of the eight critical infrastructures. The interviews, which were predominately with private-sector personnel although some public-sector people were also interviewed as appropriate, had the objective of collecting representative responses regarding issues of vulnerabilities, threats, emergency response, and recovery related to physical and/or cyber incidents. While the specific questions asked during the interviews varied

somewhat from one critical infrastructure to another and with the specific interviewers, the general points of discussion were centered on the above topics.

### 1.3 Report Organization

The remainder of this report is organized as follows: Chapter 2 includes a brief summary of the interview process, Chapter 3 includes a brief, overall summary of the findings (with emphasis on the needs) in each of the eight critical infrastructures, and Chapters 4 through 11 give more detailed summaries of the interviews. Appendix A shows the Interview Question Template that was used as a guide while conducting the interviews.

# 2 INTERVIEW PROCESS

## 2.1 Background

To provide proper perspectives on the infrastructure protection status and needs within the private and public sectors, the Commission requested input from selected organizations that are considered representative of the variety of organizations within each of the eight critical infrastructures. Argonne National Laboratory (Argonne) was commissioned by the Commission to collect this input via a series of interviews and to prepare a summary of these interviews which characterizes the issues of concern, the state of vulnerability identification in the various infrastructures, their needs, and their recommendations. These findings will be combined the results of the Capabilities and Technologies Surveys conducted on behalf of the Commission to make recommendations regarding near- and long-term protective measures, as well as potential areas for research and development in the area of critical infrastructure protection.

## 2.2 Identifying Interviewees

Based on discussions with the Commission, Argonne undertook to identify candidate organizations for these interviews. The goal was to conduct approximately 30 such interviews. Argonne prepared an initial list of candidates which was based on the experiences of Argonne personnel in the respective infrastructures and on literature searches via tools such as the Internet. Fiscal, schedule, and geographic factors were also considered in developing this initial list.

The initial list was then presented to the Commission for their comments and review. In the resultant discussions, the Commission and Argonne agreed on a set of candidates which would serve as the basis for the interviews. In most cases, the organizations on that final list of candidates were interviewed by Argonne. Some organizations however, chose to not participate in these interviews because they have already participated in other Commission activities. Some additional organizations not on this list were also interviewed because the opportunity for an interview presented itself or because one or more earlier interviewees noted that a particular organization has unique capabilities in the area or that they are viewed as a benchmark in a particular area of interest. More than 40 interviews were ultimately conducted by Argonne as part of this effort.

## 2.3 Conducting Interviews

To assist them in preparing for the interview, the interviewees were generally provided with the Interview Question Template prior to the interview. This template notes the items to be discussed. These discussion points served to keep the interview on-track but allowed sufficient flexibility to allow each interview to follow a course most appropriate to the specific critical infrastructure involved and the individual interviewees.

Interviews were conducted either in person-to-person discussions or over the telephone. In most cases, two or three Argonne people conducted each interview. The interviews typically lasted for one to two hours.

## 2.4 Individual Interview Summaries

Following the individual interviews, the Argonne team prepared a summary report for each interview. In preparing these summary reports, they attempted to accurately portray the thoughts, concerns, and opinions of the interviewees. These individual reports were in turn summarized to reflect the information obtained from all interviews within a given critical infrastructure. The current report contains this material. It should be noted that the information was obtained from individuals and does not necessarily reflect the opinions of their organizations or of Argonne National Laboratory.

# 3 OVERALL FINDINGS

## 3.1 General Findings

Detailed summaries for each of the critical infrastructures can be found in Chapters 4 through 11. Some of the basic findings are briefly summarized below.

## 3.2 Information and Communications

Basic findings for this infrastructure through these interviews include:

- New technologies are expanding the use of networks and systems and thus increasing their vulnerability.
- Hackers have become more focused on disrupting networks and systems and have more sophisticated tools for doing it.
- Greater interconnectivity of networks and systems has allowed more participants to be integrated thereby exposing the entire system to the vulnerabilities of its weakest component. The Internet is an example of such a network.
- The interviewees consider foreign ownership of critical components in the infrastructure to be a serious vulnerability.
- Insider threats are considered significant and to be growing.
- The Year 2000 Problem represents a serious vulnerability.
- There is little testing of emergency response plans.
- Government should not mandate requirements in the protection area but rather should develop guidelines.

## 3.3 Electrical Power Systems

Findings in the Electrical Power Systems area include:

- Physical threats (both natural and man-made) is the area of greatest concern.
- Insiders can do great damage to this infrastructure.
- Pending re-regulation of the industry will allow new participants into this arena and thus increasing the vulnerability of the overall Electrical Power System.
- Competitive forces to keep costs low is negatively impacting the vulnerability of this system.

## 3.4 Gas and Oil Production, Storage and Transportation

Personnel in the gas and oil infrastructure expounded on the following basic issues:

- Are concerned for physical threats, including accidents.
- Have greater concern for terrorism (including kidnapping) than most critical infrastructures.

- Believe they are vulnerable to actions/policies of some foreign countries but also to some policies/public opinion in the United States.

- Multi-faceted, multi-national of infrastructure creates many areas of vulnerability.

- Heightened physical security during Gulf War and after World Trade Center bombing, but there is belief that security priority has declined since then.

- Have a variety of emergency response plans which are frequently practiced.

### 3.5 Banking and Finance

The interviewees for this infrastructure expressed the opinion that a considerable portion of the vulnerability to Banking and Finance is through vulnerabilities in the telecommunication industry. Other issues of concern expressed in the interviews include:

- Physical threats to customer-oriented devices, e.g, Automatic Teller Machines.

- Perceptions on the risk of cyber fraud differed among the interviewees.

- Market forces have a significant impact on vulnerabilities as efforts to consolidate produce larger computer systems.

- Competitive forces to keep costs low will likely degrade service and security.

- Simultaneous deregulation and disaggregation of the banking and finance industry and the telecommunications industry at a time when they are becoming more intertwined will increase vulnerabilities.

- Disaster response and recovery plans are based on data backup and inter-industry substitution.

- The Year 2000 Problem is a significant vulnerability to this infrastructure.

### 3.6 Transportation

The interviewees provided a great deal of information regarding the threats and vulnerabilities of the various components of the transportation infrastructure. Specific issues of concern included the following:

- Transportation systems are by their very nature vulnerable to a variety of physical threats, both natural and man-made.

- There is a need for improved technologies in bomb detection.

- Actions for vulnerability reduction have been predominately in the area of crime prevention.

- The industry is generally not prepared ( in training, equipment, or proper planning) to deal with terrorist incidents involving large scale use of chemical or biological agents.

### 3.7 Water Supply Systems

Interviews with water-supply personnel yielded the following findings:

- Infrastructure is less concerned than some others about physical threats because of physical security measures already taken and because of redundancies built into water supply systems.

- System recovery plans exist but are designed for natural disasters and not terrorism.

- Belief is that dilution and treatment make raw-water supply systems less vulnerable to NBC threats.

- Distribution networks are vulnerable to NBC threat. Issue being addressed to various extents through back-pressure protection devices.

- EPA requirement for residual disinfectant in distribution networks lessens vulnerability.

### 3.8 Emergency Services

This infrastructure must deal with many of the natural and man-made disasters that impact the other critical infrastructures. Specific areas of concern include:

- Response-equipment deficiencies exist in many areas and the problem is worsening as fiscal constraints become even tighter.

- Communications equipment is critical to appropriate response to an emergency and this
- equipment may itself be impacted by the emergency.

- Most emergency responders do not have training to respond to an NBC attack.

- Preparedness exercises should be conducted frequently and should have the active participation of decision makers who will be called upon in an actual emergency.

- Some new communication systems that can address emergency service needs are being tested and the results have been promising.

- Funding constraints severely limit the maintenance and enhancement of this infrastructure.

### 3.9 Continuity of Government Services

This infrastructure involves a wide range of services, in a variety of locations. It is thus subject to an equally wide range of threats and vulnerabilities. Specific issues of concern include:

- The infrastructure is subject to a wide range of threats and vulnerabilities.

- The aging and physical deterioration of systems, e.g., water supply systems, sewage treatment systems, or highways, creates a vulnerability for this infrastructure.

- Alternative sites to be used by government service personnel in the event of an emergency is a common method of reducing this infrastructure's vulnerability.

- Most response plans deal with natural disasters.

- There is a need for training in how to respond to terrorist incidents involving NBC agents and there is a need to establish guidelines for the establishment of response procedures to such incidents.

# 4 INFORMATION AND COMMUNICATIONS

## 4.1 General Information

### 4.1.1 Background

The information and telecommunications infrastructure includes computing and telecommunications equipment, software, processes, and people that support the transmission of data and information, the processes and people that convert data into information and information into knowledge. It is a critical infrastructure both in its own right and also due to the fact that it is integrated into almost all facets of operation of the other critical infrastructures considered by the Commission.

### 4.1.2 Organizations

The companies interviewed represent three major components of the information and communications industry: (1) communications and telephone; (2) system, hardware, and network vendors; and (3) software vendors.

A total of eight interviews were conducted as part of this effort. The eight organizations are recognizable leaders in their parts of this infrastructure. Several other prominent organizations in the information and telecommunications industry were contacted but they declined to be interviewed for this effort because they have already been working with the Commission in other phases of their program.

## 4.2 Threats and Vulnerabilities

Several general areas of threats and vulnerabilities were noted during these interviews.

### 4.2.1 Types of Threats

The types of threats identified in these interviews include external hackers (both domestic and foreign), disgruntled insiders, and physical damage resulting from accidents or natural or man-made disasters. The interconnections within this infrastructure can be viewed as both a threat and a vulnerability.

### 4.2.2 Types of Vulnerabilities

Vulnerabilities were categorized as follows:

1. "common thread" - representing the vulnerabilities that are common across the industry, such as host computers and switches; the concern regards access to these systems;

2. "technology unique" - representing those vulnerabilities specific to a new technology, such as broadband or SONET; and

3. “old problems" - representing the older, legacy problems that still exist, such as vulnerabilities from dial-in modems and password files.

Plans for dealing with risk are done at a general level, but no formal risk assessments are performed. Highly vulnerable points and links have been identified throughout the country, as has been the frequency of failures.

In one company, a study of key assets and key processing is under way. This study encompasses approximately 40 software systems, each with more than 200 key components. The evaluation of threats to these systems is currently underway.

Another company stated that modest risk assessments are performed internally each year on a site-by-site basis at different levels, an effort that results in a weakness in the assessment of the infrastructure as a whole. These plans concentrate on physical machines and diskettes with information backup. From time to time, these risks are correlated to financial metrics.

One company indicated that risk assessments of the infrastructure are performed. The frequency and types of these assessments, or "tiger teaming," have increased lately. External groups have also been called in to validate internal assessments or survey the internal infrastructures for vulnerabilities. These contractors perform an independent assessment and have a very free hand in penetrating or compromising internal systems, but, of course, no damage results from this work. The purpose is only to identify the vulnerability. Dollar values for potential losses of information are assigned to these vulnerabilities.

More specific vulnerabilities are summarized in the following sections.

#### 4.2.2.1 New Technology and Trends

The nature of the telecommunications systems is becoming more distributed, with intelligence being built into the separate nodes of the system. This development requires administration of the separate nodes and increases overall system vulnerability. Furthermore, such oversight is being hampered by current personnel constraints, and exacerbated by pressures to improve profitability by downsizing.

A vulnerability is evolving from the proliferation of the Internet, as more people have access to it and the tools available from it. These users are becoming more sophisticated. The result is greater access to tools through the Internet, some of which were placed there for well-intended purposes but can also be used for malicious purposes. Tools have already been used for other than their intended purpose.

With the development of new software based on object-oriented systems in centralized locations, the challenge is to watch the entire network and monitor information across the nation. Customers are more sophisticated now, requiring faster facilities and more bandwidth. Broadband technology is still emerging. The increased number of companies providing services leads to more problems with interconnectivity, system reliability, and security.

Proper firewall installation and administration is critical. Firewalls are the first line of defense against intrusion, and the companies interviewed generally agreed that the protection systems available are working well. One company indicated that it was experiencing more than 100 "pokes" per week at its firewall; however, the security products in place were protecting the systems well. Firewalls, however, are not the total solution to the security issue.

There are thousands of servers on the network outside these firewalls. The potential weakness is that in some cases, for limited times, these servers can connect inside the firewall. These connections, however, are transient in nature.

There is a significant concern about denial-of-service attacks (attacks that would cause the companies to be unable to provide service to customers). Such an attack could delay the order processing business. Applications like order processing are critical components of these

companies, especially at the end of the quarter or end of the year, which are always high-volume processing times.

One company mentioned that it was evolving from monolithic Local-Area-Networks (LANs) to smaller and more secure departmental-type LANs. But a problem in implementation is security versus usability.

The Computer Emergency Response Team (CERT) initiative is extremely important for the protection of systems. Enough information on threats is available, and the representatives of these companies know of good sources for this information. There is a concern, however, that customers may not know where to obtain this information.

#### 4.2.2.2 Hackers and Security Technology

The mindset of hackers has changed from their attitude about two years ago. Previously, they were interested in the theft of information and fraud. Now, there is a subset of hackers who are more focused on bringing down networks or systems and causing outages. There are more sophisticated tools available on the Internet now that can be used maliciously.

The design of security products typically lags behind the technological capability of the hackers to penetrate systems. There is a lack of forward-looking R&D to rectify this problem. Security mechanisms need to be designed as part of the product itself and not developed afterward. Software developers need to anticipate hackers. The consequences of an extreme attack include bringing down an entire network and stealing information or ideas on a product line.

#### 4.2.2.3 Interconnectivity

The vulnerability of systems arises from the interconnection of numerous networks where the entire system is vulnerable to its weakest link. An example is a small, rural telephone company which connects to the major company links. These small providers may not have the funds to invest in proper security. Similarly, breaking down large companies into smaller ones multiplies security problems since all the networks are still interconnected. Small companies with little to invest in security are the most vulnerable and become the weak links. The current trend is toward high profit margins, so items get cut out, and those items usually include security-related items

With the telecommunications reform initiatives, the industry is "unbundling" networks and giving closer access to secure systems to many service providers. The industry has been opening itself up to service providers of varying types and levels of quality. This trend results in multiple accesses to information previously treated as proprietary and available only internally.

Software that analyzes actual failures after the fact does exist, but there is no software that can predict failures. Yet failures have greater impact now because of the interconnectedness of systems and use of bigger "pipes" (cables that now route large amounts of traffic). Breaks in these larger "pipes" affect thousands of people. New systems are emerging that automatically switch traffic when problems are encountered.

#### 4.2.2.4 Foreign Threats

Foreign hackers can penetrate systems in the U.S. by using the Internet. Since laws in these countries may not be in place, punishment or enforcement is often insufficient. U.S. Government agencies monitor various countries for threat information. According to a 1996 GAO report dealing with DOD system attacks, approximately 120 countries are carrying out information warfare. However, penetrations are not always detected. It was stated that 20-30% of companies do not know whether or not they have been penetrated.

In the view of some of the people interviewed in this effort, a major threat to this infrastructure is the foreign ownership of domestic telecommunications companies and security products. Foreign companies own major parts of several U.S. companies or have influence in these companies. In addition, some security products used in the U.S. have been developed by foreign countries, such as the Firewall 1 system developed by Checkpoint Technologies, an Israeli company. Approximately 70% of companies indicate there is a major threat from foreign countries. Through connections with U.S. companies, foreign countries may be able to get information on defense products or other information that is protected. These U.S. companies may not know when information is gone.

#### 4.2.2.5 Operating Systems

Weaknesses in UNIX security have been studied in detail over the past several years. Threats to UNIX are understood, and protection mechanisms have been put in place. However, there is a concern about vulnerabilities because there problems in operating systems are well known.

#### 4.2.2.6 Internet

The Internet is vulnerable to the threat of someone taking down key servers, because they are not running secure operating systems. The Internet servers need a hardened operating system now, as do critical host systems, in case network security is compromised.

In terms of development, the industry is well on its way to the next version of the Internet protocol, which will provide better authentication and thus help in its protection.

#### 4.2.2.7 Insider Threats

Companies are generally more vulnerable to insiders than an attack from the outside. There is not much protection against insiders because employees need access to certain stores of information. The industry is also concerned about the insider threat and estimates that 70-80% of the overall threat is from the inside.

A major threat comes from disgruntled employees and their number is growing because of stiffening economics and downsizing. This is the biggest security threat to companies. Outsourcing has increased this vulnerability as the number of contract employees increases.

#### 4.2.2.8 Virus Protection

Viruses range from an annoyance to a potentially serious problem. To avert the threat of virus attacks, incoming disks are scanned. In March 1997, the Computer Security Institute (CSI) and FBI study estimated that virus incidents cost approximately $12,500 per incident.

#### 4.2.2.9 Natural and Human-Caused Disasters

A significant vulnerability to this infrastructure is its susceptibility to natural disasters and digging accidents. Because of the predominant use of railroad rights-of-way, cables can be easily cut by accident. Currently, maps are the primary sources used to locate cables. Geographic information systems (GISs) are needed to track where cables are laid. GISs are in the early stages of deployment within the industry.

The firms interviewed contact each other for assistance in cases of major disasters. Additional capability can be leased from competitors as needed. There are mutual aid agreements in place among the industry members, including common vendors. The North Dakota floods and California earthquakes are examples of where cooperation was provided.

#### 4.2.2.10 Year 2000 Problem

The people interviewed expressed the idea that the Year 2000 Problem should be a priority for the Commission. An enormous number of systems may inadvertently shut down or function improperly because of this problem. Not only will the information and telecommunications infrastructure be impacted, but virtually all other business and industries in the U.S. are potentially impacted to some degree.

### 4.2.3 Security Tool Developments and Analysis

A business impact analysis (BIA) model exists to assess vulnerabilities. This BIA methodology analyzes disasters in 11 areas of the infrastructure and attempts to quantify measures of protection. This is essentially an approach, model, or guideline to analyze the impact to the business. It removes subjectivity and indicates where to spend security dollars.

In security protection, there are tradeoffs between applying the best security all over and using a diversity of security tools and between using the latest equipment or products versus using proven, secure, but older forms. Diversity is important for safety. If one set of tools is compromised, the entire system is not subject to compromise when a diversity of tools is employed.

To enhance system reliability, one company noted that it has established a Self Healing Alternate Route Protection (SHARP) service that provides for two physically separate routes to provide security for fiber-optic facilities carrying traffic. In the event of cable failure, traffic is routed to the alternative path within 50 milliseconds. This company also has a Self Healing Network Service that employs concentric ring technology to link multiple locations via fiber optic facilities. If a failure is detected, this system can reconfigure itself and restore service within 50 to 245 milliseconds.

## 4.3 Requirements and Standards

There are two major components in the telecommunications industry: switching and transmission.

On the switching side, there is an Asynchronous Transfer Mode (ATM) Forum for high-speed data switching which attempts to define standards for this portion of the infrastructure.

On the transmission side, in the Synchronous Optical Network (SONET) area, there is a standard interface to connect equipment (a de facto standard). The T1 Committee of the Alliance for Telecommunication Solutions is an industry body that is driving transmission standards.

Each developer of hardware wants to use its own system to manage the device. Standards are needed in this area to provide the capability for an integrated service management system. There are no standard ways to connect different types of telephone gear.

There are problems with regards to international standards. For example, T1 speed in the U.S. means 1.544 Mbps, while in Europe it means 2.048 Mbps. This results in an immediate interconnect problem. The Consultative Committee for International Telegraphy and Telephone standards should be followed by all countries to abate this problem.

The companies interviewed have mixed views on the government working to develop standards with some believing that the government should work in the area of metrics and standards to help guide industry. Other interviewees however expressed the opinion that standards should be set in the marketplace, not in government. The Internet Society and International Telecommunications Union (ITU) are driving some standards development. The government should encourage

appropriate groups of engineers to settle on the standards issues. Standards are in fact, being worked on in the industry; an example is the Key Recovery Alliance which is an alliance of 53 companies that works with the government.

## 4.4 Emergency Plans

There was little discussion of emergency response or recovery plans during these interviews. Among the comments were that:

- Actual drills and testing are needed to verify recovery plans, but these have not been done yet.
- Disaster recovery plans are prepared but documented inconsistently.
- A lack of adequate disaster recovery plans, particularly for recovery from natural disasters, is a weak point.

It was noted on several occasions during these interviews that restoring the product line and delivery of customer services are major considerations in dealing with incidents that disrupt the industry. One company referred to their emergency response plans as business continuity plans.

## 4.5 Information Exchange

### 4.5.1 General Information

The companies interviewed tended to be quite active in monitoring information from various groups, conferences, and forums. For example, staff at one company have chaired the National Security Telephone Advisory Committee (NSTAC) Committee to the President for several years. The NSTAC was created when the Bell system underwent divestiture and the government was concerned about security.

The National Security Information Exchange (NSIE) is a forum through which the communications industry meets with the government to share information on threats and vulnerabilities. The Network Operations Forum is an industry committee that has monthly meetings on operational issues and addresses common operational problems. The National Reliability Forum was also noted as a means of communication within the industry.

Many of the companies interviewed indicated there is significant interchange of information with universities. The National Colloquium for Information Systems Security Education was recently held and felt to be a good forum.

### 4.5.2 Threat Information

The companies have different views on whether they obtain sufficient, complete, and timely information provided about potential threats.

Various organizations provide information on potential threats. Information is available from the Computer Emergency Response Team (CERT), Computer Incident Advisory Committee (CIAC), and Forum of Incident Response and Security Team (FIRST) groups and from subscriptions to mailing lists like **greatcircle.com**. In addition, the firewall companies provide protection and vulnerability information. The Federal Communications Commission is another source of information on threats and vulnerabilities.

Technical journals provide information on potential threats before organizations or forums have an opportunity to discuss them. They are timely and complete enough for the industry to assess the threat. The government also provides e-mail notices on potential threats.

While organizations like the Computer Emergency Response Team (CERT), the FCC, trade associations, and professional societies track threats in databases and conduct trend analyses, there does not appear to be complete data on actual incidents nor is the information always timely. Information is shared through bulletins, but no company names appear. Although anonymity in reporting problems fosters more complete reporting, it cannot totally solve the problem of offering comprehensive information. Information on outages and vulnerabilities should be separated into the technical problem (general information on what actually happened) and who was affected (private information only to be used by law enforcement and the courts).

Information needs to be shared with other infrastructure areas as well. There is a need to formally link up with these infrastructures, regardless of what their perceived needs and vulnerabilities are. Threats and vulnerabilities can then be categorized by technology.

### 4.6 Research Needs

The interviews indicated that a significant amount of research is under way, either by the companies working on their own or with universities, vendors, National Security Agency, and the Army. Specific areas suggested for continued research include:

- Encryption devices and techniques
- Broadband technology
- Firewalls and token authenticators
- Security systems with many integrated components
- Security metrics
- Autoimmune systems, which automatically detect intrusion, even through new forms
- Intrusion detection techniques and tools to address the increasing level of attacker sophistication
- Nonintrusive security systems
- Modeling and simulation tools from an emergency preparedness perspective
- New technology and retrofits on existing equipment to deal with new wire tap laws
- Software integrity
- Better network and security management
- Improvements in intelligent agents to assess vulnerabilities
- Algorithms for improved speed and reduced vulnerabilities (including cost/benefit analyses)

### 4.7 Government Role

The consensus of the companies interviewed was clearly that the government should not develop more mandates or requirements.

The government should provide guidelines, not mandate additional requirements. The industry could use help in forming partnerships. Complying with the Communications Assistance for Law and Enforcement Act (CALEA) is a major problem for the industry since the law is so encompassing and so specific. Yet the fines are heavy (perhaps $10,000/day) for noncompliance, and no one is knowledgeable in the technologies needed to comply. The most effective role for the regulators is as a persuasive presence to insure the timely adaptation of the industry to changes being experienced, rather than the time-consuming practices of rule making.

Consistency is needed in government policy. Particular examples of perceived inconsistency deal with encryption technologies and export policies.

Penalties for violating a range of laws covering breaking cables and lines to hacking need to be vigorously enforced and with greater penalties.

The issue of foreign ownership in domestic telecommunications companies needs to be addressed. Canada was cited as a good example of a country with strong controls; it precludes foreign ownership in infrastructure companies and restricts the flow of data out of the country.

The following were identified as specific areas where the government could play an important role:

- Spearhead conferences and working groups to share information among government, industry, and academia;
- Provide seed money for research;
- Coordinate information on threats;
- Provide guidance on the interpretation of court orders;
- Promote collaboration and encourage and fund discussions in a vendor- neutral forum;
- Provide tax credits to encourage companies to conduct research that they otherwise might not conduct;
- Develop a standard for the evaluation of risk in this infrastructure; and
- Be the focal point for an international focus on security.

### 4.8 Other Areas of Interest or Concern

Several companies voiced the opinion that they regard the Commission's work as very important and recommend continuation of such efforts, with their participation. It was mentioned that the Commission has a very large task ahead.

There is a concern that the telecommunications industry needs an "end to end" focus because it consists of so many providers, all with differing levels of security. One weak link in the chain can introduce a vulnerability.

Pressure and encouragement are needed to use the security tools that exist. This encouragement can be provided through educating the user community on what is available.

The companies interviewed differed somewhat in their opinions on the education that graduates are bringing to the workplace. Several indicated that the process is adequate, and others indicated that the training is too theoretical and graduates need more technical training provided by the company on the job.

University programs appear to be functioning acceptably. Graduates are generally able to function in the industry with a little training. However, they tend to have fewer and narrower skills than they need. There are not enough programs and not enough graduates. There is a need for many more qualified graduates. The new graduates from universities have no idea of security and view it as a constraint instead of a protection.

# 5 ELECTRICAL POWER SYSTEMS

## 5.1 General Information

### 5.1.1 Background

The U.S. electric power industry is composed of traditional electric utilities (investor-owned, municipals, cooperatives and federal utilities); non-traditional electricity-producing companies (non-utility generators and independent power producers); and, as a result of restructuring, power-marketers and brokers. Electric utility systems have historically operated as a regulated monopolies however recent legislation has opened the industry to competition requiring open access to the power grid.

Overall reliability planning and coordination of the interconnected power systems are the responsibility of the North American Electric Reliability Council (NERC) which consists of 10 regional councils and one Affiliate. NERC is responsible for protecting the reliability of the generating and transmission network for virtually all of the electric utilities in the U.S. The purpose of the regional councils is to promote the reliable use of the interconnected electric systems with regard to safety, environmental protection, economy of service through coordinated planning, construction, operation, maintenance, and use of generation and transmission facilities.

Interviews were conducted with representatives from the operations, transmission, coordination, and reliability elements of the electric-power generation system. Staff members from NERC and a regional reliability council were contacted for information regarding their perception of critical infrastructure vulnerabilities. Other utility security and operations staff were contacted on behalf of the Commission but declined to be interviewed and indicated that the Edison Electric Institute is the appropriate point of contact for the industry perspective.

### 5.1.2 Organizations

Representatives from the generation portion of the electric power system were from two large, investor-owned utilities. Each is the primary provider of electricity to a major metropolitan area. They provide electricity to major business communities in the United States and to a general population in excess of 5 million. The peak electrical demand in each of their service territories is in excess of 10,000 megawatts. One of these generators produces the majority of its own power while the other operates its own generation capacity to meet approximately 50% of the demand. The remainder is purchased from independent power producers or from other utilities.

Electricity is delivered by underground cable and overhead wire. The flow and distribution of electricity is managed by computer from central control centers. There may also be backup control centers should something happen to a main control center.

NERC and its regional councils are responsible for setting operational guidelines for reliability with respect to generating and transmission facilities for the electric power system. The regional councils play a primary role in coordinating construction, operation, and transmission planning of the member utilities in its region. The regional councils of NERC play a major role in electricity transmission through their coordination efforts and member utilities manage the operational aspects of the generating and transmission facilities. The regional councils monitor overall system operations in order to guarantee reliability of service throughout their entire region.

### 5.1.3 Infrastructure Involved

The basic electric power system infrastructure consists of generating plants, a transmission system, a subtransmission system, a distribution system, and a control center. The power grid, which allows the interchange of electricity between utilities, is formed by the interconnection of transmission systems. The control center monitors a utility's generating plants, transmission and subtransmission systems, distribution system, and customer loads. The primary function of the control center is to monitor system operations and provide for manual or automatic control of field equipment.

## 5.2 Threats and Vulnerabilities

According to managers of one of the generating companies, 2 elements of the distribution system can be lost (due to fire or other disaster) without the customer noticing more than a flicker in the lights. This is partly because of a tremendous redundancy built into the system, and partly because most of their power lines are underground. All equipment at their switching stations has been raised above potential flood level as a result of lessons learned from a previous natural disaster. More recently, a fire in a substation resulted in a four-day, local power outage. A major issue resulting from this outage has been the priority for restoring service to various areas and customers. Lessons learned from that incident are being applied in a multi-million dollar program for upgrading 50 substations.

The system is generally designed to protect only against credible events. From the planner's point of view, analyses done to assess system reliability and security are sufficient to guard the system against credible events and events that, though less probable, are more severe. Special protection measures such as load shedding schemes using under-frequency and under-voltage relays are considered to be sufficient to protect the system. The act of deliberate sabotage, however, is never considered in these assessments. Planners are more concerned with what actually happens and its impact to the system rather than the cause of events. Operations people are knowledgeable about real-time emergency events and the appropriate manual or automatic system response.

Deregulation presents many challenges to the electric power system, particularly during this transition phase. Deregulation has given rise to a new set of entities or players in the industry. The challenge of conveying accurate and voluminous information for use by these new power players is great. The change in market structure adds a great deal of complexity and uncertainty to traditional generation and transmission planning. A major concern is that system security and adequacy of service will be more driven by least-cost options than by reliability considerations.

### 5.2.1 Types of Threat

Specific threats to the generation and transmission system, e.g., physical threats to facilities due to natural hazards and equipment failures, were identified as the primary concern. Transformers and substations, readily identifiable pieces of equipment typically found in isolated locations, have been traditional targets for vandalism and common criminal activity. It was stated that, if someone knew what they were doing, they could black out the service area for an extended period of time.

No specific cyber threats were identified but standard precautions such as firewalls, password protection, dial-back modems are being taken to increase system security.

One of the electricity-generating organizations noted that in their last major blackout (lasting 24 hours), losses in the hundreds of millions of dollars were estimated to have incurred. The largest

loss was caused by arson and looting.[1] The provider has made arrangements (a Memorandum of Agreement) with a large customer to use their backup generators in an emergency affecting specific areas of the service area.

### 5.2.2 Vulnerability Assessments

The generators would not discuss their vulnerability assessments beyond stating that they learn lessons from exercises and drills, and from real-life experiences.

Vulnerability assessments conducted by MAIN include transient stability, load flow, and line transfer capability. A scenario approach is employed to evaluate several simultaneous inter-regional transactions under various contingency and non-contingency conditions.

Although reliability assessments are conducted, these generally do not evaluate the impact of a planned or deliberate sabotage attack, but rather focus on disruption due to equipment failure and natural hazards. The opinion expressed was that someone knowledgeable in bulk electricity power supply could feasibly cause a major system disruption through the identification and elimination of key substation and/or transmission components. For example, it was discussed that someone could potentially develop and implement a scheme to destroy certain components which are not stocked, thereby causing a total system collapse that could have a comparatively long recovery time.

Factors that contribute to the importance of a particular component to the overall system include susceptibility to damage, impact on the power system, and difficulty of replacement. Target components could be easily identified by persons with a background in power systems using open source information such as transmission maps and FERC filings.

The volume of detailed information that is publicly available is a frequently mentioned concern. There was considerable reluctance on the part of those interviewed to disclose specific areas of vulnerability. The opinion expressed was that such sharing of specific threat and vulnerability data should be done only in a framework which guarantees restricted access and confidentiality. Dissemination of information on the identification of critical infrastructures, measures taken to protect them, and recovery plans is viewed as detrimental to system security.

#### 5.2.2.1 Assessment Methods

A combination of probabilistic and deterministic assessment methods is used to evaluate system reliability. To determine the adequacy of the generating system, regional NERC councils annually conduct detailed probability studies looking 10 years into the future. The criterion used in these studies is an LOLP (loss of load probability) of one day in 10 years.

Power flow studies are used to evaluate the adequacy of the transmission system. These studies are conducted annually to determine line reinforcement needs. MAIN, for example, conducts transmission planning analyses on a daily basis to assess line loading levels based on operational and sales information. Advisory messages are then relayed to member utilities if a there's a need to adjust operations to obviate line overloading and increase transfer margins or capabilities. MAIN also issues contract curtailment advisories for specific transactions which may overload a critical lines.

---

[1] Source: U.S. Congress, Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disaster and Sabotage*, OTA-E-453, June 1990. For a breakdown of these costs, see ANL study for the Commission on the vulnerability of the electrical generation and distribution infrastructure.

Most of the transmission simulation tools are deterministic. Such tools include Power Technologies Inc.'s Power System Simulator for Engineering (PSS/E), Transmission Planning and Reliability (T-PLAN) and Multi-Area Reliability (MAREL) software. The EPRI product VSTAB is used for voltage stability analysis. Typical transmission analyses will simulate system operation at various load levels. Generation planning studies usually use probabilistic methods which incorporate system reliability measures such as LOLP and LOLE (loss of load expectation) to drive capacity expansion decisions.

#### 5.2.2.2 Areas of Vulnerability

Security at control centers and other sensitive locations is very high. However, at locations such as substations, security is not provided by human guards 24-hours a day. The facilities are locked, and there are signs warning of high voltage which keeps most intruders away. Nevertheless, there have been some incidents of vandals climbing fences to steal copper wire (which can be readily sold). Some of the vandals do make mistakes and are killed in the process because of the high voltage. However, the fact that amateurs can get in and steal material is of concern. There is also the worry of an inside job . Employees references are checked, but it is still difficult to be sure of someone's true intentions.

Monetary constraints and financial considerations are viewed as contributing significantly to system vulnerability. Upgrading or replacement of aged equipment such as breakers entails cost and funds that are often limited. Improvements, especially in the distribution level, have to be prioritized for funding allocations. All needed improvements are essential for system reliability but not all could be implemented because of funding difficulties. Operational vulnerabilities are more significant at the distribution level than at the transmission level (high-voltage) because of the radial structure of distribution delivery system. At the transmission level, the network tends to form loops that increase system reliability.

Concerns stemming from impending changes in the electric-utility regulatory environment were expressed. Uncertainty regarding system planning and the quantity and quality of the data needed for daily market operation was a recurring concern. Information must be transferred to and from the power brokers for processing, scheduling and coordination. The increased volume of transactions and retailing are likely to cause significant problems in the overall communication system. Information must be transferred to and from the power brokers for processing, scheduling and coordination. Those interviewed expressed the opinion that deregulation is moving too fast and were concerned that the utilities and their control centers would not be able to adjust to the new developments and requirements adequately.

A problem concerning the acquisition of data needed to run the increasing complex software for electricity transmission was identified. In a recent IEEE Power System Meeting, an issue was raised on the uneven level of sophistication of equipment used for data acquisition, telemetering, and transmission. Some of the equipment in the field was installed in the 1950's and couldn't support modern information transmission protocols. Other equipment has insufficient memory to meet the requirements of the new protocols. This is a vulnerability area in the power system control and operations. While the technology to elevate the quality of data acquisition equipment is available, the question of who is willing to fund the purchase of the new equipment remains a huge issue.

Reduced total system reliability is another principal concern rising from the opening of competition. The traditional generation planning approach will no longer apply as independent power producers enter the market and account for an increasing share of total generation. The changing structure of the electric industry is an important vulnerability, particularly during this transition phase.

The importance of coordinating power sources and loads in an open-access environment makes timely information exchange even more significant. In accordance with the FERC ruling of open access to third parties of the transmission system, several NERC regional councils established an open-access, same-time information system (OASIS) node. Information exchange and coordination is heavily dependent on computer integrity. In this respect, cyber attacks have a higher potential of posing a significant threat to system operations.

There is a current concern about the adequacy and security of service in parts of the United States because of the anticipated unavailability of significant amounts of nuclear generating capacity. The generation shutdowns of the units are due to various combinations of physical plant, operator, and regulatory issues which have increased the uncertainty in the return dates for these units. NERC has performed a summer assessment of MAIN and offered its recommendations.

#### 5.2.2.3 Levels of Risk

In preparation for the near-term threat of disruptions in service, MAIN has enhanced its analytical capability, reinforced its transmission systems, increased maintenance, and sought other sources of power. Despite these efforts, the combination of limited generating capacity and transmission availability are likely to cause loss of service in some areas.

#### 5.2.2.4 Impact on Other Infrastructures

Electricity is a vital resource to many residential, commercial and industrial activities. Loss of electrical services would thus dramatically impact routine functions throughout the economy. Specific examples cited by one of the generating organizations included the following examples. The water supply in the service area is not particularly dependent on electricity as it is primarily gravity fed, so only an extended blackout would affect water supply. The transportation system is dependent on electricity for running the subway, for streetlights and stoplights, for air traffic control, for bridge and tunnel safety, etc. The communications system would be severely affected by a lack of electricity, which would bring the financial markets and most other commercial activities to a standstill. The emergency services system is somewhat dependent upon electricity, but would still function in a blackout using radio communications systems and people deployed to the area (they would have to function in order to maintain safety and order).

### 5.2.3 Vulnerability Reduction Actions

The generation organizations did not discuss specific actions they have taken to reduce vulnerabilities. The electrical energy system has a great deal of redundancy built into it. Also, since many of the electrical lines are buried, they tend to be relatively trouble free, unless they are accidentally severed when the street is being worked on (for a water main break, for example).

Money is viewed as one of the main constraints in decreasing system vulnerability. Investment in system security must compete for limited funds with other programs and projects. In addition, regulatory and environmental considerations also hinder implementation of measures that could help improve system reliability.

Preventive measures could be implemented to avoid accidents that would threaten system security. For example, substations could be placed on higher ground to reduce the threat of floods. However, in one instance, after the relay sets were elevated, fire hit the pipeline carrying the cables to the relays. Accidents such as this still threaten system security. Thus, conventional fire-prevention systems and awareness should continually be in effect to lessen vulnerability. Detailed reporting and analysis of accidents or disasters could lead to more effective preventive measures.

Human error, like construction crews hitting underground cables, are often the cause of service disruptions. Measures to prevent such accidents should also be developed and implemented.

Maintenance is critical to system performance. Regular testing of relay and breakers is very essential to system protection. Current maintenance work on breakers is satisfactory. Breakers and related equipment are checked every two years. Sometimes maintenance had to be skipped because of the presumption that the breakers are working anyway and because of cost consideration

## 5.3 Requirements and Standards

None of the interviewees provided information on this issue.

## 5.4 Emergency Plans

### 5.4.1 Response Plans

Electric utilities have plans for emergency situations. One of the utilities discussed how, in case of a total black out resulting from severe system disruption, it would initiate recovery actions using their gas-fueled peaking plants. These peaking plants could be made to generate power from black start. Specific units for black starting have been identified. The generated power from these units could then be used to trigger the start of larger oil and nuclear plants.

Special protection schemes for line loadings have been developed that not only isolate faulted lines, but also can trigger load shedding actions to maintain system adequacy. Computer simulations are used to test the effectiveness of the schemes developed. When collapse of the system (either partial or total) is sensed to be forthcoming, the utility determines and implements appropriate switching operations to obviate further spread of disruption. It may be noted that in the case of the service disruption at WSSC, although there was initial failure of some of the front-line relays, the back-up relay protection actually help to limit the blackout to affect just 3 million people. A lot more people could have been affected had it not been for the protective relaying system in place through out the network.

MAIN conducts a look-ahead (one day look ahead) planning that assesses loading levels of lines based on operational and sales information provided by member utilities. Advisory messages are then relayed to member utilities if a there's a need to adjust operations to obviate line over loading and increase transfer margins or capabilities. MAIN also issues a contract curtailment advisories for specific transactions which may overload a critical lines.

For cases where deliberate sabotage is suspected, the utilities report the incident to FBI to ensure system security. This response has been taken following a major disruption affecting one of the utilities interviewed.

The other utility interviewed noted that there is a Sabotage Procedure, a procedure to adjust the way the power is distributed. They have Mutual Aid Agreements (through the Edison Electric Institute - EEI) with area utilities who will provide aid to their service area when needed, just as they have provided assistance in the past.

### 5.4.2 Exercises/Drills

At least one of the utilities interviewed has drills for black starting and they do have emergency procedures as embodied in their manuals. Emergency Rehearsals or drills have been stopped because of risk of service disruptions and cost considerations.

One of the utilities noted that when the city has drills and exercises, they participate and send a liaison to the City Emergency Operations Center. They also have their own emergency operations center with direct telephone lines to the Mayor's Office of Emergency Management (with whom they have an excellent working relationship), the Coast Guard, and other agencies they would need to work with. They have considerable resources of their own that they can muster in an emergency, including trucks, people, equipment, etc.

The above utility conducts annual drills to test its emergency plans and procedures. Copies of the plans were not available for review

#### 5.4.3 Communications/Command

The importance of maintaining functional communication links among various stations during emergencies was emphasized. The links are important to coordinate recovery or restoration procedures. The use of emergency batteries to power relays and breakers are some of the measure already in place. Emergency power supplies should also be place to power communication equipment. This aspect of preparedness is well-addressed by most utilities.

### 5.5 Information Exchange

One of the utilities expressed concern regarding the significant increase in information requirements that are likely to develop as a result of re-regulation of the electric utility industry. Some of these concerns have been previously discussed in the context of system vulnerabilities (Section 5.2.2.2).

### 5.6 Research Needs.

Some experts expressed the opinion that a structural design for compact transmission lines is needed. Such a design would allow more line capacity to be added in space-limited transmission corridors. As the system grows, more lines are needed to improve transfer margins and therefore increase system security.

**5.7 Other Areas of Interest/Concern**: The provider is concerned that increased deregulation of both power generation and distribution will increase competition to such a degree that the mutual aid cooperation that exists now may suffer as a result. In addition they are concerned that as the system becomes more open as a result of deregulation, that security of the system will decrease.

# 6 GAS AND OIL PRODUCTION, STORAGE AND TRANSPORTATION

## 6.1 General Information

### 6.1.1 Background

The gas and oil production, storage and transportation infrastructure is one that provides energy to a wide spectrum of the U.S. economy and for private consumption. It includes the production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent on gas or oil.

### 6.1.2 Organizations

A total of six interviews were conducted for this infrastructure. They included some of the largest energy corporations in the United States and involved individuals with a wide range of responsibilities. These organizations are typical of the "oil majors" that are involved with the entire process from fossil fuel prospecting and production through final sale to customers. An interview was also conducted with a private firm providing security and safeguards consulting principally to the petroleum industry.

### 6.1.3 Infrastructures Involved

In addition to the oil and gas infrastructure, this industry has major impacts on many others identified as critical to the nation, including transportation, electrical power systems, government services, and emergency services.

## 6.2 Threats and Vulnerabilities

### 6.2.1 Threats

This infrastructure must address a wide variety of threats. Physical threats from natural disasters and terrorism (particularly to the foreign components of the infrastructure) are of great concern to the industry. In pipelines one concern is that leaks will develop due to corrosion or damage by third parties, e.g. construction workers. Human error is also of concern because of the potential to cause a major accident. Sabotage, particularly on foreign operation, is also viewed as a serious threat. The industry also views cyber threats as a big concern. Certain policy actions, either domestically or by foreign governments, are viewed by some as potential threats to the industry. Environmental terrorism was also viewed as a serious threat. Kidnapping and other hostage threats and chem/bio threats were also noted to be of major concern.

### 6.2.2 Vulnerabilities

All interviewees noted that the vulnerable assets include injury or loss of life to employees and/or the public as well as significant monetary quantities. Several interviewees expressed the thought that the basic industry is sufficiently resilient to recover from a significant loss of supply capability from a single company as long as such a loss was not propagated to the rest of the industry.

The multi-faceted and multi-national nature of this infrastructure creates many vulnerabilities. Among the more vulnerable facilities are tank farms, refineries, and chemical processing plants. For example, an explosion at a refinery could release of hydrofluoric acid into adjacent communities. There is significant vulnerability through tankers and marine transportation/handling systems, including port facilities. The greatest vulnerability (in terms of economic effects) for one company is considered to be a major tanker spill, regardless of the cause. It could financially ruin the company. After the Exxon Valdez accident, many other major oil companies sold off their tanker fleet and now contract for transport services. This makes the industry somewhat susceptible to pressures from the countries of registration that wish to disrupt crude movement/supply. Pipelines are quite vulnerable but there is a recognition that not everything can be monitored and protected to the same level. There is a common feeling that their vulnerabilities are much greater overseas than in the United States.

Some in the industry believe that they are vulnerable to the public opinions and politics surrounding global warming because they could lead to a reduction or an outright ban of hydrocarbon exploration and production. Furthermore, some of them feel that the concept of Sustainable Development, strictly interpreted, potentially jeopardizes their industry if it concluded that the nation must drastically reduce consumption of natural resources.

Financial vulnerabilities lie in abandoned equipment and facilities ranging from old refineries to pipelines to drill stem/pumps, etc. at abandoned wells. Any major cleanups and disposal problems that arise would also create a financial liability.

One company expressed strong concern for environmental terrorism. They noted the bombing of gas stations and other such acts in Germany and Europe stemming from the announced plan to dispose of a North Sea drilling platform by sinking it. They stated that environmentalists extreme actions caused the plan to be canceled. They noted that Greenpeace “attacked” and marched on a overseas office of another large company to protest proposed oil exploration activities in the Atlantic Ocean.

More and more daily operations are based on computers and many of the interviewees expressed the concern that protection from intrusion may not be adequate. At least one interviewee expressed the opinion that cyber threats are not mission threatening but would rather, serve only to impact operations and general efficiency.

#### 6.2.2.1 Assessment Methods

Vulnerability assessments are typically done informally and involve specific facilities and locations. Emphasis seems to be placed on vulnerability assessments of overseas assets subjected to terrorist activities. The assessments are site-specific and case-by-case and are developed on the basis of staff knowledge and experience. It does not appear to be common practice to conduct systematic and integrated, company-wide assessments, but rather, each location/facility is to identify a worst case scenario, and then plan for prevention and response.

#### 6.2.2.2 Vulnerability Reduction Actions

A variety of vulnerability reduction actions were discussed during these interviews. Most of them dealt with enhancement of physical security. For example, it was noted that during the Gulf War (Desert Storm), many companies increased their corporate awareness of threats and enhanced security measures, primarily at marine and coastal facilities. Some interviewees however suggested that the level of awareness has lessened following the conclusion of the Gulf War. The bombing of the World Trade Center was also cited as a stimulus for heightened security.

Operational practices instituted to reduce vulnerabilities include accident prevention measures, increased safety awareness, and operational awareness of potential threats and consequences. In general, access control and surveillance of critical facilities has become more stringent in recent years. Most companies have emergency management plans, and have extensive training and drills for these plans. Companies routinely have their pipelines examined with smart pigs.

Some of the interviewees conveyed the feeling that there is a general feeling in the industry (at least with the decision makers) that the perceived risk is sufficiently low so that spending large amounts of funds on added safeguards and security against terrorism. is not justified. Most organizations want inexpensive programs and procedures, equipment, staff, etc. that do not interfere with routine operations. Several interviewees expressed the thought that the economic squeeze is such that if corporate policy doesn't stipulate an action or if regulations don't require it, it won't get done.

The industry uses off-the-shelf technologies for security. Included are items such as video, closed-circuit TV, and physical security/access control measures.

## 6.3 Requirements and Standards

### 6.3.1 Existing

There are regulations for operations (e.g. OSHA) and environmental concerns (the Clean Air Act), but nothing to safeguard a community near a major facility from security-related problems. For example, there are chemical plants with minimal security that pose a hazard to adjacent community. Hydrostatic testing of pipelines is also required on a periodic basis.

There was considerable discussion of an EPA requirement that emergency/disaster plans be posted on the Internet. The concern is that such information will provide potential terrorists with important information on the vulnerabilities of a facility.

### 6.3.2 Suggested Changes

There is a need for standards for businesses to protect employees and citizens from sabotage and catastrophes. Some interviewees also suggested a need for requirements for more stringent access control/security.

At least one interviewee felt that the required/prescriptive hydrostatic testing of pipelines is not necessary and that it generates large volumes of contaminated water that must be dealt with.

This interviewee would also like to see the FCC be more lenient/proactive in making more radio frequencies available for emergency response.

There was strong consensus that changes should be made to the practices in which regulatory agencies make detailed information on company infrastructure available and accessible to the public. Specific data, maps, facility operational data that are required by governmental regulations become readily available to public. This practice should be eliminated.

## 6.4 Emergency Plans

Before the accident with Amoco Valdez and the resultant major oil spill, this wasn't a major concern in the industry. After this incident, all companies with tankers developed emergency response plans, conducted drills and exercises, formed response teams, etc.

### 6.4.1 Response Plans

Most companies in the industry have plans for all their major facilities, both domestic and international. Drills or exercises are routinely conducted, often as a joint exercise with other companies. The Coast Guard routinely participates in those exercises involving off-shore or coastal facilities. Plans tend to be focused on industrial accidents, fires, etc. with minimal planing for terrorism. The American Petroleum Institute (API) has committees and an oversight role for emergency response.

### 6.4.2 Recovery Plans

Some large companies have contingency plans for ensuring operation of the larger infrastructure in the event of a refinery outage, pipeline problems, etc. For example, pipelines are not operating at capacity so that pipeline facilities can be shared with other companies during and after an emergency.

## 6.5 Information Exchange

The exchange of information among oil companies is felt to be good following improvements over the last few years. However, anti-trust issues tend to counteract collaboration among larger companies.

Several professional organizations exist where security information is exchanged and discussed. The American Society for Industrial Security (ASIS) which has 20,000 international members was specifically noted. Also mentioned was the American Petroleum Institute which has an oversight/coordination organization serving the industry, although some interviewees felt that very little consideration is given to security-related issues. Also noted were the Petroleum Industry Security Managers Association, the International Security Management Association (400 members with two major meetings per year), and the Petroleum Industry Security Council.

It was suggested that the API serve as organizer of meetings with high-level industry and security personnel with the objective of identifying various innovative attack scenarios and evaluating security and response measures to see if they are adequate to prevent, protect, respond effectively, etc.

## 6.6 Research and Development

### 6.6.1 Needs

A general need for improved technologies and practices to keep pace with more educated and trained terrorist forces was cited. Specific technologies included improved monitoring and detection technologies/methods. Monitoring of remote facilities from a central location was repeatedly cited as a major concern for which there is no satisfactory solution. The ability to detect explosives was also cited as a area where improvement is needed as was improved computer protection technology and methods.

A need for better equipment for sending alarm notices to all involved parties was cited. Apparently many organizations use unreliable telephone systems.

### 6.6.2 Schedule

Some interviewees expressed concern about technology cycles, particularly the long lead time for technology advancement. They felt that there is a critical need in the United States is to develop a base level of technical expertise and to maintain it to ensure availability of new technologies and to maintain international competitiveness.

### 6.6.3 Role of Government

Several interviewees expressed the opinion that the federal government should define threats and set clear guidelines as to where industry needs to be regarding the issue of safety from terrorism. Possible responses to these threats should also be developed. However, the methods to meet these guidelines should be left to the individual companies involved. Several interviewees also expressed the sentiment that there is no need for government supervision, oversight, or regulations in this area.

The role of government in providing intelligence information was discussed. The industry currently receives bulletins with important information from the government, but it was felt that better access to this information would be beneficial.

It was felt that the federal government should take steps to modify its public information practices by keeping appropriate information and data on the industry secure. The industry looking for support from government via the criminal justice system, in the intelligence community, and through education.

At least one person expressed the thought that government has a role in supporting necessary R&D because individual companies probably will not under the current economic conditions.

## 6.7 Other Issues

Some individuals from the oil and gas industry participated in the Commission meeting held in Houston in the spring. Some had also been involved in Commission meetings in Washington, DC. Many of the interviewees actively support the concept undertaken by the Commission and believe in the need for being prepared.

# 7 BANKING AND FINANCE

## 7.1 General Information

### 7.1.1 Background

The banking and finance infrastructure encompasses the retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and the associated operational organizations, government operations, and support entities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.

### 7.1.2 Organizations

The organizations interviewed represent a comprehensive cross-section of the banking and finance industry. The individuals interviewed are fully cognizant of the range of infrastructure-related issues, including corporate security, operations, physical and cyber threats and vulnerabilities, relevant surety research, and disaster recovery. Organizations interviewed include a major U.S. holding company providing a wide range of financial services; a mainstream trade organization representing the full spectrum of the financial services industry, including more than 90% of the nation's commercial banking assets, and which has been very involved with the development of electronic commerce and on-line banking since its inception; a large international organizations providing financial services to 50 million customers throughout the world; an industry trade association of telecommunications providers, state regulators, and others whose aim is to maintain the high quality and reliability of the domestic public switched network (PSN); a membership-based, not-for-profit trade organization representing the electronic commerce industry whose members deliver financial information and services through online networks via computer and home appliance systems. This organization is involved in PC banking, Internet marketing strategies, virtual banking, e-cash, cyberspace regulation, PC/TV convergence, open and private banking systems, digital cash, TV banking, interactive systems, electronic checks, standard payment protocols, smart cards, and web cards. The remaining organization interviewed for this infrastructure is a state Office of Banks and Real Estate which has supervisory and/or regulatory responsibilities for state-chartered banks and trusts.

### 7.1.3 Infrastructures Involved

The information and communications infrastructure appears to be the most obviously vulnerable infrastructure that the banking and finance infrastructure is dependent upon for network transactions. Other direct infrastructure dependencies include those of the electric power, transportation, and continuity of government services infrastructures. As a corollary, long-term disruptions to the banking and finance infrastructure would also have significant impacts on other infrastructures as payment for goods and services could be impaired, investment opportunities lost, etc.

### 7.1.4 Industry Trends Related to Infrastructure Protection

The interviews included discussions on trends affecting the banking industry. Significant trends include the move to deregulation, which is affecting regulatory changes, industry consolidation through mergers and acquisitions, nonbanking companies (e.g., insurance companies) entering the market, and new payment systems and financial products (e.g., MONDEX cards) being introduced.

Trends in telecommunications also affect the banking and finance infrastructure. As telecommunications systems become more distributed, with intelligence built into the separate

nodes of the system, administration of the separate nodes is required. However, such oversight is hampered by current person power constraints and exacerbated by pressures to improve profitability by downsizing. Advanced software is needed to manage the distributed systems from a central location.

## 7.2 Threats and Vulnerabilities

This section has been divided into topics that are relevant to industry segments that were interviewed.

### 7.2.1 Types of Threats

The threats to the banking and finance infrastructure may be divided into two categories. Cyber threats are generally nonphysically destructive, human-induced threats to the information and communications backbones, support equipment and computers. Physically destructive threats (those that depend on physical phenomena) include fires, natural phenomena such as floods and earthquakes, and noncyber terrorist actions such as bombings. Other related threats include equipment failures such as communication system faults and phone outages. The real consequences of all these threats are generally perceived to be economic rather than related to human health or safety.

### 7.2.2 Vulnerabilities

According to one interviewee, no large disasters are waiting to happen in the banking industry. Increased security increases costs, and these security-related costs need to be compared with the cost of an incident. Dual controls are implemented on all systems for protection. The likelihood of loss is low as compared with high insurance premiums with deductibles for protection.

Physical vulnerabilities discussed include impacts to common telephone lines and the computer infrastructure. It was noted that the banking industry is currently perceived to have a low vulnerability to financial threat, as indicated by the high deductibles on insurance policies. It can be said quite simply that vulnerability reduction decisions are based on cost/benefit analyses. In other words, the question being asked is, Will I save more than I invest by taking action? In fact, a cost/benefit culture is strongly in place regarding safeguards and mitigation (i.e., insure up to the point where it pays off, and do not overprotect or overinsure).

The banking industry is becoming more and more dependent on various electronic devices (e.g., ATMs). The industry needs to "trust" these devices, but there are inherent vulnerabilities. There is high motivation to "crack" these boxes, since there is a potential to obtain a significant amount of money through these means. The threat of tampering is significant.

Typical computer systems are password protected, and access logs are maintained. Off-site storage of data is provided. Computer redundancy is in place, as are links to other banks and computer service organizations. There is an overall awareness of the need for redundant controls for system entry and for the physical separation of computers and their support systems. The current systems appear workable and well run. One identified banking industry vulnerability is the carriers and switching nodes for networks.

Perceptions of relative risk varied among the interviewees. It was noted that there is a tremendous financial incentive for organized crime to carry out cyber fraud. The criminal enterprise system probably wants to keep the finance system vulnerable but healthy, so it can use it to launder money. Forms of electronic money can be tapped from a distance and tapped discretely. Small amounts of funds tapped slowly over a long period of time are difficult to trace. This issue was of more concern than intrusion by hackers to one organization. Another thought that the biggest threat is insider malfeasance, but that such misconduct is very well controlled.

The interviewees did not appear to be overly concerned about terrorist forces, because other acts of destruction would bring more desired publicity to the perpetrators. In short, it is unlikely that someone would want to bring the banking system down; there is more incentive to "tap" it.

### 7.2.3 Externalities Affecting Threats and Vulnerabilities

The industry is subject to two main types of checks: (1) safety and soundness exams that are supervisory in nature, and (2) compliance exams that check regulatory compliance.

The effect of market and technology changes on vulnerability was discussed. The deregulation-driven changes in current regulations or new regulations were not perceived to be affecting infrastructure assurance, but the market response could. For example, consolidation-driven economies of scale have competing effects: catastrophic threats affect larger populations, thereby implying greater consequences; however, larger-scale operations should have higher reliability, implying less frequent failures. The industry trend toward consolidation in banking also implies fewer targets for attack. Consolidations are reducing redundancy in operations (such as back room processing of financial information, which depends on skilled, knowledgeable employees). Vulnerabilities may increase as various banking services in smaller organizations lose redundancy. Competition is driving costs down, which will likely degrade service and security. End users will not notice the problem until the services are decreased.

It was noted that new entries in the banking market from the insurance and other industry segments may add to risk, because of their unfamiliarity with assurance vulnerabilities and threats; moreover, the emphasis on reacting swiftly to financial market forces may divert attention from surety. Certainly, the new instruments open new opportunities for fraud, from both insider and outsider attack.

Another concern stems from the relative inexperience of banking personnel with regard to computer technology and computer protection issues. Frequent technology changes may cause an over reliance on black box technology. New products open new opportunities for both mischievous hackers and organized crime to penetrate the system.

There is major concern over whether banks will continue to control payment systems or whether unregulated third parties will have the lead, because the merger of commercial and investment banking requires a thorough understanding of the reliability implications of electronic commerce. The convergence of the TV and PC is creating, in effect, an ATM machine in every home and hotel room. Bankers want to control all this via bankcards, so nonbankers will not be able to create demands on funds outside a controlled environment. The industry has technology for providing access on-line banking services at home or in the hotel room under contract.

The smart card technology emerging now may compete with credit cards. The issue of the control of payments occurs with regard to this technology, as well. One interviewee advocates that the banks should be controlling this payment system.

Security is a major concern that is largely addressed by protection from outside the industry. Companies are working on improved encryption techniques that are needed by the industry. Several banks prefer to develop their own in-house security technologies, but others feel that the commercial products are adequate.

One organization argued that there is a major change in systemic risk because of the deregulation and disaggregation of both banking and financial services and telecommunications at a time when they are becoming more intertwined. A related area of potential risk that is emerging is that of electronic commerce. Entities engaged in unregulated electronic commerce are able, in some circumstances, to shift risk to the banking system. Bankers have long been very aware of

systematic risk and competent in analyzing it. The industry regularly decides which risks it will routinely self-insure against, and which ones require specific actions to avoid. The quick rate at which new technologies in telecommunications are introduced, and the quick rate of change in the competition between banking and financial services, are making the job of risk management more difficult.

One representative believes that the insurance paradigm of catastrophe leading to new ways of doing business will prevail in the formulation of public and industry policy. It is concerned that telecommunications companies are taking little responsibility for the protection of telecommunications-related information.

### 7.3 Requirements and Standards

Standards within the banking industry usually evolve and become de facto standards. This evolution is critical to the industry for maintaining open-system architectures. Problems with standards tend to be self-solving within the industry. The government may be able to assist the banking industry with the evolution of standards.

There must be an international solution to the issue of standardization. The U.S. is now ahead in use of the Internet, but the European Community may catch up and move faster. The Banking Information Technology Secretariat (BITS) is one approach to an industry coalition to address the problem. The industry prefers self-regulation through an industry organization (similar to the Network Reliability and Interoperability Council (NRIC) in telecommunications) and could use help in structuring and initiating such an organization. The involvement of the G8 group is important to establishing international standards.

One organization stated that the environment is now characterized by standards from the periphery. In other words, changes are coming so fast that the adaptation of practices depends mostly on the states, which are in front when it comes to requiring standards for service quality, reliability, availability, etc. Very few standards are being passed down by the FCC. State authority will continue to dominate.

### 7.4 Emergency and Disaster Recovery Plans

The industry has built its disaster recovery preparation around the concepts of data backup and inter-industry substitution. The industry wide status seems to be adequate for disaster recovery, when one bases this conclusion on mostly anecdotal information. Backup systems are the main focus. Federal regulations drive corporate plans, which are implemented across a company and its various branches. One organization's plan included physical recovery and use of shared systems with other banks and computer service companies. Off-site storage of data is also considered. Mutual agreements are in place with other institutions for recovery assistance.

### 7.5 Research and Technology Needs

The interviewees suggested several areas where research and development could help to solve their technology-driven needs. One comment was that he design of security products typically lags behind the technological capability of the hackers to penetrate systems. There is a lack of forward-looking R&D to rectify this problem. Security mechanisms need to be designed as part of the product itself, not developed afterward. Software developers need to anticipate hackers.
Other specific areas for R&D include:

- Stronger, yet cheaper, smart cards. Technical solutions can be found to make them more secure, but these usually raise the cost of the card..

- Fraud with regard to electronic money and value tokens, along with the risks involved in shifting from banks to nonbanks as issuers of credit and electronic representations of value. New payment systems and instruments are coming into play.

- Year 2000 Problem. This should be a priority for the Commission. An enormous number of systems may inadvertently shut down or function improperly because of this problem.

- Encryption devices and techniques.

- Public/private key management, identification and validation of identities, and verification of electronic documents.

- Physical and cyber protection for the new instruments of money and to protect the various devices in the banking and finance community (e.g., ATMs).

- High-availability systems and systems that emphasize indicators and warnings.

- Advanced software to manage distributed systems from a central location.

- Intrusion detection techniques and tools to address the increasing level of attacker sophistication.

- Non-intrusive security systems.

- Tools and methodologies to analyze vulnerabilities and perform cost/benefit analyses.

- Threat awareness capabilities.

### 7.6 Government Role

The consensus of the companies interviewed was clearly that the government should not develop more mandates or requirements. Government involvement in setting cryptographic standards or regulations is dangerous. The industry could use help in requirements definition and functional characterization for security systems. The industry could use help in forming partnerships.

The interviewees felt that there is a need for grater consistency in government policies.

The industry needs help from the federal government in sharing information about threat detection and threat management, specifically with regard to emerging high-technology devices and techniques, and technology transfer of intrusion defense products.

The government and industry should improve the security quality of products. The government should help with research on security technologies and devices. Government-sponsored research and development in cryptography should continue and should be made openly available to the industry.

The government's role in organizing and managing on-line electronic commerce should be to define and prosecute fraud and to facilitate transactions by standardizing legal definitions of electronic documentation and identification methods and standards. The several state legislative initiatives directed at facilitating electronic commerce should be monitored and evaluated by a federal agency to promulgate the successful efforts.

The government needs to make certain that basic issues, such as standards, protocols, and security are addressed. The government could foster the formation of interindustry groups, such as a link between the banking and the telecommunications industries, since banking depends on networks for transactions.

Governments should increase the punishments for hackers. This laxness is complicated by the presence of both domestic and international threats. The U.S. needs to stiffen punishments, get laws in place, and educate the public on what the laws are. The U.S. also needs to work with foreign countries to implement similar measures abroad.

Finally, it was suggested that clarification of anti-trust laws be provided so that coordination of efforts of telecommunications companies working in the banking and finance area could be accomplished without being in violation of the law.

# 8 TRANSPORTATION

## 8.1 General Information

### 8.1.1 Background

The transportation infrastructure in the United States encompasses the aviation, rail, highway, and aquatic vehicles, conduits, and support systems by which people and goods are moved from point to point in order to support and complete matters of commerce, government operations, and personal affairs. Interviews were conducted with a variety of organizations within the transportation infrastructure to obtain a spectrum of ideas, views, and concerns relating to the protection of this major infrastructure. Organizations included the Department of Transportation for a major U.S. city, mass transit organizations for three major metropolitan areas, a private sector company involved with methods for improving surface transportation, a Port Authority, and an organization concerned with research in the transportation area.

### 8.1.2 Organizations

One of the interviews was with a private-sector organization which promotes the use of intelligent transportation systems (ITS) to improve surface transportation. ITS include computerized and centralized traffic control systems, mapping systems for vehicular navigation, and automated vehicle systems. Automated vehicle systems are long-term, but in the next 10-15 years there will be more and more computerized traffic control and mapping systems.

Another of the interviews was with the arm of the National Research Council (NRC) charged with the stimulation of research concerned with the nature and performance of transportation systems, the dissemination of information produced by this research, and the encouragement of the application of the appropriate research findings. The program is supported by state transportation and highway departments, the modal administrations of the U.S. Department of Transportation (DOT), and other organizations and individuals.

Mass transit representatives from major metropolitan areas in the United States also provided information on the transportation infrastructure. They provide mass transit service to the citizens of major U.S. cities, and also provides bus and/or rapid rail transit service into suburban communities.

The remaining interviews for the transportation infrastructure covered a variety organizations within a major metropolitan area. The city Department of Transportation (DOT), with about 4,000 employees, maintains approximately 5,700 miles of streets and highways, and more than 800 bridge structures and tunnels. It maintains and coordinates lane closures, traffic signals, and parking infrastructures, and develop transportation-related policies and strategies. The Department also operates alternative modes of transportation, such as ferries, monitors private ferry services, and administers the subsidized private franchise bus program.

A regional metropolitan transportation authority was created by the state to set policies and budgets for transportation agencies in the major city of the region and several suburban counties. Part of this authority operates most of the city's mass transportation including subways and buses.

The Port Authority is a public authority formed to improve terminals in the port and related transportation facilities. It oversees specific bridges and tunnels and a railroad. Part of this railroad is now a rapid transit system that connects outlying stations (including out-of-state locals) to the city and carries about 200,000 passengers per day. The Port Authority also oversees operations at the three regional airports. The Port Authority built a bus terminal which

is the depot for all commuter and interstate bus companies. The Port Authority also built a major container port as well as a world known business center..

### 8.1.3 Infrastructure Involved

The private-sector organization focuses on the surface transportation infrastructure, but is indirectly involved with telecommunications, relying on the latter for equipment and service.

The National Research Council, with the Transportation Research Board (TRB) playing a role, has the responsibility of maintaining an Advisory Committee to U.S. Department of Transportation (DOT) on a research and development (R&D) agenda for infrastructure security. However, the TRB has expressed concern about whether any attention will be paid to a research agenda on this subject.

#### 8.1.3.1 Mass Transit

The infrastructure for those organizations or agencies dealing principally with mass transportation includes railroad lines at grade, in tunnels, and over elevated structures; bridges spanning the rivers and other transportation rights of way; bus terminals and garages; and transit train storage and service facilities. Operation of these facilities requires the use of electrical cabling for carrying current through third rails, as well as both wireless and cable communications land lines that permit the remote control, activation and deactivation of vehicles and various support systems.

The mass transit portion of this infrastructure includes a multi-faceted mass transportation system, including buses, subways, and ferries. Buses typically run 24 hours a day, every day. Subway systems also typically operate 24 hours a day. Above-ground rapid-rail systems are also a part of some of the mass transit systems interviewed in this effort.

Alternating current (AC) is used to operate signals, station and tunnel lighting, ventilation and miscellaneous line equipment. Direct current (DC) is used to operate trains and auxiliary equipment such as water pumps and emergency lighting. Electrical-power substations receive high- and low-voltage electrical current. Substations may receive as much as 27,000 volts and then convert it for use in the subway. A typical voltage requirements for a subway's contact (third) rail is 625 volts. Power is distributed throughout the system via thousands of miles of cable. The power required to operate a subway system during peak hours may reach approximately 500,000 kW.

#### 8.1.3.2 Ports and Harbors

Information was received from representatives of one of the largest ports in the United States. More than 4,000 ship calls with cargo tonnage of approximately 50 million tons and a value in excess of $60 billion are handled annually.

#### 8.1.3.3 Bridges and Tunnels

In addition to bridges and tunnels used by mass transportation systems, there are often hundreds (sometimes thousands) of bridges used by vehicular traffic. Such bridges are often considered as crucial transportation links into a city since much of the commercial traffic (supplies and products) comes into the city in this way. Many freight trucks are too large to fit through the tunnels, and hazardous materials such as propane, fuel and heating oil, chemicals, etc., often cannot be transported through the tunnels.

Principal bridges and tunnels used by cars and trucks are sometimes monitored on closed-circuit television. One interviewee noted that if something unusual happens, the police are usually there within a few (3-5) minutes. Private or agency police forces are also sometimes used to monitor and protect critical bridges and tunnels.

#### 8.1.3.4 Airports

Some of the world's largest airports (in terms of passengers and/or cargo) are the responsibility of some of the organizations interviewed during this effort. Both domestic and international flights use these facilities. Security is typically the responsibility of some combination of local police forces, the federal government, and agency-specific protection units.

## 8.2 Threats and Vulnerabilities

The opinion was expressed that the task of screening U.S. transit systems for terrorist threats to be extraordinarily difficult, yet a first-line vulnerability. Most U.S. transit systems have numerous access points and their competitive status is very poor, leading to both a lack of resources to deal directly with many threats and a reluctance to do so if implementation of such capabilities would further inconvenience their (now-dwindling) user base. He noted that some transit systems, in addition to traffic control systems for some large cities and railroads, have central computer controls that may be vulnerable to sabotage by physical or electronic attack. Moreover, as Intelligent Transportation Systems (ITS) become more widespread, with more centralized computer control, the networks they regulate could be more subject to chaotic breakdown in the event of such an attack.

### 8.2.1 Types of Threat

The main threats to intelligent transportation systems include power outages and interruptions of fiber optic and telecommunication services. The main effect of such threats is severe traffic congestion or gridlock. No mass disasters would result unless another threat existed. For example, if the evacuation of an area because of an oncoming hurricane were severely hindered by a non-functioning computerized traffic control system, the potential for a mass disaster could exist. A more typical concern is that emergency personnel could be hindered in any severe traffic congestion situation.

#### 8.2.1.1 Mass Transit

By definition, all mass transit systems with extensive fixed infrastructure and unrestricted public access to property are soft targets. Specific areas of concern are possible bombs, chemical-biological hazards, track obstructions and other security breaches of their system. Mass transit rail lines may lead to airports, and these lines may pass directly underneath one or more government buildings. Mass transit systems may have a score or more stations, some of which are open 24 hours a day. Security personnel cannot staff all of these stations every hour that they are open. Local police departments (possibly including K-9 units) and agency-specific protective forces may share the responsibility for providing security for transit operations.

There have been a number of frightening incidents in subway systems, including Molotov cocktail-type bombs and gun violence. Of great concern is the possibility of a chemical-agent incident such as the one in the Tokyo subway system. As with closed-circuit television, the cost of installation and maintenance of chemical sensors throughout the subway system may be prohibitive because there is so much steel dust created as the wheels run down the tracks that the sensors would need to be cleaned and maintained on a daily basis and, even so, would probably emit false alarms frequently. Currently the ability of the first responders and subway personnel to respond effectively to a nuclear, biological, or chemical incident is severely limited.

Cutting the electricity to the subway could also cause a serious problem, although not necessarily a very dangerous one. During previous blackouts, people have walked out of subway tunnels to safety without incident. However, cutting the electricity, in combination with other malicious activity, could be very effective in creating a dangerous, terrifying situation.

Subways are vulnerable to flooding from water-main breaks and from severe storms. A sudden rush of water into the subway can cause serious problems (trapping people and even drowning

them); a situation that would be exacerbated because of the high voltage that it takes to run the subway.

#### 8.2.1.2 Ports and Harbors

The large amount of foreign and domestic cargo coming into and through the ports and harbors is of concern to authorities. Explosives detection equipment and trained personnel are needed.

#### 8.2.1.3 Bridges and Tunnels

Although main bridges and tunnels used by cars and trucks are often monitored by closed-circuit television, it is possible that a tunnel or a bridge could be severely damaged by using explosives. In a tunnel, use of chemical agent would also be catastrophic. Great loss of life could be the result, particularly if it were done during a peak rush hour. It would be difficult for police and other emergency personnel to respond quickly.

#### 8.2.1.4 Airports

There is a continued absence of modern bomb-detection equipment in America's major airports.[2] Machines designed to detect plastic explosives (such as Semtex) in checked or carry-on luggage are already in use at many airports in Europe and Asia but are still awaiting approval by the Federal Aviation Authority (FAA) for use in then united States.

Local agencies having security responsibilities at U.S. airports cannot force the airlines to do something about security. This is a different situation from that what exists in Continental Europe, England, and Israel, for example. Also of concern is the fact that airline employees are not necessarily thoroughly checked out before being hired; nor are precautions (such as fingerprinting) taken when they are hired. There should be training to specific standards for airport personnel, and better pay as a result. In many rural airports in this country, airport security personnel don't get paid more than minimum wage. And in most places, security at the airport is an entirely civilian endeavor; the police are not involved.

### 8.2.2 Vulnerability Assessments

A variety of vulnerability assessments have been conducted by or for several of the organizations interviewed. For example, a recent study on counter-terrorism strategies and methods was funded by transit agencies themselves as part of a pooled research program managed by the Transportation Research Board.

One of the agencies interviewed noted that in the wake of the World Trade Center bombing, it has conducted several vulnerability assessments of its various systems, and has implemented procedures to combat these vulnerabilities to the extent that it is within its power to do so. It has no standing committee focusing on the vulnerability of the systems to physical, cyber or other threats, but its Security Services Department is a full-time operation. Their security personnel have participated in counter-terrorist and other relevant training and security workshops offered by the FBI (Quantico), the Federal Transit Administration, and various other law enforcement agencies. Other interviewees noted that their personnel have conducted similar assessments and have also participated in training and security workshops.

#### 8.2.2.1 Assessment Methods

Little information was obtained on the assessment methodologies for the transportation infrastructure. Some interviewees noted that they used surveys and interviews while others indicated that lessons learned from exercises and drills as well as from actual incidents are important factors in their vulnerability assessments

---

[2] Stoller, Gary, *Why the Bomb in This Suitcase Won't Be Detected; U.S. Airports Lack the Latest Equipment*, Condé Nast Traveler, June 1996, pp.37-42.

#### 8.2.2.2 Areas of Vulnerability

Several interviewees expressed the opinion that their areas of vulnerability have previously been identified under the designation of Types of Threat and Vulnerability Assessments (Sections 8.2.1 and 8.2.2, respectively). Specific areas of greatest vulnerability for subway systems include transfer stations (where two lines meet), service and repair yards, the underground tunnels in downtown areas and vent shafts throughout the system.

#### 8.2.2.3 Levels of Risk

The levels of risk associated with the transportation system (particularly mass transit systems) are high. The potential for the public to be harmed while in transit is great, and has happened in the past (such as when Molotov cocktails were thrown in a subway station injuring a number of passengers, as noted above).

If the threats became fact, property damage, loss of services, personal injuries and death and financial loss could all occur. Financial loss could occur because of a) the need to repair damaged property, b) the need to decontaminate portions of the metro system, c) civil litigation resulting from personal injury and death, and d) loss of ridership due to a change in the current public perception that mass transit systems are safe.

#### 8.2.2.4 Impact on Other Infrastructures

If something catastrophic happens to or in the transportation infrastructure, the most significant impact on other infrastructures would be in the emergency services area as police and other emergency teams respond to the incident and medical personnel attend to the sick or injured.

Some mass transit systems share or have adjoining facilities to other parts of the transportation infrastructure. Furthermore, mass transit systems often serve many government facilities. Thus where mass transit is vulnerable, so too are these facilities. Also, some interviewees suggested that there is a potential for copy cats to adversely affect the public transportation infrastructures in other regions if damage is done to one mass transit system.

### 8.2.3 Vulnerability Reduction Actions

Vulnerability reduction actions discussed during these interviews can be divided into two categories: Operational Practices and Technologies. The following paragraphs summarize the findings in these areas.

#### 8.2.3.1 Operational Practices

In addition to increased support from local police departments, at least one mass transit system has hired off-duty police officers to ride buses in order to provide on-board security capability. In addition, a private security firm has been contracted to provide trained staff and dogs to ride their trains. A private security company has a contract to provide nighttime security staffing at bus terminals (garages) and railway storage yards. Beginning in late-June, 1997, the mass transit system inaugurated a program that will eventually place a security guard in every transit station that remains open for at least a portion of the late-night hours.

The Department of Transportation for one large U.S. city plans to add surveillance equipment (CCTV) at additional street intersections. In this same city, a safety feature refereed to as the Halon System has recently been installed at each token booth in the subway. If a match is lighted near the booth, the system will immediately activate and extinguish the flame. This system was instituted to protect attendants from a rash of attacks that involved throwing lighted explosives into the booths, thus injuring and even killing a number of these workers. This does not protect these workers from the other hazards of the job however. Token booth attendants have been

preyed upon with some regularity, and this continues despite progress on reducing crime in the subways.[3]

Some sectors in the transportation infrastructure have developed operational plans and formed alliances to reduce their vulnerabilities. See Section 8.4.1, Response Plans, for additional information on some of these plans.

One of the organizations interviewed in this effort has its own police department and that department is knowledgeable about terrorist tactics, bomb threats, and chemical-biological hazards. Department staff have taught courses to others on terrorist tactics. They drill and train continuously. They coordinate with the police and fire departments of the local government jurisdictions in which mass transit system operates and with medical personnel to prepare for and deal with emergencies. They are also attempting to increase public awareness of potential threats so that the public can help identify potential threats.

#### 8.2.3.2 Technologies

The number one need for emergency preparedness and response in mass transit systems was identified by one group of interviewees to be better communications systems. The radios used in their subways (and radio is the primary method of communication in the subway) have dead spots and the systems used by other organizations, including the local police and fire departments, do not work below ground. Therefore, runners are used at the site of a subway emergency. That is, people run up and down the subway stairs relaying information from below ground to emergency responders at street level. The limitations of this system are obvious; information is not transmitted rapidly enough, there is the potential for information to become garbled or misconstrued (as in the child's game of Telephone ), and the runners may be exposed to hazardous conditions as well as adding to the general confusion themselves.

Other technology needs include better bomb-detecting equipment (that can detect plastic explosives) for the airports and for major ports.

Another mass transit organization is sponsoring a study with the U.S. Department of Energy on chemical-biological releases and how to identify them. They are in the process of buying a portable X-ray machine to be used to determine if a package is a bomb. They are also purchasing disposable Quick Masks to be used by police in the event of a potential chemical-biological hazard; the police using them will be directing the public out of stations. A canine team is currently being trained in identifying explosives. They are seeking a federal grant to enhance the security of its train yards through infrared technology/night imagery photo-recording.

#### 8.2.3.3 Investment Considerations

The mass transit organizations interviewed in this effort have taken their security concerns seriously enough to invest in the higher level of station staffing, bus and train riding by security personnel, etc. However, their resources are constrained, and investments in infrastructure protection are generally always made at the expense of staffing and service in other operations areas.

Purchasing up-to-date equipment (such as better communications equipment and improved bomb-detecting equipment) is expensive, but will be done when it becomes available. Additional federal funding for such purchases would be helpful.

---

[3] Onishi, Norimitsu, *In His Safe Station, Subway Clerk, 60, Is Killed*, New York Times, March 25, 1997, p.A1.

One mass transit organization would like to see investments made to the level needed to achieve zero tolerance of potential incidents. However, they also suggested that a cost analysis needs to be conducted to determine what an acceptable level of risk is. They are interested in securing grant money to improve the protection of their infrastructure. They are also considering joint ventures with businesses that are adjacent to metro stops (i.e., to set up security cameras, etc).

## 8.3 Requirements and Standards

### 8.3.1 Existing or Planned

There are many existing regulations, standards and company practices which must be met. American Public Transit Association, the Federal Transit Administration, the Department of Justice, the International Association of Chiefs of Police, and state training commissions all have requirements which must be met. Building codes (for subway construction which is still ongoing) may also affect how threats and vulnerabilities are addressed. Every transit agency must meet similar requirements, but all are ultimately different because of the varying requirements of different local governments. Each agency also develops its own standard operating procedures.

The Federal Transit Administration of the U.S. Department of Transportation is conducting a one-year study to evaluate procedures now in place, then to define the minimum standards necessary for good security practices on mass transit systems.

The U.S. Department of Transportation has defined and is in the process of refining a system architecture for all installations using intelligent transportation systems; however, this architecture will be predominantly a shell framework into which various protocols (such as frequencies for transmission and reception of communications from various media, including roadside toll tag readers and transponders in vehicles; a uniform geo-location referencing system; specifications for weigh-in-motion devices; etc.) will be inserted. None of these protocols have yet been finalized by the organizations or committees charged with setting them.

### 8.3.2 Suggested Change

A specific example of a shortcoming in current procedures is the need to update venting and exhaust standards for clearing smoke and gases from subway tunnels. Most current regulations assume that about the most noxious substance to be vented is smoke from electrical fires, and thus permit some degree of venting to surface streets, but in the wake of the Tokyo Sarin incident, this procedure may have to be reexamined.

## 8.4 Emergency Plans

Emergency plans for the transportation sector must be designed to deal with relatively common emergencies such as snow storms or accidents, as well as natural or man-made disasters that immobilize or destroy portions of transportation systems.

### 8.4.1 Response Plans

The mass transit organizations interviewed appear to have standard operating procedures and response plans to address the routine emergencies. These response plans are believed to effectively integrate the responsibilities of the affected agencies, e.g., police and fire departments, medical personnel, electrical service personnel, operations and maintenance personnel. In at least one major U.S. city, there does not appear to be an actual unified response plan per se that covers all potential agencies. However, there has been at least one drill conducted in which there was participation from multiple municipal agencies. This drill involved a terrorist attack scenario. At least one organization has an evacuation plan as part of their overall emergency response plan.

One mass transit organization noted that it is preparing (in response to a requirement of the Federal Transit Association requirement) a System Security Program Plan which is to be completed in January, 1998.

#### 8.4.1.1 Exercises/Drills

Transit organizations routinely conduct exercises covering the various aspects of system security. One such drill in a major U.S. city posed a scenario of a sarin gas release in the subway. The lessons learned included the realization that the system is so open, that it would be relatively easy to stage such an attack. This drill prompted a directive that spells out actions to be taken if two or more people become disabled with specified symptoms having no obvious cause, such as smoke. There is some doubt regarding the effectiveness of the actions called for in this directive in the event of a serious attack with a chemical agent.

In addition to drills, at least one major city provides additional classroom training on emergency plans and procedures; frequent refresher training is required. Training videotapes of the special challenges of responding to an incident in the subway have been made for use in their own classrooms, and for use by other responding agencies, such as the fire department. There is cross-training of dispatchers for the various responding agencies as well as training in a common language to be used during emergency situations, instead of the jargon that different services use amongst themselves.

#### 8.4.1.2 Communications/Command

In one city, incidents that transcend the capabilities or jurisdiction of any one agency or department are managed from the city's 911 Command Center (effectively, the city's Emergency Operations Center, a recently-opened, high-tech state-of-the-art facility). In this center, the designated responsible representatives of all affected organizations interact face to face and disseminate timely, coordinated instructions to the field.

In at least one city, a mass transit control center functions as an emergency operations center during an emergency. The center is equipped with a variety of communication equipment and is linked to other command centers during emergencies. Emergency equipment is stored in self-contained cases at strategically located areas throughout the system. The cases contain communications equipment (cellular telephones and mobile radio), a lantern for power off and night operations, special safety vests, appropriate emergency signs, a log book to retain pertinent information, etc. The chain of command for emergencies on property owned by this agency is defined in procedures; if the incident is a fire/smoke incident, then the fire department is in charge. For an evacuation of the subway trains, the mass transit agency is in the lead. For bomb threats, the police department is the lead organization. There is still confusion over who has the authority in a chemical/hazmat incident.

## 8.5 Information Exchange

### 8.5.1 Current Methods

Mass transit organizations are typically provided with extensive information on terrorist activities, potential threats to the infrastructure and technologies which might be used to protect the infrastructure. This information is provided by the FBI, the Department of Defense, local police departments, the Federal Transit Association, and the American Public Transit Association, and other organizations

There is information exchange in the area of emerging technologies. For example, private and public sector interests are currently working together in jointly-operated projects as part of U.S. Department of Transportation's intelligent transportation systems Field Test and Model Deployment Programs.

### 8.5.2 Areas of Deficiency

While a great deal of information sharing arises naturally from private and public sector interchanges, the corporate participants have proprietary interests to protect and thus often do not make public the essential content of hardware and software products they contribute to the deployments.

Concern was expressed that even the task of *coordinating* emergency responses to disasters across multiple agencies and jurisdictions is extremely difficult. Rampant problems in response to hazardous materials emergencies (e.g., incompatibility of communications channels, failure to use "Incident Commander" hierarchical command-and-control systems) were cited as a vivid example of this shortcoming.

Radio frequencies are not always shared among agencies having to respond to a transportation emergency. Moreover, separate frequencies must be used for subway and surface operations (and subterranean radio communications are always a problem).

### 8.5.3 Suggested Improvements

Interagency incompatibility in radio frequencies can be significantly mitigated by the function of a 911 Center, in which all agencies' command staffs are in direct contact with one another and can communicate frequent and accurate updates and instructions to their personnel in the field using their own communication systems.

One organization indicated that it would be desirable to have more information on what's coming next. In other words, if some new terrorist technique is being developed and if government intelligence learns about it, it is desirable for the potentially impacted agencies to be forewarned.

## 8.6 Research Needs

### 8.6.1 Unmet/Inefficiently-met Needs

There is a need to more fully understand the vulnerability of transportation systems to a hacker. This need will become greater with the implementation of intelligent transportation systems and as these systems are integrated into emergency response plans. The level and type of protection built into these systems must be investigated.

The vulnerability of new technologies, including training on how to avoid and respond to threats, was noted as a potential area of increased research.

The role of government in helping the private sector respond to emergencies was cited as an area in which greater understanding is needed.

As noted above, more effective bomb detection devices and communications systems that work in subway systems are needs that have been identified by the transportation infrastructure.

More research is needed on chemical and biological hazards and the equipment that should be used when operating in a hazardous environment (e.g., the protective suits and breathing apparel that should be worn). Ideally, something like a personal pager which detects poison gas and other gas detection devices is needed. Techniques for dealing with suspicious packages need to be better developed.

### 8.6.2 Government Role

One interviewee suggest that the federal government provide training grants to transit agencies and their associated security services and that a centralized security practices training center, possibly along the lines of the Emergency Management Institute in Emmetsburg, MD (or,

alternatively, a mobile training facility) be established to assist transit agencies in dealing with security and protection issues.

Another interviewee offered the opinion that it is the government's responsibility to support or encourage research into improved bomb-detecting equipment and then to approve security equipment to be used in airports (or other ports of entry).

Defense contractors who develop technologies for dealing with hazardous situations for the military could be funded to consider the requirements of transportation infrastructures such as those of typical mass transit systems. It was also suggested that the military could provide training to mass transit agencies in dealing with various emergencies.

# 9 WATER SUPPLY SYSTEMS

## 9.1 General Information

### 9.1.1 Background

The water supply system includes those sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration and cleaning systems, the pipelines, the cooling systems and other delivery mechanisms that provide water for domestic and industrial applications. These include systems for dealing with waste water and fire fighting.

### 9.1.2 Organizations

Three main organizations were initially contacted to identify industry needs in this area. These are the American Water Works Association (AWWA), the American Public Water Works (APWA), and the Army Corps of Engineers. All three organizations were contacted between May 23, 1997 and June 11, 1997

The Army Corps of Engineers subsequently advised Argonne to contact the APWA to obtain information on water supply vulnerabilities. The APWA and the AWWA each, in turn, advised us to contact cognizant members of their organizations.

Six organizations were subsequently interviewed to provide information to their individual systems. These organizations were selected because they represent a broad spectrum of water purveyors that ranged from small to large, are located on each coast and in the Midwest, and include systems that are predominately supplied by surfacewater and others that rely predominately on groundwater.

## 9.2 Threats and Vulnerabilities

### 9.2.1 Threats

Each stakeholder was asked to provide information on physical, chemical, biological, and radiological vulnerabilities to their system. In all cases, physical threats were not considered to be viable because of security measures already in place (e.g., fences, locked gates, internal and external security patrols, surveillance cameras, etc.), system redundancies (e.g., multiple treatment facilities, multiple post-treatment reservoirs, etc.), and load-switching capabilities. Recently, security at many of these facilities was heightened in response to the Gulf War, political conventions, and conditions of unrest. Even if a physical threat was successful, the primary concern expressed by the water purveyors was loss of supply to the distribution consumers. System recovery under such conditions is detailed in existing contingency plans, albeit, for natural disasters, such as earthquakes or dam failures. Similarly, cyber threats to the water supply systems were deemed possible, but the only impacts would be to the availability or pressure of the water.

### 9.2.2 Vulnerabilities

Each stakeholder expressed confidence that their system is not vulnerable to a nuclear, biological, or chemical (NBC) terrorist attack on the raw water supply of the facility because of the combined effects of large volumetric dilution and subsequent treatment. In cases where groundwater is the primary source, the supply is veiwed to be even less vulnerable because terrorist contamination of groundwater supplies is highly unlikely. On the post-treatment side, the stakeholders were not as sanguine, although the use of underground, concrete post-treatment holding tanks offer a very good defense against terrorist activities.

In every case, the stakeholder admitted a vulnerability to NBC attack within the distribution network, e.g., injecting an agent into the distribution network through a residential tap, fire hydrant, etc. However, they also indicated that they were unaware of what specific agents would most likely be used. A number of the respondents indicated that they are trying to reduce potential contamination in the distribution network by using back-pressure protection devices. For example, in one system, more than twenty-five percent of their connects are protected with dual-valve back-pressure devices. In another system, back-flow protection is required on all residencies that are duplex or larger. For the other stakeholders contacted, back-flow protection was generally used on commercial buildings, irrigation connections, and industrial complexes.

In addition to using back-flow protection devices, all of these stakeholders use a residual disinfectant in the distribution network, as required by the Environmental Protection Agency. The levels of residual disinfectant maintained would be adequate to mitigate the effects of many chemical and biological agents. Even if the system did not completely destroy the agent, the decrease in residual disinfectant would be noticed in routine monitoring and would be brought to the attention of senior personnel (because sampling is not done continuously in the distribution network, significant time could elapse between agent introduction and detection). If detected, one or more pressure zones could be isolated, load shifting could be implemented, and other contingency plans enacted. It should be noted that in some cases (e.g., the chemical agents VX, BZ, and sodium fluoroacetate; the toxins trichothecene mycotoxin T-2 and botulinum toxin; and the biological agent *Bacillus anthracis),* residual disinfection would have little effect on the agents. If one of these agents was introduced into the distribution network, large numbers of fatalities could be produced before any contingency plans could be initiated.

### 9.2.3 Vulnerability Reduction Actions

Although none of the stakeholders is specifically doing any activities specifically directed toward mitigating NBC attacks, a number of them are using policies and methods that would mitigate a terrorist's actions. These activities include the following: limiting access to detailed plans of the distribution network, thereby increasing the uncertainty of a successful terrorist attack; maintaining high levels of pH in the network, thereby promoting agent degradation; using multiple pressure zones that can be isolated if an attack is detected; adopting system redundancy and load-shifting policies; and in some cases, installing particle counters to detect the protozoa *Cryptosporidium parvum* and *Giardia* at the treatment plant**.**

## 9.3 Requirements and Standards

Other than the Environmental Protection Agency requirement for residual disinfectant in the water distribution network, none of the interviewees noted any specific regulatory requirements.

## 9.4 Emergency and Disaster Recovery Plans

Contingency plans are in place, extensive operator training takes place, some amount of public education occurs, and some recovery plans have been promulgated. However, few, if any, of these activities relate directly to terrorist activities. At the present time, natural disasters, such as earthquakes, hurricanes, etc., and system failures are given the highest priority. Although some of the contingency plans would be effective in the event of a terrorist attack, their utility would be fortuitous.

## 9.5 Information Exchange

This topic was not explicitly discussed during the interviews. However, the fact that the American Water Works Association and the American Public Water Works Association were both instrumental in assisting Argonne in arranging interviews with their members suggests that there is at least a working method of information exchange within this infrastructure.

## 9.6 Research and Development

### 9.6.1 Infrastructure Needs

As discussed in Sections 9.3 and 9.4, the stakeholders indicated that their systems are vulnerable to terrorist attack through their distribution networks, and that little has been done in the way of contingency planning, operator training, public awareness, or recovery planning. Most of them stated that a real-time monitoring device capable of detecting high-risk NBC agents would be valuable, particularly if the device was easy to use, inexpensive, and reliable (had a low false-positive rate). The following suggestions were made concerning areas of meaningful research to address needs of this infrastructure:

- Particle counters that could detect and discriminate biological agents by size and provide this information to a central point in real time;
- Detection of chemical agents through the use of conductivity probes;
- Real-time detectors for both chemical and biological agents;
- Integration of hydrological system models with real time water quality through GIS applications; and
- Satellite imagery for physical protection and identification of potential problems (e.g., algae blooms).

To further reduce the impacts of a terrorist attack, the stakeholders suggested that a good-engineering manual should be written for water supply systems. This manual would include such topics as:

- Potential terrorist threats and likely NBC agents;
- NBC agent physical and chemical characteristics;
- Anticipated water-quality changes for terrorist activities;
- Proper design of a distribution network to minimize the impacts of a terrorist attack;
- Recommendations on the type, number, locations, and sampling frequencies for monitoring devices;
- Typical contingency plans that should be in place to promote rapid and effective response to an attack;
- Recovery plans that could minimize system down time ; and
- Typical public awareness programs.

In addition to improved instrumentation for early detection and an anti-terrorist manual, the stakeholders strongly indicated that more communication on the subject of terrorism and technologies would be welcome, particularly in small forums of adjacent water purveyors.

### 9.6.2 Funded Research

The AWWA and the federal government both have funded research that may be applied to terrorist activities. Within the AWWA, the American Water Works Association Research Foundation (AWWARF) sponsors practical, applied, and future-need based research for drinking

water. The federal government also contributes money to this activity. For 1997, AWWARF supports 215 projects with a budget of $12.1 million. The number of research contractors is 158. From 1986 - 1997, 34% of the research funding went to treatment, 15% went to monitoring and analysis, 17% went to distribution, 14% went to management, 13% went to resources, and 7% went to health effects.

The 1997 research program is heavily weighted toward disinfection and microbial issues, including seven projects on *Giardia* and *Cryptosporidium*, three projects are on emerging pathogens, and four projects on disinfection by-products (e.g., trihalomethanes - THM). Eight studies focus on distribution issues, and other studies to cover such diverse subjects as particle counting, taste-and-odor analysis, and effluent trading. Although none of this research was apparently dedicated to mitigating the consequences of terrorist activities, there are some research projects that may be relevant to terrorism threats as perceived by the interviewees.

### 9.6.3 Role of Government

Although the research areas and manuals discussed above would be very useful to mitigate potential terrorist activities, each of the stakeholders indicated that it would be unlikely that they would sponsor such research from their own funds. Existing problems with their infrastructures (such as maintaining a delivery capability and meeting EPA drinking water quality guidelines) had a much higher precedence than potential threats. If funding were available from an outside sponsoring agency (such as the federal government), they all expressed a willingness to attempt to reduce potential consequences.

## 9.7 Other Considerations

In all cases, the stakeholders indicated a need for additional communication between the government and water purveyors, particularly in the area of terrorist activities and mitigation strategies. It was felt that the best procedure for accomplishing this goal would be small forums of government officials and small groups of water suppliers. Further, many of the participants indicated that the type of information discussed in such forums should be kept out of the hands of the public to avoid widespread paranoia.

As a general rule, the stakeholders stated that while terrorist activities could have a severe impact on their systems, current funding was being directed to immediate and pressing issues, in particular, meeting EPA water quality standards, maintaining their physical systems, and meeting consumption demands. If Congress could be convinced of the criticality of water supply systems, and government funding were made available to perform the required research, the water purveyors would cooperate fully to reduce the threats of terrorist activities.

# 10 EMERGENCY SERVICES

## 10.1 General Information

### 10.1.1 Background

The emergency services infrastructure includes medical, police, fire, and rescue personnel who are called on to prepare for and respond to an emergency. A number of city-level agencies are typically involved in various aspects of emergency planning, preparedness and response, including the Mayor's Office of Emergency Management (or equivalent), the police and fire departments, and an emergency medical team. From a state and regional perspective, the a state Emergency Management Office, and the Federal Emergency Management Agency (FEMA), may be involved. For certain emergencies, response by the National Guard may also be appropriate. Many private-sector organizations also have personnel who are trained and equipped to respond to emergencies specific to their individual industries. Each of these agencies was visited or interviewed by telephone for this Commission effort.

### 10.1.2 Organizations

Each city represented in these interviews has established a control center that is responsible for coordinating the responses to emergencies. These control centers will typically operate the 911 Center" within the city. As a rule, these centers are modern facilities with up-to-date communications equipment and telephone, radio, and, in some cases, sonet networks linking them with the actual response agencies. Individual response agencies, e.g., fire departments, are part of this infrastructure and participated in several of the interviews conducted for the Commission.

State-level Emergency Management Office (or the equivalent) is the agency that is responsible for emergency response planning for the state and for responding to emergencies that involve more than one county or other government entity, or that occur on or involving state property. In some cases, the National Guard has this responsibility.

The Federal Emergency Management Agency is the federal agency charged with providing both emergency planning guidance and emergency response and assistance after a disaster occurs (either natural or technological).

The private-sector company interviewed for the Commission a major U.S. corporation that is an important component of the energy infrastructure both in the United States and worldwide. Its major products are oil, natural gas, and chemicals. It has site- and hazard-specific emergency response teams and security teams at each of its major locations, including its Research Center. This Center allows a good perspective on the decentralized nature of emergency response capabilities. A followup interview with the Executive Director of Crisis Management at company headquarters provided detailed information on how they place a strong emphasis on preparedness planning and exercises, including real, not token, involvement by top management in decision making during real and simulated major emergencies.

Many of the organizations interviewed have some sort of mutual aid agreement with neighboring communities and other government entities that provide for assistance in emergency response and defines a system for responders that has no jurisdictional boundaries.

### 10.1.3 Infrastructure Involved

Although the primary infrastructure is that of emergency services, virtually all other infrastructures are potentially involved in emergency situations. The interviews were focused on

the threats, vulnerabilities, and needs of emergency service organizations and personnel rather than on the separate infrastructures in which an emergency may exist.

## 10.2 Threats and Vulnerabilities

### 10.2.1 Types of Threats

Threats to the Emergency Services Infrastructure include the natural and man-made threats that can impact all other parts of society. These threats are numerous and include crime, fire, flood, contamination, accidents of all types, etc. Emergency services personnel are very concerned about potential terrorist acts.

A wide spectrum of threats is also dealt with by the private company interviewed for this infrastructure, with the lesser ones (e.g., relatively low impact floods, small fires, spills) addressed in a decentralized manner at local level while keeping their headquarters informed. Major emergencies (e.g., earthquakes, tornadoes, major oil spills, fires, chemical releases, kidnapping, explosions) are handled with considerable Headquarters involvement, direction, and support.

### 10.2.2 Vulnerability Assessments

The capability of the Emergency Services infrastructure to respond to an emergency is often impacted by the emergency itself. This is especially true during and after natural disasters such as floods or earthquakes. Another vulnerability within the emergency services infrastructure is that traffic problems can hinder emergency response. Lack of information about the cargo in an hazardous material (hazmat) accident is also a threat to an adequate emergency response.

Equipment deficiencies were cited as a vulnerability to the emergency services infrastructure. A specific example for one city, is the lack of a speedy boat to evacuate fairly large numbers of persons from a boat, perhaps a sightseeing or casino boat, and to fight fires on that craft. A hovercraft could provide such a capability.

Another area of vulnerability exists in the telecommunication systems used by emergency communications. To reduce the vulnerability of incoming calls, they may be routed to the 911 Center from either of two phone company control centers. Different telecommunications standards in different states can also be a problem. A lack of radio frequencies for public safety organizations was cited twice as a potential vulnerability. Closely related to this issue was inter-operability between Federal disaster responders and local responders. It was suggested that all communication be APCO 25 approved standard.

Most emergency responders (police, fire) do not have training in responding to a radiological, biological or chemical weapons attack. Although hazmat teams do have training in responding to chemical spills and/or fires that might occur during manufacture or transportation of industrial chemicals, they do not have training in responding to Weapons of Mass Destruction (WMD). Recent unannounced exercises of this type of scenario in one major U.S. city have shown just how unprepared they are; it was estimated that the first two waves of firefighters and police on the scene of such an exercise would have become victims themselves.

An aging infrastructure is a vulnerability to emergency services. A specific example is that of old water delivery systems (some were made of wood more than 100 years ago) that may suddenly fail and thus hamper fire fighting efforts.

The private company has assessed its vulnerabilities to worst-case oil and chemical release accidents and prepared and exercised emergency plans accordingly, both locally and corporate-wide. A key difference between this company and the public sector organizations interviewed is

that its preparedness, response and recovery activities have to also accomplish business interruption strategies.

### 10.2.3 Vulnerability Reduction Actions

A number of threats have been considered in designing emergency communications system and 911 centers. They have been designed, in at least some cases, with several features to reduce vulnerabilities to natural disasters such as tornadoes and earthquakes. Electrical power is provided by two substations, and the centers are backed up with uninterruptable power supplies. Two separate transmitters for radio communications may be used. Access to the building is limited and there are security personnel (police) present at all times. There are also internal security perimeters within the building. Internal fire protection is provided. The design may allow the building to be sealed off from outside air, which reduces vulnerability to chemical or biological weapons activated externally

One state has installed a fiber optics network that connects each county with the State Operations Center. This network also links federal agencies (within the state), other state government sites, hospitals, and three universities that can make chemical and biological experts available. This same state has also constructed a highly sophisticated State Emergency Operations Center that is self-contained, yet with extremely well connected communications systems. The new fiber-optic cable system is buried four feet below ground level and is not subject to many of the threats, e.g., floods, that conventional communications face.

#### 10.2.3.1 Operational Practices

Specific vulnerability reduction actions taken by one or more of the organizations interviewed for this Commission effort include changes in operational practices such as:

- Participation in statewide emergency response communication and mutual aid systems;
- Working with private-sector companies in the area to coordinate emergency response and provide use of their equipment as needed. Some organizations have purchased additional, modern equipment and provided more comprehensive training to their personnel;
- Preparing updated, integrated emergency response plans;
- Creating a Geographic Information System (GIS) that will map the city's gas and steam pipes; electric cables; water mains, pipes and valves; the subway system; buildings and their floor plans, etc. The goal is to be able to access this information at the scene of an incident (on laptop computers) making response faster, safer and more effective;
- Participating on the Joint Terrorism Task Force;
- Participating in the Chemical Terrorism Task Force; and
- Creating a Medical Strike Team to respond to, provide support for, and provide assistance to local and regional jurisdictions to effectively address responder safety issues, incident management, and public health consequences of NBC incidents that result from accidental or deliberate acts.

#### 10.2.3.2 Technologies

Vulnerability reduction actions in the technology area include:

- Purchase of new fire department communications equipment with the capability of being interoperable with police, medical, and other local organizations using this equipment;

- Testing of a new 311 emergency communications system designed for minor emergency calls so as to reduce the volume of 911 emergency calls; and

- Seismic improvements that have been made at fire stations.

Vulnerability reduction actions for the private company have included the installation of extensive security systems for admission to sites; fire alarm and suppression systems; regularly practiced emergency and security teams; various and extensive voice (radio, telephone, loudspeaker), tone alert, and siren warning systems; and hazard-specific mitigation response and recovery equipment, plans, and exercises (see Section 10.4). A key component of their vulnerability reduction infrastructure is a 24-hour corporate-wide emergency notification center at corporate Headquarters. The headquarters for this company also reduces vulnerabilities with computer virus warnings and other cyber security practices.

## 10.3 Requirements and Standards

A Federal Emergency Management Agency (FEMA) standard for backup power systems to Emergency Operations Centers requires an 8 hr reserve capability. FEMA also requires a 14-day un-interruptible fuel supply to the generators, which means they must be fueled by propane or diesel. Natural gas fuel, since fed through a pipe line that can be interrupted (e.g., during an earthquake), is not acceptable. Meeting this requirement is a very important element in ensuring continuing emergency and other important government services.

Requirements for hazmat team training, emergency plans and procedures, include those of the federal and state Occupational Safety and Health Administration (OSHA) requirements.

The Nuclear Regulatory Commission requires periodic emergency response exercises in those areas hosting commercial nuclear power plants.

Corporate preparedness requirements must be met by the oil, natural gas, and chemical operations of the company. For chemicals in particular, the interviewed company has adopted the Chemical Manufacturers Association (CMA) Community Awareness and Emergency Response (CAER) Program emergency preparedness standards, and the pollution prevention and other related standards of the CMA's Responsible Care Program.

## 10.4 Emergency Plans

### 10.4.1 Response Plans

Most emergency response planning within the boundaries of major U.S. cities done on an integrated basis by the agencies involved, with the fire department often responsible for coordination. Mutual aid agreements among some fire departments and fire protection areas have worked well but these may be somewhat limited.

A least one city is in the process of developing a bioplan for infectious disease outbreaks. The primary perceived threat is that international travelers coming into the airport will bring in disease agents. Planning for a sudden disease outbreak is presumably similar for deliberate or accidental causes.

#### 10.4.1.1 Exercises/Drills

Some city-wide disaster plans are exercised annually, participants include the city, suburbs, State, County, Federal and private agencies and the media. The scenarios vary yearly with full EOC

play and limited field play. More specific exercises dealing with, for example, an airplane crash, are also conducted. However, these exercises can be expensive and thus cause a significant drain on limited financial resources.

The private-sector company also has extensive emergency plans, procedures, and practices at both the local level for its facilities and personnel, and at the corporate level to respond to national or international threats. They test these plans, procedures, and practices at all levels with tabletop exercise discussions, drills that focus on limited numbers of functions (e.g., communications procedures and equipment), and full scale exercises. Local facilities participate in these kinds of activities with local fire departments and other emergency response organizations.

The corporate-wide exercises are directed by the Executive Director of Crisis Management, and are carried out by the Crisis Management Technical Support Team, which includes key personnel from throughout the company. One exercise involved an international scenario in which major natural hazard damage to an overseas facility caused a hazardous materials release that destroyed a town and caused significant pollution of a river.

There was an important ingredient in this private-sector exercise that is often lacking in exercises that test private and public sector response capabilities in the U.S. Namely, the Chief Executive Officer of the company participated extensively in the exercise to demonstrate his commitment to corporate emergency preparedness, as well as to obtain practice in, for example, information analysis and response decision making during an emergency. Such demonstrated high level commitment and participation is in stark contrast with many company, local government, state, and federal exercises conducted in the U.S. in which only representatives of officials participate, so that the officials themselves receive no practice in dealing with problems and making decisions during emergencies.

Plans and exercises dealing with natural disasters have been developed and practiced. The same is true for radiologic releases from commercial nuclear power plants. However, responses for terrorist threats, particularly those involving nuclear, biological, or chemical agents are only in their infancy and there is little guidance to help the responsible organizations in preparing such plans. Some municipalities have, however, begun to make progress in this area.

### 10.4.2 Recovery Plans

One of the new areas being researched is referred to as Business Resumption Planning. This portion of emergency planning examines how to get large businesses back in business following a shutdown in an emergency.

### 10.4.3 Communications/Command

Some the more sophisticated emergency response systems make use of microwave and fiber optic networks. In Phoenix, which was cited by several municipalities as a benchmark for emergency planning, emergency responders, and all city agencies can communicate on such a city network that is outside of the local telecommunications company. The system is entirely redundant with back up power available at all critical nodes. The fiber cables are buried four feet deep with a slurry backfill and a concrete cap and signal emitting locators. The 911 system is separate from this system to provide a redundancy. Radios used in the field are composed of 150 MHz for primary communications, 450 MHz for SAUs and a few 800 MHz in the MDTs. All radios are planned to be upgraded to 800 MHz by the year 2000. This is a $ 70 million project expected to take three years.

Another innovative concept used in Phoenix is their global positioning system software that allows their emergency response coordinators to know the precise location of each emergency

response vehicle at all times. Several other municipalities expressed a desire to have similar capabilities.

## 10.5 Information Exchange

A great deal of information is circulating on the subject of terrorism, and the media reports terrorist incidents thoroughly. Attention is being focused on the subject by activities of Congress such as the Nunn-Lugar bill . But there is a feeling and a concern on the part of many emergency managers that the information they get is too diffuse. Nor do they have a time-effective way of determining if the information is applicable to their particular mission or location. They suggested the need for some sort of central clearinghouse for relevant information and guidance. They would like to see a centralized, federal organization responsible for collecting and disseminating information and guidance on planning and preparing for the threat of terrorism. This information would include training opportunities, planning guidance and assistance, emergency response exercise expertise, relevant literature on the subject, funding sources, etc.

A key improvement to information exchange in at least one state is the state mutual aid frequency which is being used by the state's largest counties. This 800 MHZ, ultra-high frequency, with a narrower band, increases the range of communications to far greater distances, increases transmission clarity, reduces atmospheric interference, and transmissions can be relayed by microwave communications towers. Although not fully interoperable, this and other frequencies allow organizations to listen to each other on one frequency and broadcast on another frequency. In addition, the State and its radio stations converting from the old Emergency Broadcast System to the new Emergency Alert System is improving local government interfacing with radio stations and the public by providing shorter, faster, and more direct communications of emergency information through the stations to the public.

The use of emergency response networks in the area of telemedicine for patient diagnosis and care has been beneficial. Procedures including toxicology, pathology, radiology, and cardiology, as well as patient consultations, can now be conducted at medical centers with visual, audio, and data information sent from remote hospital locations over the network. Lives are already being saved, especially in the area of pediatrics.

## 10.6 Research and Development

### 10.6.1 Unmet or Partially-Met Needs

The most commonly expressed unmet or inefficiently met needs are those related to specialized training and specialized equipment. Specialized training needs include:

- Nuclear, biological, and chemical (NBC) training for first responders and support personnel,
- Explosive detection/technician training, and
- NBC training for Emergency Medical Personnel.

Another training issue brought out in these interviews is that exercises should, but do not typically, include the active participation of elected and appointed officials having decision-making responsibility in the event of an actual emergency.

In many cases, the specialized equipment to deal with NBC incidents (detection/monitoring equipment, special communications equipment, vehicles, laboratories) is unavailable or very costly. Many emergency service personnel are very concerned about this issue. Research is needs on methods of prioritizing emergency calls during a wide-spread disaster such as earthquakes.

A high priority for research as expressed by several emergency service personnel is the development of an ability to send live video images from police at the emergency site back to his Emergency Operations Center. In a research project underway in one state, live video has been sent of a simulated drug bust through a prototype wireless digital mini-camera on a policeman's uniform through a Code Division Multiple Access overlay onto available cell phone frequencies to a microwave dish for relay back to a viewing screen at the Emergency Operations Center and other locations on their network. Thus, there is a need to transfer this capability to other emergency service locations.

### 10.6.2 Role of Government

The government has a significant role in assisting the emergency services infrastructure become better equipped and prepared to meet the increasing threat of terrorism within the U.S. In fact, only the federal government has the capability of assisting the states and cities in this effort. Equipment, some of it only available from the military, needs to be made available or developed. General information on terrorism planning and preparedness needs to be gathered by a central clearinghouse and disseminated to state and local governments. National standards for terrorism preparedness need to be set and planning guidance needs to be promulgated. Communications-interoperability problems need to be addressed and solved. Intelligence information needs to be shared.

Several specific research projects were noted in the interviews with the suggestion that the results be transferred as quickly as possible to emergency-services experts throughout the nation.

It was recommended that a national fiber optic cable network be developed to connect state emergency organizations with centralized federal resource centers such as the Centers for Disease Control (CDC). This network would allow the successful, instantaneous transmission of very high resolution microscope slide images to the CDC in case of biological or chemical weapons attacks in locations hundreds of miles from CDC locations. It was noted that federal government funding support, plus federal and state grants of rights-of-way for such cables, are needed.

Federal support in the use of fiber optic networks for conducting live anti-terrorism training simultaneously in multiple locations was suggested. Such training can address the problem of training local first responders like police, paramedics, and firefighters who would have to deal with a chemical or biological attack on key infrastructures and the operational personnel in the first 30 to 90 minutes.

Other roles for the federal government that were discussed in the interviews fall into the categories of funding and legislation. Several people commented that the great expense of emergency response (particularly as terrorist incidents are becoming of greater concern) has stretched city budgets and that federal funding is needed to maintain and expand these capabilities. It was noted that the limited funding provided under the Nunn-Lugar legislation is only sufficient for initial training and initial equipment and supplies purchases. It was recommended that this or similar legislation provide recurring funding over time to provide for refresher training, maintenance of equipment, and replenishment of outdated medical and other supplies.

There is a significant issue with radio traffic congestion on some fire channels and on some police channels. There is a bill pending in Congress, that would make available a 24 MHZ-wide frequency band to public safety radio. This band width was formerly reserved for television. Allocation of this frequency band would more than double the channels available to public safety radio and help solve radio traffic congestion problems.

The lack of standards for minimum requirements concerning equipment and supplies to support emergency responders, as well as a lack of minimum, standardized training goals, were also indicated as matters of concern about the Nunn-Lugar legislation. It was recommended that follow-up legislation contain such provisions. It was also noted that the existing hazmat and urban search and rescue teams provide a good example of standardization, and that appropriate additions could be made to the existing hazmat training standards.

It was suggested that the federal government develop, as was done for the Radiological Emergency Preparedness Program, and the Chemical Stockpile Emergency Preparedness Program, guidelines (*not requirements*) for Anti-Terrorism /Infrastructure Protection Planning and that these guidelines be made available to all state and local emergency planners. The guidelines should address the critical, vulnerable aspects of the infrastructure, and should include a planning methodology and recommendations for protection of the infrastructure.

# 11 CONTINUITY OF GOVERNMENT SERVICES

## 11.1 General Information

### 11.1.1 Background

Continuity of government services refers to the ability of federal, state, and local governments to meet the needs for essential services to the public during and after an emergency. Such emergencies include natural disasters (e.g., floods and hurricanes), military attack, technological emergencies, or any other emergency that seriously degrade or threatens the Nation's security. Preparedness planning in this area requires the identification of functions that would have to be performed during an emergency, the identification of personnel for performing those functions, the development of plans and the capability to execute those plans. This critical infrastructure is closely linked with each of the others considered by the Commission.

### 11.1.2 Organizations

In an attempt to gain perspectives from each of the federal, state, and local levels of government, interviews were held with two federal agencies, one state agency, and a representative of a large U.S. city. The two federal agencies are the National Security Council (NSC) and a regional office of the Federal Emergency Management Agency (FEMA).

Each federal agency providing services such as Social Security checks and airport flight controllers, is responsible for ensuring the continuity of those services. The NSC's role in this infrastructure is to provide clear guidelines to other federal agencies concerning necessary components of the continuity of operations plans required of each agency.

FEMA is comprised of ten regions. It is the responsibility of these regional offices to implement the policies and actions of the main office and to coordinate federal activities during an emergency in their region and provide aid during recovery from a disaster, even if it is directly affected as well. One of these regions was interviewed as part of the Commission effort.

A state Comptroller's Office was also interviewed. This office is responsible for paying the state's debts by issuing and mailing checks. The payees of these checks include vendors, public aid recipients, unemployment insurance beneficiaries, state employees (payroll checks); and taxpayers (refund checks).

At the local level, a representative of the city office of Emergency Preparedness and Disaster Services was interviewed. The government services addressed were mainly concerned with government functions such as keeping the courts open and maintaining government records such as vital statistics, tax records, and land ownership records.

### 11.1.3 Infrastructure Involved

As noted above, the continuity of government services infrastructure is closely connected with each of the other infrastructures identified by the Commission. To the extent that it is a government responsibility to maintain services in each of the other infrastructures, there is a direct connection with them.

## 11.2 Threats and Vulnerabilities

### 11.2.1 Types of Threats

Persistent threats to this infrastructure include physical threats (e.g., bombs, tornadoes, earthquakes) that can cause death or injury. Depending on the type of service provided, and to an extent the modernization of the system with respect to being a paperless organization, physical threats could severely disrupt operations without causing significant property damage or injury.

There have been several instances of actual or potential loss of official records due to natural floods or floods caused by disruption of man-made facilities, e.g., water mains. Loss of electrical power is another threat that can directly impact government services. Many organizations have back-up power generators, but long term outages could have significant impacts.

The primary threats to this infrastructure are dependent upon the type of services provided by individual agencies. Services such as Social Security and Medicare checks face cyber threats to computer systems and data bases, whereas airport controllers face both cyber and physical threats. Examples of airport cyber threats cited include losses of controller computer systems. Chemical or biological weapons attacks on personnel could cause either temporary or long term damage to the airport infrastructures depending upon how much corollary physical damage results (e.g., building, runway, computer damage).

The types of threats that FEMA responds to are primarily natural disasters, such as flooding, hurricanes, and earthquakes, although they are also charged with responding to technological emergencies involving radiological or hazardous material releases. Specific threats to the operation of FEMA itself include explosion, or hurricane damage, etc. Another threat that was discussed is the possibility of losing (either because of an accident or because of malicious interference) FEMA's computer records. Loss of communications is also of concern. In those instances where government computers are connected to the Internet to provide public information warehouses, a cyber threat to the security of confidential files arises.

Many government services are dependent upon communication, information flow, and physical action between and among other government agencies. For example, one agency may be responsible for issuing public aid checks but another agency is responsible for maintaining a database of eligible recipients. Thus the continuity of an agency's services is vulnerable to threats on its own infrastructure but also of threats on other agencies and the associated links between them.

An example was cited in which the local electric utility company had failed to provide the city with up-to-date information about its distribution system. This hampered efforts to fight fires and restore power. Loss of electrical power to the county court and county jail was prolonged unnecessarily because changes that had been made to the distribution system were not communicated to the city.

The physical deterioration of many infrastructures in the United States is also a threat. The inability to utilize these infrastructures can impact the operation of government and, in those cases where a government is responsible for maintaining and operating them, can increase costs and cause losses or hardship to the public. For example, if a natural gas distribution system deteriorates to the point where it can no longer provide gas for heating a government building, the services provided in the building are vulnerable. If the gas distribution system is government owned, then the gas service provide by the government to the public has also been compromised.

### 11.2.2 Vulnerability Assessments

It was indicated that a threat assessment has been conducted for federal services overall, and that vulnerability assessments are taking place on a decentralized, agency-by-agency, basis. These assessments are being made to identify vulnerability-reduction actions needed to ensure each agency's continuity of operations, which is the foundation for continuity of government services. It was noted, for example, that events such as the World Trade Center and Oklahoma City bombings can extensively disrupt government services in a given region for a substantial period of time.

The FEMA Regional Office has not performed formal assessments of their own vulnerability. However, vulnerability of areas of the United States to flooding, hurricanes, earthquakes, and

other natural disasters is part of their ongoing programs and they have participated in assessments of a variety of infrastructures for a variety of natural and man-made threats.

### 11.2.3 Vulnerability Reduction Actions

In common with other State agencies, the Comptroller's Office has a disaster recovery plan, including an alternative site for operations. This alternative site is a "hot site", that is, it is kept in a state of readiness with periodic tests, so that operations could be quickly moved there if necessary. The applications being implemented on the IBM mainframe are supposed to be "year 2000 compliant" so that the system will not be disrupted when January 1, 2000 arrives. The State is planning to convert to paying public aid recipients by using electronic benefit cards, which would be similar to debit cards. Means to ensure that these cards are not misused must be developed, but the interviewee thought that it should be relatively easy to encode limits on use into them.

It was also indicated that federal investments for infrastructure protection and improvements in the area of government services have included federal funding contributions to development of: 1) the new digital Emergency Alerting System for providing emergency instructions to the public, 2) military chemical/biological response teams for consequence management of terrorist attacks, 3) training, equipment, and supplies packages for accidental or deliberate lethal chemical/biological releases to be provided to state and local emergency responders under the 1997 Nunn-Lugar anti-terrorist legislation, 4) various detection systems (e.g. sensors), 5) communication systems (e.g., fiber optic cable, satellites), and 6) dispersion modeling studies related to chemical and biological releases, also under the Nunn-Lugar legislation.

Additional training of employees and emergency-response-personnel is frequently mentioned as a means to reduce vulnerabilities. Adequate equipment is also an important factor.

### 11.2.4 Investment Considerations

Only one of the interviewees chose to discuss investment considerations. This was the representative from the state-level Comptroller’s Office. He indicated that as an auditor, he thinks in terms of risk. Before making an investment, he balances the severity of the risk against the costs of mitigation. Connecting the mainframe computer to the Internet is but one manifestation of a generic vulnerability - the use of facilities or equipment also used by the public. Firewalls could protect confidential files on the mainframe from intrusion from the Internet, but firewalls are expensive. Use of telephone lines that go to exchanges present a vulnerability of public access that is eliminated if dedicated lines among State agencies are used. However, the costs of these mitigation techniques should be weighed against the reductions in risk to determine whether the investment is worthwhile.

## 11.3 Requirements and Standards

Key requirements have been set for each federal agency’s planning and response to natural, accidental, and deliberately caused impacts upon critical infrastructures in Executive Order 12656. These call for the agency continuity of operations plans as well as key backup capabilities to ensure that these plans can be implemented even with the loss of important infrastructure components (e.g., telephone communications, electricity). Of course, all actions must be in compliance with applicable laws.

One interviewee noted that the American National Standards Institute, Commission 12, is addressing standards for electronic data transfer.

## 11.4 Emergency Plans

### 11.4.1 Response Plans

FEMA is in the process of producing a regional plan for continuity of government. This plan will designate an alternate regional office (and Emergency Operations Center) for use if the regional offices are disabled. This alternate site will be located in a different local from the current offices. When completed, the new regional plan will need to be tested (exercised).

The national Federal Response Plan (FRP)[4] does not specifically address continuity of government services either, but it does indicate that federal assistance will be forthcoming in event of a disaster. The FRP and the National Contingency Plan supplement the individual agency continuity-of-operations plans and facilitate the coordinated response by multiple federal agencies when critical infrastructures are threatened or attacked. Federal drills and exercises related to natural disasters and terrorist attacks are conducted frequently to improve preparedness and response to high impact events on critical infrastructures and the public. These exercises deal in vague ways with both the response to and recovery from high impact events such as earthquakes, hurricanes, and terrorist attacks on subway systems, convention centers, etc. The FRP is currently undergoing review and revision and FEMA is the lead for the interagency FRP review.

Most emergency response planning within the boundaries of major city represented in these interviews is done on an integrated basis by the agencies involved, with the city fire department responsible for coordination. In the greater metropolitan area, there are mutual aid agreements among fire departments and fire protection areas which have worked well.

The city is in the process of developing a bioplan for infectious disease outbreaks. The primary perceived threat is that international travelers coming into the international airport will bring in disease agents. Presumably, planning for a sudden disease outbreak is similar whether the cause is deliberate or accidental.

### 11.4.2 Recovery Plans

The FEMA interviewee suggested that an assessment be done and a determination made regarding which government services must be maintained in the event of an emergency. The services should be delineated and prioritized so that (1) the most important functions are adequately protected (including ones that affect the functioning of FEMA regional offices), and (2) to establish the order in which services would be brought back on line following disruption. This latter thought was also suggested by the representative of city government who also suggested that city government should be high on that list of priorities.

## 11.5 Information Exchange

A variety of organizations or working groups are examining issues relating to continuity of federal government services. These include several federal interagency task forces, such as the Commission itself, the Technical Support Working Group which addresses terrorism, and the U.S. Interagency Disaster Information Task Force, which addresses the issue of how to best use federal information and networking technologies and systems to support the public and private sectors prior to, during, and following natural disasters. Finding of these groups should be shared among the potentially impacted federal, state, and local governments.

---

[4] *Federal Radiological Emergency Response Plan*, Federal Emergency Management Agency, May 1, 1996.

Two professional organizations were noted that do research on reducing risks of electronic data interchange and publish journals that provide for information exchange. These are the Institute of Internal Auditors and the Information Systems Audit & Control Association.

### 11.6 Research Needs

The key research needs identified in this area were detection capabilities for chemical and biological releases, dispersion modeling refinements and enhancements, and the need for improving national communications systems to better link federal, state, and local governments with the industries comprising critical infrastructures. Each of these research areas provide opportunities for better ensuring that federal government services will not only maintain continuity, but also be enhanced.

Governments role in the sponsoring research and development for improved technologies. Several specific technologies were noted including a means of rapidly identifying and locating hazardous-materials spills following a transportation accident, personal protection systems that simultaneously guard against fire and hazardous materials, improved thermal sensors for fire detection, chemical detection sensors, and personal monitoring devices (blood pressure, heart rate, breathing rate, etc) to be worn by emergency-response personnel.

# APPENDIX A

# INTERVIEW QUESTION TEMPLATE

## APPENDIX A

## INTERVIEW QUESTION TEMPLATE

The following is an early list of proposed questions will provide a general structure for conducting interviews in all of the critical infrastructures. However, all interviews must be allowed to take a course that permits each party to express needs and concerns on these and other, related issues and to allow discussion of needs and concerns of specific interest to each individual infrastructure.

- Have you identified specific threats to your infrastructure area?
  - Physical
  - Cyber
  - Conventional
  - Nonconventional

- Have you conducted a vulnerability assessment?

  - Where they conducted by in-house personnel or contractors?
  - What methodologies were applied?
  - Where methods developed in-house?
  - Where are greatest areas of vulnerability?
  - What is the vulnerability?
    - Financial
    - Loss of property
    - Loss of life
    - Loss of services
    - Other

- Does vulnerability extend beyond your specific sphere of responsibility?

  - What areas
    - Other parts of infrastructure
    - Other infrastructures

- Are there established requirements or standards that must be met?

  - Regulatory
  - Industry standards
  - Company Practices

- How do regulations in your area promote, or detract from, protection of critical infrastructure?

  - Think in terms of:
    - Direct requirements for security such as restricted access, background checks on employees, emergency planning requirements, etc.

    - Requirements aimed at general system reliability that may incrementally reduce vulnerability against attack, e.g., equipment interconnection, inspection requirements, etc.

Rules that may indirectly affect investment in security, e.g., rules that limit liability for service outages or that prohibit information sharing, etc.

- Do you have ideas on how to improve the situation through changes in rules, e.g., newer, better, or fewer rules?

- Do you have emergency response plans?
  - What types of drills are conducted and how often?

- What kind of system or operational enhancements will lessen vulnerability?
  - Protection
  - Detection
  - Response
  - Mitigation
  - Recovery

- Are you aware of existing capabilities/technologies to reduce vulnerabilities?
  - Have any been implemented or are plans underway?
  - How was decision made to implement?
  - Have implemented actions been successful? (Define successful)

- What level of investment would you be willing to make to improve infrastructure protection?

- Are there areas of concern for which you know of no feasible enhancements to system or operations to reduce vulnerability?
  - Do any technologies/capabilities exist?
  - Are existing technologies/capabilities ineffective?
  - Are existing technologies/capabilities not cost effective?

- Do you know of any R&D programs that address these issues?
  - What is being done, by whom, and status?
  - What R&D areas should be addressed?
  - What is time frame of need?

- Is there adequate information exchange on threats, vulnerabilities, technologies, etc. regarding infrastructure protection?
  - What mechanisms exist?
  - How might existing mechanisms be improved?
  - What other mechanisms do you suggest?

- Is there a role for government in conducting research on any of the following?
  - Methods development for threat or vulnerability assessment?
  - Hardware development for infrastructure protection?
  - Collecting, storing, and distributing information?
  - Other areas?

- Other areas of concern and discussion

# APPENDIX B

# WATER SUPPLY STAKEHOLDER'S QUESTIONNAIRE

## STAKEHOLDER QUESTIONNAIRE FOR PROTECTION OF CRITICAL WATER SUPPLY SYSTEMS

1. Have you identified specific threats to your potable water supply system?

    a. Physical threats (e.g., destruction of impoundments, destruction of distribution system components [pump stations, valves, control units, etc.], water hammer).

    b. Chemical threats (e.g., nerve agents [e.g., BZ, VX, GD], other highly poisonous chemicals [e.g., trichotecene mycotoxin T-2, sodium fluoroacetate, botulinum toxin]).

    c. Biological threats (e.g., *Bacillus anthracis*, *cryptosporidium parvum*, hepatitis A).

    d. Nuclear threats (e.g., cobalt-57, calcium-45).

    e. Cyber (e.g., loss of control of critical system components).

2. Have you conducted a vulnerability assessment for your system?

    a. What methods were used?

    b. Where are your greatest vulnerabilities (e.g., raw water supply, treatment plant, distribution network)?

    c. What is the vulnerability (e.g., financial, loss of property, loss of life, loss of services, other)?

3. What kind of system or operational enhancements would decrease your vulnerability?

    a. Protection (e.g., minimizing access to your system and its detailed plans, filtering, changing to a more effective disinfectant, maintaining higher levels of residual disinfectant, maintaining a high system pH).

    b. Detection (e.g, chemical or biological agent-specific monitoring devices, optimized monitoring device locations, continuously monitoring the level of residual disinfectant).

    c. Mitigation (e.g., back-flow prevention devices, automatic residual disinfectant injection).

    d. Response (e.g., detailed contingency plans, operator training, public awareness).

    e. Recovery (e.g., detailed long-term plans for system rehabilitation).

4. Are you aware of existing capabilities/technologies to reduce your vulnerability?

    a. Have any been implemented or are plans underway?

    b. How was the implementation decision reached?

    c. Has implementation been successful?

5. What level of investment would you be willing to make to improve infrastructure protection?

6. Are there any areas of concern for which you know of no feasible enhancements to system or operations that would reduce vulnerability?

    a. Are there any known existing technologies that address this problem?

    b. Are existing technologies ineffective?

    c. Are existing technologies too costly?

    d. Do you know of any research and development programs that address this area?

    e. What is being done, by whom, and what is the status of the research?

    f. What specific research and development should be addressed?

    g. What is the time frame of interest?

7. Is there adequate information exchange on threats, technologies, etc., regarding infrastructure protection?

    a. If not, how might it be improved?

8. Are there any other areas of concern or discussion?