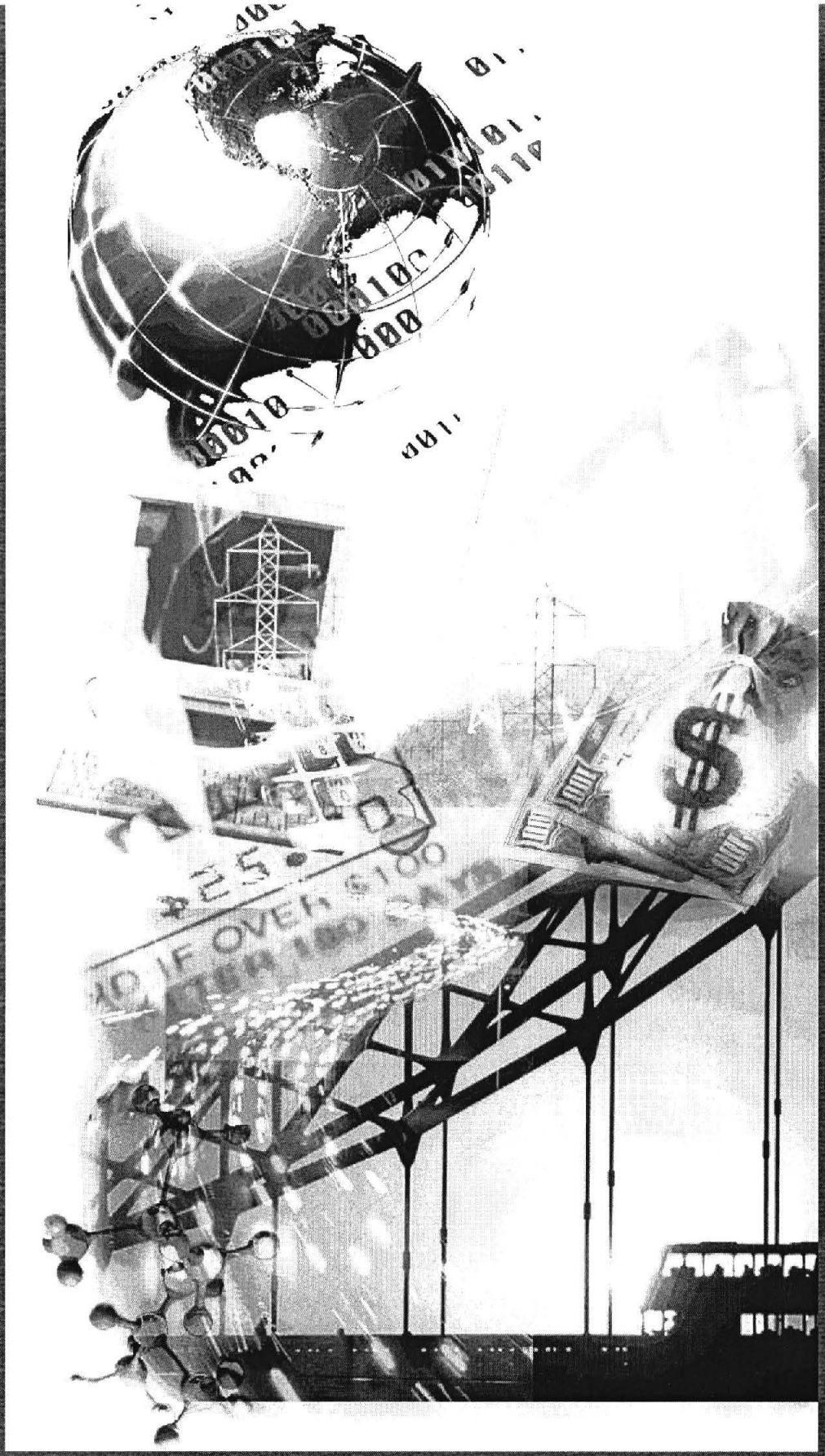


US INFRASTRUCTURE ASSURANCE STRATEGIC ROADMAPS

AUGUST 1998

STRATEGIES FOR PRESERVING OUR NATIONAL SECURITY

STRATEGIES FOR PRESERVING OUR NATIONAL SECURITY

US INFRASTRUCTURE ASSURANCE STRATEGIC ROADMAPS

AUGUST 1998

Sponsored by:

The President's Commission on Critical Infrastructure Protection
US Department of Energy
US Army Medical Research and Materiel Command
Sandia National Laboratories

Roadmap Champions:

Telecommunications Technologies International (TTI)
Electric Power Research Institute (EPRI)
Scientech, Inc.
Banker's Industry Technology Secretariat (BITS)
Alliance Transportation Research Institute

SAND98-1496

Issued by Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

table of contents

foreword

OBJECTIVE

As individuals and as a nation, we depend on US infrastructures to provide the essential services that support our economic prosperity, national defense, and quality of life. Some of these services have become so vital that if they were disabled or disrupted, there would be a debilitating effect on the nation or on specific regions of the country. National concern escalated in 1996 to the point that the President's Commission on Critical Infrastructure Protection (PCCIP) was formed by President Clinton to assess vulnerabilities of the critical infrastructures and recommend strategies for their continued protection.

This document presents six roadmaps designed to guide the improvement of infrastructure surety.

In support of this effort, Sandia National Laboratories facilitated two US Infrastructure Assurance Prosperity Games™ to validate or invalidate strategic options for policy, process, and supporting technology applications that substantially increase the surety (security, safety, and reliability) of US infrastructures. These Prosperity Games™ were interactive exercises sponsored by the Department of Energy, the National Communications System, and the PCCIP.

This document presents technology and policy roadmaps that build on results of the Prosperity Games™ for each of the six critical infrastructures identified in the games - Communications and Information, Electric Power, Oil and Gas, Banking and Finance, Transportation, and Emergency Services.

The US Infrastructure Assurance Prosperity Games™ were an initial vehicle for roadmap development.

> Roadmaps are strategic plans for the development and introduction of technologies and policies into an essential system to improve the valued outputs of the system. Outputs can be cost, quality, performance, or any other featured system product.

US INFRASTRUCTURE ASSURANCE PROSPERITY GAMES™

Two US Infrastructure Assurance Prosperity Games™ were conducted in 1997, one in January in Albuquerque, NM, and the other in March in Chantilly, VA. Prosperity Games™ are interactive simulations that explore complex issues in a variety of economic, political and social arenas. The simulations are high-level exercises of discretion, judgment, planning and negotiating skills. These events brought together over 200 stakeholders with expertise in technologies and policies pertaining to each of the critical infrastructures. Stakeholders included entities from government, industry, academia, and citizen's organizations.

A wide range of infrastructure stakeholders participated in the Games.

The games provided an environment in which alternative futures could be created. The games established for the participants:

Participants were able to gain understanding of opportunities and obstacles facing critical infrastructure surety.

- a format for prioritizing issues amidst an environment of competing self interests
- a process for addressing high-level solutions to very large problems that may not be solvable by other methods
- a unique environment for fostering collaboration and managing conflict

foreword

The two games were played in series so that the second game built on the results of the first. Both games were structured around three objectives:

- Objective I: Produce insights on the perceived advantages and disadvantages of a variety of solutions for protecting the infrastructure.
- Objective II: Produce insights on the relationships most effective—including government, industry, or industry-government partnerships—for implementing solutions.
- Objective III: Develop a clear understanding of missions, roles and functions of organizations that should be involved in planning and implementing priority solutions.

ROADMAP DEVELOPMENT AND DISTRIBUTION

These roadmaps represent industry's perspective.

Following the Prosperity Games™, an industry expert from each of the six critical infrastructures was identified from among the game participants to champion the development of respective infrastructure roadmaps. This approach was taken to capture the perspective of issues and concerns that surfaced in the games and to provide continuity in this infrastructure assurance project. The champions formed their own workgroups of experts in technology and policy from their infrastructure sectors. Roadmap champions provided the initial drafts of the roadmaps, which were subject to revision by the roadmap project manager. Revisions were performed to provide the most current information available on the critical infrastructures and to include information that would help strengthen the individual roadmaps and this overall document.

In order to continue progress toward the goals detailed in the completed strategic plans, these technology and policy roadmaps will be disseminated to consortia and working alliances committed to the assurance of the nation's critical infrastructures. Infrastructure stakeholders must provide the follow-up essential to achieve the goals outlined in the roadmaps.

FINAL COMMENT

Cooperation and support resulted in an overall plan for the future of US infrastructure surety.

We greatly appreciate the cooperation and support of the sponsoring organizations, champions, and all others who contributed to the development of the roadmaps. Their support has been instrumental to the success of this project. The list of cosponsors for the overall effort include:

- The President's Commission on Critical Infrastructure Protection
- National Communications System
- US Department of Energy
- US Army Medical Research and Materiel Command
- Telecommunications Technologies International (TTI)
- Electric Power Research Institute (EPRI)
- Scientech, Inc.
- Banker's Industry Technology Secretariat (BITS)
- Alliance Transportation Research Institute
- Sandia National Laboratories

foreword

We would also like to extend our gratitude to the many reviewers of the roadmaps, whose comments proved invaluable throughout the roadmap development process.

The roadmaps that follow comprise technology and policy strategies to provide for the surety of the nation's critical infrastructures. This plan is an initial step in a comprehensive infrastructure assurance effort and is intended to enhance and complement infrastructure protection activities initiated by other entities. The complexity and scope of protecting US infrastructures will require close cooperation by all infrastructure stakeholders in order to ensure the continued prosperity and security of our nation.

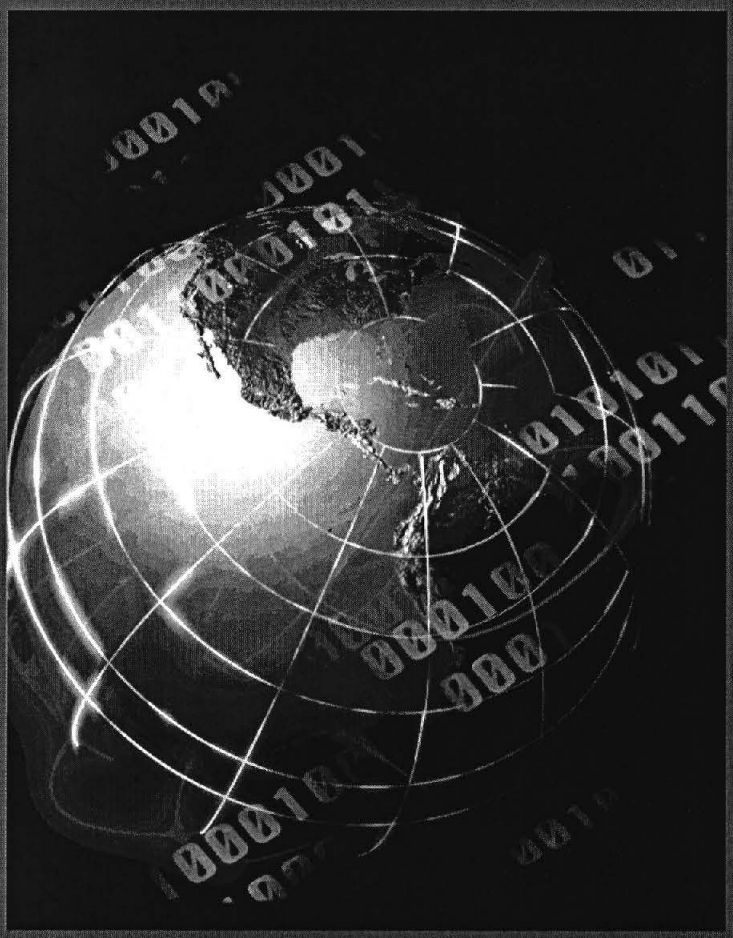
Samuel Varnado
Director, Energy and Critical Infrastructure Center
Sandia National Laboratories

Jennifer Nelson
Manager, Critical Infrastructure Surety Department
Sandia National Laboratories

Juan J. Torres
Roadmap Project Manager
Sandia National Laboratories

foreword

US Communications and Information Infrastructure Strategic Roadmap



The US has the most advanced communications and information infrastructure in the world, with high-quality, ordinarily reliable services. These services are essential to national defense, our economy and the infrastructures that support our society and each of us personally, and we take for granted that they will remain secure. But, in fact, our communications and information infrastructure is vulnerable to physical and cyber attacks that could harm national security and the economy and endanger human lives. The list of vulnerabilities is long. There are divergent views on their seriousness, and there is no consensus on what to do. These are serious concerns for all of us. The federal government, equipment and service providers, and customers must work together to improve infrastructure surety.

This chapter provides an overview of the communications and information infrastructure and its vulnerabilities and concludes with a roadmap to greater security and reliability.

DESCRIPTION

The primary concerns of the highly competitive communications industry are functionality, speed, and cost.

The US Communications and Information Infrastructure is characterized today by rapid, powerful, and competing technologies and services provided by companies both new and long-established in the communications industry. This infrastructure is no longer the unified, centrally planned nationwide telecommunications network that served our country so reliably for much of the twentieth century. Telecommunications services are now provided by intensely competitive local and long distance companies and resellers, and the infrastructure comprises a large number of computer networks and the Internet as well. Federal, state, and local government, emergency care providers, financial institutions, the transportation sector, energy sectors, all major industries, and Americans in every walk of life depend increasingly on communications and information. Functionality, speed, and costs are primary concerns in this competitive environment; national security and reliability are secondary.

In a network-of-networks environment, competitive companies must work together.

In spite of the differences among the industries represented, a network-of-networks is evolving that impacts our entire society. Even though individual industries were not contemplated to work together seamlessly and interactively, as they converge, they must begin to collaborate.

Competition is no guarantee of security or reliability.

Regulatory restructuring is opening the doors for competitors to enter all major segments of the telecommunications industry. Competition generally brings new and better services and lower prices for both business and residential customers, but competition does not guarantee greater security and reliability.

Communications and information services are rapidly expanding in the US and throughout the world, and wireless services, in particular, are growing at a steep rate. It is estimated that the number of telephone subscribers throughout the world will increase from a billion today to three billion in 2010. The number of wireless subscribers will increase in those same 12 years from approximately 150 million today to more than ten times that number in 2010, when they will make up more than half of all subscribers.[1]

The rate of growth for information services is no less remarkable. As one indicator, the number of host sites on the Internet has grown dramatically, and at an accelerating pace in recent years. Some estimates indicate that as many as 50 million Americans will be regularly logging onto the Internet by the end of 1998.[2]

The US Communications and Information Infrastructure is an intimate part of a rapidly expanding international and global communications infrastructure. Our infrastructure is closely linked with networks in other countries, and the flow of communications and data to and from the US is large and growing. Financial and banking transactions provide an obvious and important example, and, more generally, electronic commerce is increasing across a broad range of industries.

The global communications and information infrastructure can have serious and widespread effects upon the security and reliability of the US infrastructure. The assessment of threats and vulnerabilities in this roadmap includes domestic, international and global factors.

ALL CRITICAL INFRASTRUCTURES DEPEND UPON ADVANCED COMMUNICATIONS AND INFORMATION SERVICES

Advanced communications have already made a fundamental change in commerce, transportation, public safety, and utilities.

Advanced information technologies are introducing fundamental changes into our basic institutions and infrastructures.

- In banking and finance, information technologies have displaced manual and paper transactions in processing payments, transfers and withdrawals, and in overall business operations. Electronic banking has simplified and greatly accelerated a wide range of transactions essential to a productive economy.
- In transportation, commercial aircraft and land and sea vessels rely on state-of-the-art communications for navigation and safety, as do military and private vehicles. All forms of transportation depend upon communications for signaling, weather information, scheduling, personnel and materials handling, passenger reservations, ticketing, billing, and more.
- The links between electric power and telecommunications are long-standing. For many years, electricity transmission companies have deployed communications lines along their rights-of-way to monitor their facilities, afford reliable contact and information for maintenance and repair workers throughout their systems, and, increasingly, to optimize the use of electric power for the benefit of both customers and the environment.
- Oil and natural gas transport companies use information in some of these ways also. With the passage of the Telecommunications Act of 1996, some electric power and natural gas companies are leasing their rights-of-way to telecommunications companies or using excess capacity in their communications lines to offer telecommunications services themselves. The industries are interacting more closely than ever before.
- Federal, state, and local governments rely on the communications and information infrastructure to provide services, and the national defense community, in particular, depends increasingly upon the public telecommunications network (PTN) and commercial information technologies for everything from administration, to recruiting new personnel, to achieving battle readiness.

- State and local governments depend upon communications and information in their day-to-day operations and could not function without this infrastructure. Transportation, electric power, natural gas, water, and sanitation systems typically operate under state or local supervision, and in many instances utilities are publicly owned and operated. In all cases, they depend on the communications and information infrastructure.
- In cities, towns and rural areas all across America, police officers, firefighters, and emergency medical service (EMS) providers count on the PTN for contacts, critical information, and assistance. Dependable communications services, particularly wireless services, afford vital links between police officers, firefighters, EMS technicians, hospitals, and doctors and patients, especially in life-threatening situations.
- Communications and information service providers rely on electric power, oil and natural gas services, transportation, banking and finance, emergency services, and government at all levels for the very basic resources they need in order to operate. The brown-outs that swept across the western states in early July 1996, the severe ice storm that afflicted the northeastern US and Canada in late 1997 and the first days of 1998, and the severe floods in the Midwest in 1993 and in California in 1997 all disrupted power and communications services for millions of people in those areas. Our nation's critical infrastructures are interdependent, and strengths or weaknesses in one infrastructure typically have significant impact upon others.

INCIDENTS SUGGEST WIDER VULNERABILITIES

Infrastructures are highly vulnerable to cyber attacks, human error, and technology weaknesses.

These and many other disruptions in our communications and information services cost American taxpayers and American companies hundreds of millions of dollars, destroy valuable work, and jeopardize people's economic security and even their lives. The incidents indicate that the communications and information infrastructure is open not only to cyber attacks, but to administrative and operational problems resulting from human error, equipment obsolescence, incompatible technologies, system overload, system complexities, and other factors.

Physical vulnerabilities must not be ignored. Although the bombing at the World Trade Center in New York City in 1993 and the bombing of the federal building in Oklahoma City in 1995 were not directed at communications facilities, they demonstrate the ability of extremists to damage and destroy facilities of all kinds, with devastating consequences. Natural disasters, hurricanes, floods, and storms can also wreak far-reaching damage to critical communication components such as switching systems, routers, signaling systems, and transmission lines.

Following are just a few examples of recent attacks and disruptions on the information infrastructure.

- Galaxy IV Satellite Incident – May 1998
  From one end of the continent to the other, 80 to 90 percent of our 45 million pagers suddenly stopped beeping, gas pumps would not take credit cards, and TV and radio broadcasts were knocked off the air—all because a single satellite rolled out of position. Doctors, midwives, TV meteorologists, and law enforcement officers scrambled to find ways to cope with the technology breakdown. It was a stark demonstration of the vulnerability of technology and our dependence on instant communication.
- DoD – February 1998
  Hackers made at least 11 assaults on US military computers in February 1998 in what officials called a "fairly heavy-duty cyber-attack." Two California teenagers were suspects in the incidents, and one of the boys was caught hacking into an unclassified Pentagon computer. The boys' homes were searched, and equipment and software were seized, but the boys were not arrested.[3]
- Kansas City Air Traffic Control Center – December 1997
  In December 1997 at the Federal Aviation Administration's air traffic control (ATC) center in Olathe, Kansas, the systems that display radar information and enable controllers and pilots to communicate by radio failed. These information and communications system failures were the result of an accidental disruption of electric power caused by simple human error. Hundreds of planes bound for Kansas City and St. Louis had to be diverted or held, causing delays for tens of thousands of passengers traveling to and from airports throughout the Midwest for much of the day. This was the latest in a series of disruptions of air traffic control systems in recent months.
- FBI and CIA – 1996
  Hackers successfully broke into the web sites of the FBI and CIA and defaced their home pages. The incidents indicated a greater vulnerability than was previously realized.[4]
- Department of Defense – 1993-1995
  DoD officials estimate as many as 250,000 costly and damaging attacks on DoD computer systems from 1993 through 1995. Attackers stole, modified or destroyed data and software, installed "back doors" to circumvent systems' security and allow the attackers unauthorized access and the ability to shut down entire systems and networks.[5]

- Bell Atlantic and Pacific Bell – June and July, 1991

  From June 10, 1991, to July 2, 1991, Bell Atlantic and Pacific Bell experienced six separate service disruptions caused by malfunctioning of their Signaling System 7 (SS7) networks. The worst of the outages, on June 26, 1991, affected service for more than five million customers in Maryland, Virginia, West Virginia, and the District of Columbia. In each instance, an apparently random event occurred that led to severe congestion at a signal transfer point (STP), which, in turn, affected other STPs and disabled the signaling network. The signaling system sets up the connections required for all telephone calls and data messages and is an essential part of telecommunications.[6]

- AT&T – 1990

  In New York City, software problems caused a chain reaction of AT&T switch failures that resulted in a nine-hour outage. All three of the major airports in the New York City metropolitan area were forced to shut down, and 65 million calls were blocked nationwide.[7]

- The Morris Worm – 1988

  In this notorious case, Robert Morris, a young student at Cornell University in Ithaca, NY released a destructive software code into computers connected to the Internet. The Morris Worm, as it came to be known, penetrated and damaged functions in as many as 4,000 computers, about 10% of all computers on the network at that time.[8]

FUTURE TRENDS: ADVANCING TECHNOLOGIES, POTENTIALLY GREATER VULNERABILITIES

As computers and systems grow larger and more complex, the greater the possible damage from intrusions.

The Communications and Information Infrastructure today will likely face even more serious vulnerabilities and threats in the years ahead.[9] As computers and communication systems gain greater capacity and speed, and communications lines simultaneously carry large blocks of graphic, video and multimedia information along with a multitude of message data, a small software mistake or intrusion can quickly and easily cause a loss of critical data or interrupt vital communications links. For some service regions, the greater capacities of advanced switching and transmission systems increase routing alternatives and reduce denial-of-service vulnerabilities, resulting from heavy traffic or large bursts of information. However, redundancies and capabilities in other service areas have not been increased, leaving many users vulnerable and, unless made more secure and reinforced, will provide greater exposure as their capacity increases.

Accelerating and far-reaching advances in computer processing speed, power, memory, and storage capabilities are bringing new systems and software to the marketplace at a furious pace. Because of this rapid replacement cycle, there is ever-greater likelihood that flawed systems and software will be introduced into the Communications and Information Infrastructure, endangering communications and information that are critical to national security and the economy. More complete and accurate information on the possible problems with new technologies, systems and software, and better dissemination of such information among customers may be helpful in mitigating this danger. Better information might encourage providers and other large organizations, which depend fundamentally on communications and information systems, to regularly and methodically conduct their own thorough tests on new systems and software before using them.

Faster and more frequent advances in technology also increase the chances for introducing weakness into the infrastructure.

Advancing technologies will bring needed services, but will also afford opportunities for serious harm. Both physical and cyber threats will be exacerbated. Products and software are updated rapidly, and providers and their customers may be less concerned with potential bugs in the new products and more focused on getting systems in place to meet immediate needs. Thorough testing can be a lengthy and costly undertaking, and customers may opt for something less, thinking that no matter what equipment or software is chosen, it will likely be obsolete soon. Vulnerabilities are easily introduced in this environment.

Vulnerabilities are more likely to be introduced in a rush-to-market environment.

Vulnerabilities, if ignored, can give rise to threats that may never have arisen otherwise. Targets of opportunity may simply be too attractive for dissatisfied employees, the mischievous, competitors, criminals, dissident individuals and groups, organized crime, terrorists, or hostile nations. Therefore, if vulnerabilities increase, threats may increase also. The US position as a world military superpower and economic leader also makes it a more visible target. US armed services maintain secure and robust communications for all key command, control, and intelligence operations. For less essential but still critical operations, DoD, like other federal departments and agencies, depends on the PTN; its reliability cannot be taken for granted. We must assure that our defense against information warfare is as effective as our physical defense.

Reliability and security cannot be taken for granted.

Some factors that may increase vulnerabilities include:

- Increasing importance of communications and information in every aspect of our lives, creating new opportunities and new exposure. The increasing use of services for transmitting sensitive, personal, and proprietary information highlights such vulnerabilities.

- Convergence of diverse industries in communications and information services, often bringing together diverse and incompatible systems, architectures, technologies, and software.
- Rapid expansion and change in the infrastructure to accommodate new and challenging demands, with comparatively little time and effort being spent on the security concerns that may arise from such new applications.
- Rapid growth in hardware and software complexity, capacity and speed.
- Increasing reliance on high-capacity, high-speed, "keystone" systems whose functions and capabilities may increase interdependencies with other facilities or infrastructures.
- Sharp growth in the number of individuals and companies accessing information and using communications, with greater likelihood of accidental or intentional interference.

DEFINING INFRASTRUCTURE PRIORITIES

To create a roadmap that will secure the Communications and Information Infrastructure, we must first identify and prioritize this infrastructure's most critical issues.

PRIORITY 1: DEVELOPING EFFECTIVE FEDERAL, STATE AND LOCAL GOVERNMENT LEADERSHIP AND CLEAR POLICY GUIDELINES

Government leadership is critical to motivating all infrastructure stakeholders for unified action.

A number of federal departments and agencies have responsibilities in addressing Communications and Information Infrastructure vulnerabilities and threats. However, these agencies currently lack the resources, as well as the clarity of responsibility, jurisdiction, and authority for defining and enforcing national policies for the Communications and Information Infrastructure. Therefore, the first priority is for government to define and adequately fund an agency responsibility and reporting structure for the Communications and Information Infrastructure. Government leadership is essential in initiating this infrastructure assurance effort and in motivating all infrastructure stakeholders for unified action.

Although many agencies are interested and working in infrastructure security, the efforts are piecemeal and need focus.

The National Security Telecommunications Advisory Committee (NSTAC) reports to the President, but through three separate offices, making it difficult to establish a strong leadership role; the National Security Council (NSC) and the National Security Agency (NSA) focus on national security concerns; the Defense Information Systems Agency (DISA), through its National Communications System (NCS), focuses on the important area of assuring communications services for the federal government, but not beyond that.

The National Reliability and Interoperability Council (NRIC) of the Federal Communication Commission (FCC) tracks failures in the telecommunications network, but has chosen not to extend its jurisdiction to the Internet and has not addressed critical issues arising from industry convergence and the entry of companies into nontraditional market sectors. The National Telecommunications and Information Administration (NTIA), within the Department of Commerce (DoC), has not adequately addressed security and reliability issues. More leadership and coordination among these organizations are necessary in addressing Communications and Information Infrastructure surety.

In February 1998, the DoJ and the FBI established a National Infrastructure Protection Center (NIPC), with support of the DoD. The NIPC will permit the DoD and DoJ to better coordinate their mutually supportive efforts to enhance the viability and security of the nation's critical infrastructures, including the Communications and Information Infrastructure. The NIPC will have ties to the Departments of State, Commerce, Treasury, Energy, and Transportation; the Federal Emergency Management Agency (FEMA); and the private sector. The NIPC's base in the intelligence and law enforcement agencies raises questions, however, as to its role and effectiveness in broader commercial and social infrastructure areas.

Not all communications and information industries are subject to federal regulation.

With the present trend toward ever-greater regulatory restructuring of communications, cable, and information services, current federal law does not provide seamless authority to departments and agencies to provide security and reliability in this infrastructure, and not all communications and information industries are presently subject to federal directives with respect to the security and reliability of the infrastructure.

State and local governments must also be active players.

States, counties and municipalities must become central players in promoting greater security and reliability in the Communications and Information Infrastructure. Through their national leadership organizations, such as the National Governors Association (NGA), the National League of Cities (NLC), and the National Association of Counties (NAC), they can and must take concerted, active steps toward achieving a more secure and reliable communications infrastructure.

Among the most difficult and most important challenges we face is that of building a partnership based on trust and mutual commitment between industry and government. This will take leadership, courage and determination on all sides, but without it, no significant progress will be made.

PRIORITY 2: OBTAINING ACCURATE, COMPLETE, AND TIMELY INFORMATION ON THREATS AND VULNERABILITIES, ON INTERNATIONAL INCIDENTS AND TRENDS, AND ON INDIVIDUALS, GROUPS AND NATIONS THAT POSE POTENTIAL THREATS TO THE US COMMUNICATIONS AND INFORMATION INFRASTRUCTURE

Companies are reluctant to report outages fearing it will harm sales.

Since the network outages of 1990 and 1991, the FCC has required telecommunications common carriers to report service interruptions affecting 30,000 or more customers and lasting 30 minutes or longer. The carriers are required to indicate the reasons for the interruption and what actions have been taken to correct it. However, communications and information service providers are characteristically reluctant to report problems originating from or affecting their facilities, operations or services, for fear that customers will desert them for one of their competitors.

Companies need to recognize the high cost of unsecure systems.

Privately, industry representatives acknowledge their reticence and admit that good reporting on such incidents would provide information that would help everyone. Until companies are confident that such disclosures will not harm them competitively, they are unlikely to risk the consequences of disclosure.[10] The success of any effort aimed at obtaining substantive information on threats and vulnerabilities will depend on whether or not corporations recognize that such reporting ultimately is in their best interest.[11] Some companies, however, are beginning to recognize the high costs of unsecure systems.[12]

The lack of reporting results in a weak database and insufficient information to develop policies and programs to adequately address surety of the Communications and Information Infrastructure, with negative repercussions for national security, economic security and the safety and welfare of the American people.

An inadequate database and insufficient research will hamper efforts to strengthen infrastructure security.

Besides the lack of information from industry, there is inadequate information on international incidents and trends and on individuals, groups and nations that pose potential threats to the US Communications and Information Infrastructure. Exacerbating this situation is a lack of empirical research on security and reliability issues and effective approaches to strengthen security and reliability of critical infrastructures, including communications and information.

Priority 3: Developing clear requirements for strengthening the security and reliability of the communications and information infrastructure for national defense purposes and for delivery of emergency services

The national defense community has been most outspoken over the past several years in acknowledging incidents of attack on systems critical to our nation's security and to the safety of service men and women, and in calling for action to address threats and vulnerabilities.[13]

The defense community has been the most active in addressing vulnerabilities.

In statements surrounding the formation of the NIPC in February and in comments on the series of attacks on the Pentagon, the national defense community has expressed its intentions to take actions to improve the security and reliability of critical communications and information systems.[14]

The need for a more secure and reliable communications system for EMS providers is widely recognized. Communications systems are critical to coordinating an effective response and recovery effort in crisis scenarios.

Emergency service providers at all levels have a critical need for secure and reliable communications.

Priority 4: Engaging industry, customers, universities, national laboratories and the American people in a commitment to improved infrastructure surety

With limited federal government leadership and involvement, companies manufacturing or supplying communications and information equipment, together with service providers, have made few noteworthy attempts to strengthen the security and reliability of the infrastructure. While customers and the public have generally been silent on the issue as well, experts on telecommunications and information technologies, computer networking, the Internet, and other areas have spoken out on the need for greater protection of the Communications and Information Infrastructure.

At present, industry and the public seem unconcerned about vulnerabilities in the Communications and Information Infrastructure.

There is need for widespread commitment from the private sector. At present, industry seems quite unconcerned with threats or vulnerabilities in the Communications Infrastructure – or in other critical infrastructures – and the implications of these threats and vulnerabilities for the US.

PRIORITY 5: RESEARCHING, DEVELOPING AND DEPLOYING ADVANCED COMMUNICATIONS AND INFORMATION TECHNOLOGIES AND SYSTEMS TO ADDRESS VULNERABILITIES ARISING FROM CONVERGING INDUSTRIES AND NEW CUSTOMER DEMANDS

New defenses must keep up with new threats.

Cyber vulnerabilities present new and formidable challenges to the security and reliability of the nation's Communications and Information Infrastructure; cyber technologies must be used to counter these vulnerabilities. Whether vulnerabilities result from accidents or deliberate actions in software code, or from viruses that corrupt or destroy essential system files, sophisticated algorithms can be used to detect a broad range of unauthorized and potentially damaging incursions and can shield systems or networks from them.[15] The advanced software for such sophisticated detection and tracking is generally well understood, and in some cases already deployed, but more extensive applications in all major systems of very critical importance will require intensive research and development because new attack modes are being developed daily.

Interruptions caused by traffic overload can start a continuing string of system derailments.

Severe traffic overloads can cause switching, signaling, routing and storage systems to become blocked and inoperable, sometimes systematically derailing a string of systems in the network. This concern is heightened when the processors and transmission lines handle extraordinarily large quantities of messages as a matter of course. Any interruption of such facilities causes far-reaching tremors throughout the system. This vulnerability is also exemplified in wireless services. It is well known that wireless connections are less secure than wireline services, with exposure to both accidental and deliberate eavesdropping. Digital wireless services are inherently more secure than analog from eavesdropping and other interruptions, but digital systems are not yet widely deployed, and they still have problems with fading, black-out areas, and disruptions that occur when traveling through tunnels, over bridges, near power lines, etc.

Industry generally regards standard-setting as its responsibility and resists government involvement.

US industry generally holds to the view that the standard-setting process is largely its responsibility and has resisted attempts by the federal government to take an active role in setting standards. Without active government participation in the process, however, companies with competing technologies may have little or no incentive to agree on a common standard, and there may be very real incentives not to do so. On the rather rare occasions when the federal government and industry have worked together in the standard-setting process, as happened with advanced television (ATV) several years ago, government can be an important catalyst in achieving agreement on a standard.

Encryption standards remain an especially troublesome issue. Encryption is essential to protect the privacy and security of both data and voice communications, especially where sensitive national defense, proprietary corporate transactions, and medical, legal or personal information is in question. Business, consumer and privacy representatives favor the strongest forms of encryption, while the FBI, the NSA, and other government agencies have advocated a system that would entrust an encryption key to federal law enforcement bodies. This would then allow select law enforcement agencies to tap into communications when authorized by federal courts for legitimate law enforcement purposes. There is strong opposition from the private sector to any such approach that would give government officials direct access to private communications. Furthermore, there is little acknowledgment by industry that government has a need to wiretap for legitimate law enforcement purposes.

There is especially strong opposition to the establishment of encryption standards.

Priority 6: Protect keystone targets from physical and cyber attack

A high concentration of critical communications and information traffic travels over limited transmission, switching, signaling, and routing systems, which may be vulnerable to physical and cyber attack and to interruption from natural causes and accidents. These systems may be described as "keystone" targets, because their functions and capabilities are interrelated with those of other facilities, so that damage to one results in damage to others as well. Examples of such facilities would be those serving critical federal government offices, including offices of the President, Vice President, senior Cabinet officers, including the Secretary of State, the Secretary of Defense, the Secretary of Energy, the Attorney General, offices of Congressional leaders and justices of the Supreme Court, the federal reserve system, and the New York Stock Exchange. These facilities, systems and networks must be made extraordinarily robust, must be concealed and safeguarded, and backed by 100% redundancy in a separate system at a distant location.

A successful attack on a keystone system would bring others down with it.

In some cases, an otherwise secure and reliable system operates interdependently through a switch, node or other unsecure facility. It is commonly acknowledged, for example, that the Internet backbone passes all traffic through a small handful of nodes, which, if damaged or infiltrated, would expose the Internet to serious and widespread disruption or even collapse. The ramifications of such an event would extend throughout all critical infrastructures.

Even systems that are otherwise secure and reliable can suffer from an attack on a critical node.

Denial-of-service shutdowns should be replaced with "safe-fail" systems.

Current communications systems are designed to handle excess traffic by closing down and diverting traffic to alternative points, which results in customers being shut out of the system until the problem is corrected. This is frequently described as the denial-of-service problem. What is required in place of this fail-safe approach is a "safe-fail" system, which responds to severe traffic overloads by slowing rather than cutting off the affected system or dispersing incoming traffic to several other systems rather than one, while the troubled system itself comes to a gradual halt or returns to normal operation. This approach already is employed in critical defense systems.

It is possible for a person or a small group to attack critical infrastructure nodes that could inflict serious, widespread damage without grave risk of being harmed or even being caught. Single-point-of-failure and high-impact facilities, such as major switching systems and centers, are particularly likely to be targeted for such attacks.

TECHNOLOGY AND POLICY OBJECTIVES

After assessing the range of vulnerabilities in the Communications and Information Infrastructure, we turn to a plan through which we can strengthen this base, which is fundamentally important to national defense and to our nation's other key infrastructures.

From a policy perspective, government leadership and direction are essential to achieve a secure, reliable infrastructure, but the primary role in this effort belongs to private industry. For a century and a half, private industry has designed, built, and maintained this infrastructure and provides an increasingly broad range of communications and information services. Under the leadership of the federal government, private industry must take responsibility for the security and reliability of this infrastructure.

Under government leadership, industry must take responsibility for the security and reliability of the infrastructure.

Dramatic technology advances have effected broad shifts in the structure of the communications and information industries, requiring approaches different from those that have worked in the past. Technology gives power to individuals and groups unlike any that they have previously known. Their objectives and aspirations may be different from those we are accustomed to, so we must be careful not to gauge vulnerabilities and threats within only traditionally defined parameters. Creating a long-term strategic roadmap for a secure and reliable Communications and Information Infrastructure must begin with a clear statement of desired objectives for policy, technology, and process.

As described in the last section, vulnerabilities and threats in the Communications and Information Infrastructure point out a number of high-priority needs and challenges, which are restated here as policy and technology objectives.

1. **DEVELOP EFFECTIVE FEDERAL, STATE, AND LOCAL GOVERNMENT LEADERSHIP AND CLEAR POLICY GUIDELINES.**
2. **DEVELOP SYSTEMS AND TECHNOLOGIES THAT WILL OBTAIN ACCURATE, COMPLETE AND TIMELY INFORMATION ON THREATS AND VULNERABILITIES.**
3. **DEVELOP CLEAR REQUIREMENTS FOR STRENGTHENING SECURITY AND RELIABILITY OF THE COMMUNICATIONS AND INFORMATION INFRASTRUCTURE FOR NATIONAL DEFENSE PURPOSES AND FOR DELIVERY OF EMERGENCY SERVICES.**
4. **ENGAGE INDUSTRY, CUSTOMERS, UNIVERSITIES, NATIONAL LABORATORIES, AND THE AMERICAN PEOPLE IN A COMMITMENT TO IMPROVED INFRASTRUCTURE SURETY.**
5. **RESEARCH, DEVELOP, AND DEPLOY ADVANCED COMMUNICATIONS AND INFORMATION TECHNOLOGIES AND SYSTEMS.**
6. **PROTECT KEYSTONE TARGETS FROM PHYSICAL AND CYBER ATTACK.**

TECHNOLOGY AND POLICY ROADMAPS

Requirements necessary to meet the objectives over the next 15 years are outlined in the following roadmaps.

OBJECTIVE 1: DEVELOP EFFECTIVE FEDERAL, STATE, AND LOCAL GOVERNMENT LEADERSHIP AND CLEAR POLICY GUIDELINES.

Roles and responsibilities must be clearly defined.

The first step toward the objectives must be to define a structure that will clarify roles, responsibilities, and relationships for federal agencies that support the Communications and Information Infrastructure. It is particularly important for all federal departments and agencies whose responsibilities require reliable communications and information services to actively participate in this effort. Through their procurement processes and their interactions with other organizations and the public, these agencies may be in a position to promote constructive dialog between suppliers and users of communications and information services, and even to encourage higher standards of security and reliability in commercial off-the-shelf (COTS) equipment, networks, systems, and related services.

Communications and information surety requirements for defense, emergency and other critical areas must be identified.

Equally important is the definition of communications and information surety (CIS) requirements (safety, security, and reliability) for national defense and national security, emergency services, and for each of the remaining critical infrastructure areas. From the beginning, but increasingly in the mid-term and long-term periods, it will be more and more necessary to emphasize common concerns and synergistic relationships among all critical infrastructures. According to Presidential Decision Directive 63, signed May 22, 1998, the DoC has the lead role in this regard, but other departments and agencies, such as the DoD, can have an important impact. The National Aeronautics and Space Administration (NASA), for example, relies on advanced, high-performance systems, as is the case with the National Institutes of Health (NIH), and other agencies. They are in an excellent position to promote enhanced security and reliability in all aspects of communications and information. Industry will then have a strong economic incentive to apply universally the same security and reliability requirements in equipment, products, software, systems, and services.

OBJECTIVE 1: Develop effective federal, state, and local government leadership and clear policy guidelines.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Define a structure to clarify federal agency roles	Active interest, participation by all federal agencies, organizations	No federal agency has sufficiently broad leadership responsibility	Participation of all agencies in defining requirements stated above	Mutual cooperation and support of all federal agencies	Full interagency cooperation and interaction, exchanges of personnel
CIS plan in place for all federal agencies and operations	Common CIS measures applied in all federal agencies	No common CIS requirements across agencies	CIS for national defense, EMS, and critical infrastructures	All federal agencies agree on comprehensive CIS plan	CIS plans and policies fully operational, regularly reviewed
Direct involvement of the President and Congress	President reaffirms commitment; Congress has hearings enacts legislation	Administration actions not definite; no wide or strong interest in Congress	Budget allocation for FY 1999 and subsequent years	Administration and Congress develop and implement cross-infrastructure plan	Annual assessments and necessary adjustments of goals
Cooperation of states, cities, local government	Federal, state, local governments agree on CIS policies, goals	Little coordination; some state/local government resentment	Advise and work with states, cities, local governments and their associations	States, cities, local governments actively engaged in the process	Widespread inter-government interaction and coordination

Strong support and commitment from the President and Congress will be needed to focus government funding and interest to adequately address the surety of the Communications and Information Infrastructure. In the intermediate period (3-6 years), a comprehensive long-term plan must be developed to strengthen and sustain security and reliability in the Communications and Information Infrastructure for the national defense, national security, and emergency services. The plan must explicitly recognize the interaction and interdependency of the Communications and Information Infrastructure with other infrastructures and should have as a goal the continuous improvement of the quality of life for all Americans. Assignment of responsibilities toward long-term goals will also include coordination of the federal government's role in infrastructure surety with state governments, cities and local governments.

Interrelationships of infrastructures must be recognized.

OBJECTIVE 2: DEVELOP SYSTEMS AND TECHNOLOGIES THAT WILL OBTAIN ACCURATE, COMPLETE AND TIMELY INFORMATION ON THREATS AND VULNERABILITIES.

Overcome reluctance of manufacturers and suppliers to report data.

An immediate priority is to put in place mechanisms to obtain accurate, complete, and timely information on present threats and vulnerabilities. A difficulty is that manufacturers, software developers, service providers, and customers are reluctant to acknowledge either threats to their systems or services or known vulnerabilities, for fear of their being perceived as having weaknesses that their competitors do not have. This is so even though companies and their customers are frequent targets of attack.

Protect the privacy of information providers.

To overcome this reluctance, all available existing information must be brought together to demonstrate to companies the enormous hidden costs they are paying because of threats and vulnerabilities. Available information should also be assembled to show companies the advantages they would gain from a more secure and reliable infrastructure. Tax credits and fast-track regulatory approval processes should be considered as additional incentives. Companies providing information should have confidence that their identity, privacy, and proprietary concerns will be protected.

Offer companies economic and regulatory incentives to provide information.

In the intermediate years, as a comprehensive technology roadmap is developed and put in place, processes should be refined to facilitate timely development and exchange of necessary data and the implementation of related policy and technology objectives. Legislation should be proposed to Congress offering economic and regulatory incentives for companies that provide information on any unauthorized damage, break-in, entry, use, interference, or alteration of equipment or systems, any other violations of security or reliability, and any such occurrence attributable to accident, obsolescence, failure, etc. Computer network operators, Internet service providers, private communications and data network operators must be encouraged to provide relevant information. Incentives could take the form of expedited consideration of applications for entry into new markets, tax credits, etc.

All information and data must be kept secure and private.

It is critical that industry and government form a common trust so that threat and vulnerability information can be shared and used to its full advantage in protecting and securing the infrastructure. Information received from companies must be kept secure and proprietary. This information must be analyzed and stored in a fully secured electronic database for exclusive use by the appropriate agencies. Information may be used to assist industries and companies in addressing security and reliability issues in the Communications and Information Infrastructure.

OBJECTIVE 2: Develop systems and technologies that will obtain accurate, complete and timely information on threats and vulnerabilities.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Companies must be convinced of the inherent advantages of providing information on threats/vulnerabilities	Detailed, accurate reporting of incidents and suspected threats and vulnerabilities on a timely basis	Companies are reluctant to report any problems, although this may be changing somewhat	Assemble all available information to show costs of vulnerabilities and advantages of more secure infrastructure	Outline plan for comprehensive reporting and immediate response to any attacks	Detailed and comprehensive reporting and response plan in place
Incentives to companies providing information on threats, vulnerabilities	Companies provide accurate, specific, timely data on threats, vulnerabilities	Only piecemeal information is provided	Enact tax credits and other incentives for companies providing information	Measure the effectiveness of incentives, focus on those which are most effective	Comprehensive plan in place to encourage full industry cooperation
Industry and government have accurate timely information on risks, effective CIS policies, technologies	Accurate up-to-date database on risks, CIS policies and technologies available	Only sparse anecdotal information is available	Define parameters of database, providers, government/private customer surged to provide data	Database is operational, provides solid information for added CIS measures	Continual refinement of database, broader input, better understanding of sound CIS measures
International intelligence assessment	Awareness of threats, risks, potential perpetrators	CIA, FBI obtain intelligence information	National intelligence center on cyber/physical threats	Build effective, timely response system	Refine and improve the intelligence-gathering process

In the long term, processes should be reviewed on a regular basis to assure that organizations are not encumbered by bureaucratic problems or otherwise rendered less effective in achieving stated goals.

Extend data acquisition to include international incidents.

The intimate links between the US Communications and Information Infrastructure and the rest of the world make it imperative that we adequately address international as well as domestic threats. A national indications and warning center with a full range of expert intelligence skills and related technologies could monitor both domestic and international threats to the US Communications and Information Infrastructure. This center could also gather information on incident trends and on individuals and groups that pose potential threats to the US Communications and Information Infrastructure.

OBJECTIVE 3: DEVELOP CLEAR REQUIREMENTS FOR STRENGTHENING THE SECURITY AND RELIABILITY OF THE COMMUNICATIONS AND INFORMATION INFRASTRUCTURE FOR NATIONAL DEFENSE PURPOSES AND FOR DELIVERY OF EMERGENCY SERVICES.

National security and reliability must have top priority.

CIS requirements for national defense, national security operations, and intelligence must be addressed as matters of top priority for federal security and reliability. Federal law enforcement and other essential federal government operations must also be addressed. The offices and agencies with these areas of responsibilities must also recognize those segments of the Communications and Information Infrastructure where security and reliability are of paramount importance, such as telecommunications.

Each of the major branches of military service is critical to this effort, because only they can specify the aspects of the Communications and Information Infrastructure that are most critical for their operations. They must also specify perceived threats and vulnerabilities to the infrastructure.

Emergency services of critical importance must also be included.

Emergency and other services are of critical importance to the nation and the American people, and their CIS requirements must be included as well. The vast amount of communications and information that these services rely on are vital in saving lives and preserving our public safety on a day-to-day basis.

All participants in the Communications and Information Infrastructure must therefore engage in a national effort to improve the security and reliability of this critical infrastructure for national defense, national security, emergency services, and the welfare of all Americans.

OBJECTIVE 3: Develop clear requirements for strengthening the security and reliability of the Communications and Information Infrastructure for national defense purposes and for delivery of emergency services.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Clear statement of essential CIS requirements for national defense and essential government services	Federal defense agencies agree on CIS requirements. Agencies set essential government services	Federal defense and other agencies have differing views and pursue separate paths	Defense, and other agencies develop near-, mid-, long-term telecom and infrastructure goals	Comprehensive surety requirements for key infrastructures and quality of life	Fully articulated long-term surety policies
Clear statement of emergency service CIS replacements	Federal, state and local governments agree on CIS requirements	Little agreement on emergency service requirements	Federal, state/local governments agree on emergency service requirements	Comprehensive CIS emergency service requirements in place	Increasing improvement of emergency service

OBJECTIVE 4: ENGAGE INDUSTRY, CUSTOMERS, UNIVERSITIES, NATIONAL LABORATORIES, AND THE AMERICAN PEOPLE IN A COMMITMENT TO IMPROVED INFRASTRUCTURE SURETY.

Providers of equipment and services, customers, and the public must work together to achieve greater security.

With the exception of some critical national defense systems, private industry owns and operates all major segments of the Communications and Information Infrastructure. Providers of equipment and services, customers, and the public must therefore actively work together to achieve greater security and reliability in the infrastructure.

In achieving this cooperation, it would be beneficial to form an independent providers and customers reliability panel with representatives from all major communications and information industries and customers. This panel would provide private sector support for security and reliability goals and objectives.

Universities and national labs can play a vital role in developing safeguards.

Universities, national laboratories, and other major research institutions have important resources for building the knowledge base required to define intermediate and long-term goals. The resources include skills, technologies, and systems integration capabilities in security and reliability. These institutions can also assist in weighing capabilities and needs, as represented by providers and customers, and in gauging their value for achieving the desired objectives.

Incentives can be offered to customers who purchase secure systems and services.

The American people must be informed and alerted to the dangers posed by present threats and vulnerabilities. Widespread public awareness and participation will make a significant difference in obtaining government and industry's commitment and resources to bolster infrastructure surety. Incentives could be considered for customers who purchase more secure and reliable systems and services.

OBJECTIVE 4: Engage industry, customers, universities, national laboratories, and the American people in a commitment to improved infrastructure surety.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Establish a providers and customers reliability panel	Active participation of representatives from all major industry vulnerabilities	Major industries lack attention to Communications and Information Infrastructure vulnerabilities	Panel commits to immediate goals in Communications and Information surety roadmap, and begins implementation	Panel supports R&D, databases, implementing roadmap in key Communications and Information Infrastructure	Industry fully engaged with government, national laboratories, and others in coordinated effort in all infrastructures
Long-term plan by providers and customers to strengthen security and reliability of Communications and Information Infrastructure	Federal agencies, communications and information providers and others follow long-term plan	Long-term planning is done only by defense community, some communications and information providers	Define long-term plan and near-term tactics	Develop and coordinate goals, measurements, etc.	Comprehensive plan in place, regularly reviewed and updated
Informed and committed national organizations with input from providers and customers	Leading organizations support long-term plan	Little knowledge of issues or concern by leading groups	Promote public forums on security, reliability of infrastructure	Industry assigns, academia and research groups to support long-term plan	Industry assigns, others play active role in plan for security/reliability of Communications and Information Infrastructure
Incentives for users purchasing secure/ reliable systems and services	Customers demand more secure and reliable products, systems, software and services	Customers accept providers assurances on security and reliability	Agreement on desired CIS requirements in place, incentives in effect	Wide publicity on benefits of security to customers, including economic and insurance benefits	Ongoing public relations campaign to gain customers and public support for strong CIS

OBJECTIVE 5: RESEARCH, DEVELOP AND DEPLOY ADVANCED COMMUNICATIONS AND INFORMATION TECHNOLOGIES AND SYSTEMS.

Establish a government and industry standards advisory group.

Immediate technology objectives for Communications and Information Infrastructure security and reliability include establishing a government/industry standards and technology advisory group. This group is needed to facilitate progress toward standards, including encryption standards, which will improve security and reliability in critical areas of the Communications and Information Infrastructure. The standards advisory body should include government representatives from the NCS, NIST, and the FCC; industry members should include representatives from NSTAC telecommunications, broadcast radio and television, cable television, computer manufacturers, software developers, computer and data networking, and Internet equipment suppliers and service providers. Specific resources and capabilities in security and reliability available at major universities, research institutions, and at national laboratories must also be recognized and cultivated.

Address the increasingly more complex interdependence of all infrastructures.

The specific actions recommended here are initial elements of a long-term strategic roadmap that defines policy, technology, and process considerations needed to guarantee long-term security and reliability of the Communications and Information Infrastructure. In addition, a comprehensive technology roadmap must be jointly developed by industry and government. This roadmap should address specific milestones, research, funding, and proposed participants from government and industry. The roadmap must address the complexities introduced by increasing interdependencies among the various infrastructures. More details, specific goals, and specific measurements for near-term, intermediate, and long-term horizons should be integral parts of a comprehensive technology roadmap.

OBJECTIVE 5: Research, develop, and deploy advanced communications and information technologies and systems.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Create a government/ industry standards and technology advisory group	Agreement on approach for timely introduction of standards	Long delays in adopting standards, standoff on encryption	Create effective principles/procedures, move on overdue issues	Expedite consideration of outstanding high-priority standards	Consensus on standards-setting in government and industry
Comprehensive technology roadmap for security of critical infrastructures	Federal agencies, Communications and Information industries, others follow technology roadmap	Recognition that a roadmap may help on long-term security and reliability goals	Government and industry initiate technology roadmap and engage needed research	Roadmap done, R&D of technologies with security, reliability applications	Government and industry function in complementary, coordinated roles
Safe-fail technologies to continue service through high demand periods	Switching, signaling, systems continue service, close gracefully	Systems hit with bursts of traffic close down, shift traffic to another system	Research and develop technologies for safe-fail	Test and introduce modifications as they are developed	Refine and further deploy technology

Take measures to avoid domino-effect failures.

An initial technical element that must be addressed is the problem introduced by some existing fail-safe equipment. Major switching systems, routers, and protocols typically are designed with fail-safe programming, each identical to other systems of the same type, to shift excess traffic to associated facilities. In the event of a major surge in traffic, this system design feature can cause a domino shutdown effect throughout the network. The problem is said by experts to characterize major signaling and switching systems, including the widely used Signaling System 7, the industry's leading Class 5 switching system—the #5ESS, the synchronous optical network (SONET), and Internet routers. Systems experts contend that altering the design from one system to another would invite greater security and reliability risks because of the difficulty and cost involved in training experts to maintain and repair distinct systems.

OBJECTIVE 6: PROTECT KEYSTONE TARGETS FROM PHYSICAL AND CYBER ATTACK.

Near real-time information about the state of the infrastructure on a national level will minimize or prevent disruptions.

An extremely important goal is the identification and protection of critical and vulnerable nodes. However, a vulnerable node is not necessarily critical. For instance, a vulnerable node may be backed up through sufficient redundancy or system flexibility. The key attributes sought here are criticality and vulnerability.

Of particular concern are high-impact transmission lines and switching systems that can be disrupted by hurricanes, earthquakes, floods and storms, augers and backhoes, or those that can be located and attacked by bombs or other means. Major switching systems and routers can be disrupted by sabotage to hardware or software, or fail because of electric power loss, sporadic bursts of traffic or heavy traffic demands.

To better protect critical nodes in the Communications and Information Infrastructure and to minimize the quantity and size of disruptions, it is necessary to have near real-time information about the state of the infrastructure on a national level. This would aid early identification of coordinated attacks and help to detect events that could lead to large-scale disruptions. Such a national indications and warning system could also be used to correlate system failures with problems in specific equipment, software, or training. Considerable coordination and trust between government and industry are needed for this much-needed system to be successful.

OBJECTIVE 6: Protect keystone targets from physical and cyber attack.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Identification of critical nodes	Facilities are uniformly defined and identified	Incomplete information on vulnerable high-impact facilities	Identify high-impact points for defense, essential federal government operations and emergency services	Identify high-impact facilities for all critical infrastructures	Comprehensive traffic engineering to reduce vulnerabilities
Rugged protection of high-impact facilities, and remote back-up facilities	Facilities are fully protected and remote back-up facilities are in place	Incomplete information on vulnerable high-impact facilities	Secure telecom facilities to support defense, essential federal government operations and emergency services	Install remote back-up for high-impact facilities for defense and federal government critical infrastructures	Disperse traffic from high-impact facilities and build remote redundancies throughout the Communications Information Infrastructure
Development of a national indications and warning system for the Communications and Information Infrastructure	No intrusions or major disruptions in the Communications and Information Infrastructure	Harmful codes cause major service disruptions, instances of unauthorized entry and tampering	System for early detection and prevention of possible large-scale disruptions. Early detection of unauthorized intrusion attempts to critical defense and emergency services systems	System to detect all unauthorized entry attempts into communications information systems for all critical infrastructures	System to prevent all unauthorized entry attempts into communications information systems for all critical infrastructures

TECHNOLOGY AND POLICY DRIVERS

Technology and policy drivers are key factors to the success of roadmap objectives.

Implementation of this roadmap requires us to identify the essential technology and policy drivers for success – the forces and events that are so fundamental that without them the effort cannot succeed. The following technology and policy drivers are key factors for the success of the objectives defined in this roadmap.

- Federal government leadership, especially leadership representing national defense, emergency services, and national security interests.

  The security and reliability of the US Communications and Information Infrastructure affect our nation at every level, from national defense, to the economy, to the conduct of our lives. Although the infrastructure was built and is managed by the private sector, its use for national security is ultimately the responsibility of the federal government. As the infrastructure has changed dramatically over the past quarter-century, federal leadership to assure its security and reliability has not kept pace. Reestablishing that leadership role is critical.

- Commitment of industry providers, equipment manufacturers and suppliers, software developers, and customers.

  The Communications and Information Infrastructure — diverse, ubiquitous, technologically sophisticated – belongs to industry. Companies in every part of the many industries involved, from those engaged in researching and developing new technologies, to software developers, equipment manufacturers and suppliers, and customers, all have important roles to play if the infrastructure is to be made secure. The task is huge and requires responsible commitment by all parties.

- Accurate, up-to-date information on threats and vulnerabilities.

  Threats and vulnerabilities cannot be effectively and satisfactorily addressed until better information is available. Today we are working with piecemeal and anecdotal data, which provide valuable knowledge and insights into the dangers to the infrastructure, but which are not accurate, complete, or timely enough to provide a sufficient base for a comprehensive, long-term surety plan.

- Engagement of state and local governments, other critical infrastructure industries and their customers, universities, national laboratories and research institutions, leading business and private organizations, and the American people.

  The roadmap outlined here contemplates a task that will require consensus and commitment at all levels of government; among industries in this infrastructure and all other critical infrastructures that depend on communications and information, and their customers; participation and cooperation of national institutions and organizations; and the strong backing of the American people.

OPPORTUNITIES AND SHOWSTOPPERS

OPPORTUNITIES

- The principal opportunity to make significant, long-term, strategic progress toward a more secure and reliable Communications and Information Infrastructure is represented by the work and recommendations of the PCCIP and the processes beginning to unfold to move the recommendations to implementation.

  It is especially opportune that the DoD and DoJ have moved forward expeditiously to establish the NIPC to better coordinate their efforts to promote more secure and reliable infrastructures, including the Communications and Information Infrastructure. The NIPC will have ties to other key departments and agencies and to the private sector. This quick action by these two departments, which are so crucial to the overall effort, presents an extraordinary opportunity for creating more effective federal government leadership.

- Another important opportunity is represented by the fact that the present administration seems willing to address the issue of infrastructure threats and vulnerabilities, as are a number of members of Congress, DoD, and the FCC.

  Statements by responsible federal officials since release of the PCCIP report in October 1997, indicate greater awareness of the reliability issue and determination to take action. Deputy Defense Secretary John Hamre, for example, said recently that attacks on Pentagon computers had "...dramatically accelerated the Pentagon's and the federal government's plans to get on top of this problem".[16]

- A further opportunity is presented by passage of The Telecommunications Act of 1996, rapid growth of wireless services, rapid expansion of the Internet, and by the FCC's present revisions of the NRIC charter.

  The communications industry is still very much in transition, with regulatory rules still not firmly in place. This situation affords the FCC and other federal agencies the opportunity to place the security and reliability of the infrastructure as a high priority, and to develop long-term plans and objectives with respect to information on outages and service denials and interconnectivity and interoperability standards, and to formulate specific timelines and measurements toward these and other objectives. The FCC also may choose this opportunity to formulate procedures for coordinating NRIC and other FCC objectives and activities with those of the IPC and other agencies.

SHOWSTOPPERS

Two developments could seriously impede progress toward a more secure and reliable Communications and Information Infrastructure.

- If the federal departments and agencies with responsibility in this matter fail to come together in a concerted effort to address this issue, the effort could be sidetracked into piecemeal actions that are simply insufficient to meet the long-term problem.
- Similarly, if industry and customers choose not to become actively involved and determined to improve the security and reliability of the infrastructure, government initiative alone will not suffice.

NOTES

1 Estimates made at Bell Laboratories using documented, but unpublished, research in 1997.

2 Alan Pearce, Ph.D. Article on Internet growth prepared for publication in America's Network, March 1998.

3 The New York Times, Feb. 28, 1998, p. A6.

4 Cfr. Robin Gaster, "Network Security in the Information Age." Unpublished manuscript. February 1998, p. 3.

5 United States General Accounting Office, Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84. May, 1996. p. 2.

6 Stephen J. Downs and Stephen Gould, "Telecommunications Networks and Signaling System 7," CRS Report for Congress. March 9, 1992, p. 1.

7 Downs, op. cit., pp 2ff.

8 Peter J. Denning, Computers Under Attack: Intruders, Worms and Viruses. Addison-Wesley, 1990.

9 Cfr. "Outlaws on the Loose," Network World, February 19, 1998.

10 Cfr. Peter H. Lewis, "Threat to Corporate Computers Is Often the Enemy Within," The New York Times, March 2, 1998, p. D1f. "'Most firms would rather go public with the news that their chief executive officer was an active alcoholic than the news that there was an insider security problem,' said William J. Malik, a vice president and research director for the Gartner Group," p. D6.

11 US corporations sustain damages in excess of $10 billion annually because of cyber attacks, according to an ABC Television News report, February 28, 1998.

12 Cfr. Lewis, op.cit., "While incidents of both internal and external computer crimes are on the rise, some see a positive sign in the fact that more cases of computer attacks are being reported. 'The growing acceptance that there is a widespread problem has probably led other people to go ahead and report incidents,' Mr. Power of the Computer Security Institute said." P. D6.

13 Cfr. United States General Accounting Office, op.cit. Cfr. also John Deutch, Director, Central Intelligence Agency, Foreign Information Warfare Programs and Capabilities. Statement for the Record. United States Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs. June 25, 1996, pp. 2-4, ff.

14 Cfr, e.g., statements of Deputy Defense Secretary John Hamre in "FBI, Pentagon Probing Military Computer Break-In," Reuters, February 26, 1998.

15 Cfr. National Science and Technology Council, Committee on Computing, Information, and Communications, Technologies for the 21st Century, esp. chapter on "High Confidence Systems." Supplement to the President's FY 1998 Budget, p. 22.

16 Reuters, op.cit.

SOURCES

"Australian Experts Warn of Computer Terror Threat," *Reuters*. February 17, 1998.

Timothy D. Casey. "A New Threat to Privacy," *Interactive Week*. February 2, 1998.

William R. Cheswick. and Steven M. Bellovin. Firewalls and Internet Security. New York: Addison-Wesley, 1994.

"Computer Hacker Shuts Down Tallahassee, Fla., Internet Provider," *Tallahassee Democrat*. January 20, 1998.

"Ex-Employee Nabbed in $10M Hack Attack," *ComputerWorld*. February 24, 1998.

"FBI, Pentagon Probing Military Computer Break-In," *Reuters*. February 26, 1998.

Federal Communications Commission. *Final Report of the Network Reliability and Interoperability Council*. July 15, 1997.

Marie L.Garcia. and Olin H. Bray. *Fundamentals of Technology Roadmapping*. Sandia National Laboratories. April 1997.

Robin Gaster. "Network Security in the Information Age," Unpublished manuscript. February 1998.

"Internet Security Holes Widen," *ComputerWorld*. March 3, 1998.

"Internet Sites Leave UK PLC Critically Exposed to Security Breaches, New Survey Reveals," *M2 PRESSWIRE*. February 27, 1998.

Ivan P. Kaminow. and Jane Bortnick Griffith. "Internet Technology," *CRS Report for Congress*. April 22, 1997.

"Keeping Mobile Users Secure," *PC Week*. February 11, 1998.

Peter H.Lewis. "Threat to Corporate Computers Is Often the Enemy Within," *The New York Times*. March 2, 1998, p. D1.

Steven W. Lodin. and Christoph L. Schuba. "Firewalls Fend Off Invasions from the Net," *IEEE Spectrum*. February 1998.

John Markoff. "Clinton Continues to Stumble Over the 'E' Word (Encryption)," *The New York Times*. February 27, 1998, p. C1.

National Cable Television Association. *Cable Television Developments*. Fall 1997.

SOURCES (continued)

National Science and Technology Council, Committee on Computing, Information and Communications. *Computing, Information, and Communications Technologies for the 21st Century.* Supplement to the President's FY 1998 Budget.

National Governors Association. *Terrorism: Is America Prepared?* February 1997.

"OCC to Heighten Tech Management Scrutiny," *American Banker.* February 9, 1998.

"Outlaws on the Loose," *Network World.* February 19, 1998.

"Pentagon Focusing on Cyber Threats, Boosts Funding," *Phillips Publishing.* February 3, 1998.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* October 1997.

"Protection of Information Systems Is Too Lax Too Often," *American Banker.* February 12, 1998.

"Reno Unveils Cyberattack Center as Feds Hit Hackers," *Newsbytes.* March 3, 1998.

Michael J.Riesenman. (ed.) "Communications," *IEEE Spectrum.* January 1998.

"Russia 'Hacker' Pleads Guilty to Breaking Citibank Network," *Itar - Tass.* January 26, 1998.

Sandia National Laboratories with Prosperity Institute. *US Infrastructure Assurance Prosperity Games Final Report.* June 1997.

"Securing Servers Means Using an Array of Tools," *Internet Week.* February 26, 1998.

"Security Leak Compromises Data on 90,000 People in Japan," *Newsbytes.* January 29, 1998.

Marcia S. Smith. "Encryption Technology: Congressional Issues," *CRS Issue Brief.* December 4, 1997.

"Telecom Carriers Arm Themselves to Fight Fraud," *Internet Week.* February 4, 1998.

US Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs. *Transcript of hearing on Security in Cyberspace.* June 5, 1996.

US Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs. *Transcript of hearing on Security in Cyberspace.* June 25, 1996.

United States General Accounting Office. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks.* May 1996.

glossary & acronyms

ATC	Air Traffic Control
ATV	Advanced Television
CIA	Central Intelligence Agency
CIS	Communications and Information Surety
COTS	Commercial off-the-shelf
DISA	Defense Information Systems Agency
DoC	Department of Commerce
DOE	Department of Energy
DoJ	Department of Justice
EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
NAC	National Association of Counties
NASA	National Aeronautics and Space Administration
NCS	National Communications System
NGA	National Governors Association
NIH	National Institutes of Health
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NLC	National League of Cities
NRIC	National Reliability and Interoperability Council
NSA	National Security Agency
NSC	National Security Council
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
PCCIP	President's Commission on Critical Infrastructure Protection
PCRP	Providers and Customers Reliability Panel
PDD-63	Presidential Decision Directive 63
PTN	Public Telecommunications Network
STP	Signal Transfer Point

participants

CHAMPION

Richard Thayer, Ph.D.
President
TTI - Telecommunications & Technologies International, Inc.
www.ttinetwork.com

PARTICIPANTS

The Champion wishes to express his thanks to all of those, named and unnamed, who have helped in preparing this roadmap. The list of participants and contributors which follows implies no agreement on the part of any one of the persons named or others with the views presented here.

Robin Gaster
President
North Atlantic Research

Frederic Leykam
President
The Washington Institute

Alan Pearce, Ph.D.
President
Information Age Economics, Inc.

CONTRIBUTORS:

The following list is not complete because some individuals with federal government agencies asked not to be identified to prevent any misconception that their views might represent official or unofficial positions of the agencies they represent.

John D. Abel
President/CEO
Datacast

Richard Albright, Ph.D.
Head, Technology Strategy and Assessment Dept.
Bell Laboratories

Don Baker, Esq.
Former Assistant Attorney General
Antitrust Division, DoJ

D. Elliott Bell, Ph.D.

Stephen R. Bell, Esq.
Willkie, Farr & Gallagher.

Robert Blau
Vice President
BellSouth Corporation

Gregory E. Blonder
AT&T Research

C. David Broecker
Marketing Vice President
NEC America, Inc.

Philip C. Cashia
Associate Director
Center for Telecommunications Management
University of Southern California

Michael G. Clinton
AT&T Division Manager
Retired

Joseph F. Coates
Coates & Jarratt

Donald P. D'Amato, Ph.D.

Irwin Dorros
Executive Vice President
Bell Communications Research
Retired

participants

Richard V. Ducey, Ph.D.
Senior Vice President
National Association of Broadcasters

Don Dulchinos
Director
Cable Labs

William Ashley Evans
Captain, USN

Marie L. Garcia
Strategic Business Development Consultant
Sandia National Laboratories

Rick Kemper
Director for Secure Systems
Cellular Telecommunications Industry Association

Kenneth Looloian
Executive Vice President
DiGiorgio Corporation

Henry L. Marchese
HLM Consulting

Eugene E. McNany
Bell Communications Research
Retired

Nicholas P. Miller, Esq.
Nicholas & Van Eaton, P.L.L.C.

Michael R. Nelson, Ph.D.
Director, Technology Policy
Federal Communications Commission

David L. Nicoll, Esq.
Associate General Counsel
National Cable Television Association.

Richard M. Nunno
Analyst in Science and Technology
Congressional Research Service
Library of Congress

Marcia S. Smith
Specialist in Aerospace & Telecommunications Policy
Congressional Research Service
Library of Congress

Rick Talbot
Director
Ciena Corporation

Richard Van Atta
Assistant Director
Science and Technology Division
Institute for Defense Analyses

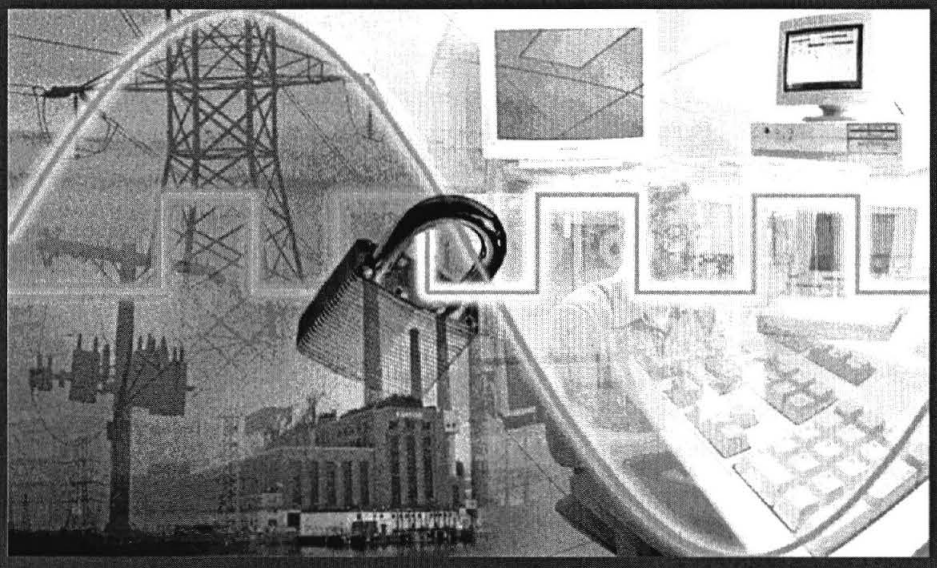
Philip L. Verveer, Esq.
Willkie, Farr & Gallagher

Daniel T. Woolley
Leader
Information Security Services
Ernst & Young, LLP

Nancy Saiz
Saiz Design

US Electric Power Infrastructure Strategic Roadmap

Electricity is the lifeblood of a modern nation; it materially enables our economy and directly impacts our overall quality of life. Moreover, the Electric Power Infrastructure shares multiple interdependencies with other infrastructures, making it a critical component in our national security. The major changes currently taking place in the electric power market and in technology present us with additional challenges. These challenges will be continually complicated by the forces of nature and the need to counter threats posed by various malicious elements, both foreign and domestic. Therefore, the goal of this roadmap is to identify technology and policy objectives to continue and to improve the availability, surety, and quality of the nation's electrical power supply both in the near and far terms.



DESCRIPTION

This roadmap focuses on what must be done to guarantee the surety of our Electric Power Infrastructure.

As a society, we have become so dependent on the reliability of the US electrical power system that even short and infrequent widespread interruptions cause great loss of public confidence and productivity. As a regulated rate-of-return industry, there is a long history of cooperation to develop and manage the nation's electric supply as a ubiquitous resource with high margins of safety and reliability.

The changes taking place in the industry will disturb the traditional modes of operation. The most significant change is industry-restructuring and the introduction of competition into the market, which will have both positive and negative effects on nearly every aspect of providing and managing the infrastructure. This roadmap is focused on what must be done to guarantee the surety of the Electric Power Infrastructure needed by the nation in the next millennium.

ELEMENTS OF THE ELECTRIC POWER INFRASTRUCTURE

The Electric Power Infrastructure includes all elements involved in the generation and delivery (transmission and distribution) and in its overall management. The network of sensors and control mechanisms that supports these functions is also included and is necessary for the infrastructure to operate safely and reliably as an integrated whole. Privately owned systems used for providing self-sufficiency or back-up, while sometimes important, are not considered in this roadmap.

GLOBAL VISION 2020

The utility industry's vision of the future is to provide a higher quality of life for all.

The utility industry vision is summarized in the Electric Power Research Institute (EPRI) background report entitled *A Preliminary Vision of Opportunities*,[1] which states, "Our vision of 2020 is a world with a higher quality of life for all with improved health, longevity, public safety, and national security. This future will be based on a broad range of innovations now within reach through electricity and its many uses." This is a vision based on the expectations of broader markets, greater competitiveness, and more high-value jobs through a responsive and reliable electricity infrastructure. By the year 2020, major progress can be made towards sustainable global development with cleaner air and water and a safe and stable biosphere.

RELIABILITY

The electric power industry is seeking a higher level of reliability despite increased vulnerabilities.

The electric power industry has been successful in developing and adopting reliability standards largely because of efforts made by the North American Electric Reliability Council (NERC). NERC was formed in 1968 as a collaborative effort by the utility companies to adopt voluntary standards that are now uniformly adhered to throughout the US.

The industry performs planning and operational studies on a continuing basis to assess electrical system reliability and to predict the potential impacts of certain events. Overall management of the power system involves regional planning, engineering, and operations in time frames ranging from decades to milliseconds. These efforts are coordinated by the electric power industry on a regional and national basis, working through NERC and its regional reliability councils.

When failures occur in the bulk power components (large generators, main transmission lines, high-voltage transformers), the impacts can be dramatic. Most of the service interruptions that customers experience are, however, short lived and occur locally.

> The key challenge will be to maintain reliability in a new competitive framework and under likely threats that involve multiple, distributed, and simultaneous or cascading incidents, both accidental and deliberate.

SCALE AND COMPLEXITY

Complexity will grow by several orders of magnitude.

The US electric power system is one of the largest and most complex structures of the current technological age. Furthermore, its management complexity may be increased by several orders of magnitude as the infrastructure continues to grow and as regulatory restructuring is implemented. This expansion would involve a large increase in the communication and control and status networks, thus adding complexity and posing additional risk to the infrastructure. Models and tools are needed to deal with system complexity because unaided, operations staff could not respond quickly enough to detect and correct problems. The large-scale and real-time distributed control requirements of the power system will continue to challenge the state of the art in distributed system management.

The Electric Power Infrastructure makes extensive use of information technology and has to accommodate the same risks as other information-intensive industries. Therefore, the complexity of the power system is compounded by the information technologies required to meet its unique needs.

DEMAND FOR TOUGH STANDARDS

Standards that served well in the past need to be assessed for their suitability for the future.

Operating standards used by the industry are either voluntarily developed by the NERC or imposed by regulating bodies such as the Nuclear Regulatory Commission and local public utility commissions (PUCs). Some of these standards apply to the direct control of the power systems while others are planning related. These standards have served the industry well in the past, but now it may be appropriate that those that impact systems control and the handling of sensitive information be reviewed to determine if they need to be revised or mandated.

Power continuity and quality are required by the computing systems that underpin much of our national defense and our efficiency and effectiveness as a nation. Yet the future reliability of the power system is unpredictable in the face of mounting competitive economic pressures and expansion in scale, complexity, and dependencies on information. Furthermore, future market conditions and new market participants create the need for higher standards to protect power system data and networks against various forms of misuse for financial gain, competitive advantage, extortion, and sabotage.

INCREASED THREATS AND VULNERABILITY

The infrastructure is vulnerable to both natural events and intentional acts of sabotage.

The nature of electric power systems requires that assets used to transmit and distribute power are dispersed over large geographic areas, making them vulnerable to both natural events and intentional attack. The industry understands and has experience with designing for and repairing physical damage to these types of assets.

Intentional coordinated acts against physical assets to disrupt power systems would be attractive to terrorists. The terrorist threat, however, has always been difficult to mitigate because of exposures in both rural and urban settings. Natural and man-made threats are realistic to consider, and exposure to them may be reduced but cannot be completely eliminated in a cost-effective manner.

Systems heavily dependent on communication and information networks are especially vulnerable.

In addition to overt physical disruption, open market forces and some technology trends are making the power system more dependent on information systems and supporting communications networks. Information integrity is critical to assuring sound economic and operational decisions, in addition to providing reliable planning data.

The advent of real-time power dispatching over the last 20 years has provided the industry with considerable knowledge of systems operation. Looking ahead, the expected competition in retail power markets may stimulate innovation in management techniques; however, other challenges of operating in a restructured environment might serve to put great pressure on the reserve margins currently

maintained by electric utilities. The desire to operate closer to these limits requires a more accurate and timely understanding of what the limits are, where one is operating, and how contingencies might take effect. Such assessments depend upon reliable real-time data on conditions over a wide geographic area coupled with real-time decision support tools.

As industry restructuring continues, more points of entry into command and control systems could become accessible to legitimate users and, unless adequate measures are taken, to potentially hostile individuals or organizations. For example, there needs to be assurance that each entity providing access to systems information provides for the protection of its interconnected partners and its own systems.

Flawed software or operating systems are an easily exploitable weakness.

For economic reasons utility computer systems are being moved from proprietary to more commonly used operating systems whose weaknesses are widely known. There is also the general problem of software quality because first-to-market advantages are stronger than bug-free or robust products. Because of design and implementation flaws, software systems are rarely free from defects that may be exploitable security weaknesses.

A relatively new development that has raised serious security concerns is the use of mobile code programs that transfer data from one processor to another over a network. Users may not know that this is happening, so an attack (which may be mounted against large numbers of systems at once) may not be recognized at the time it takes place. Robust operating systems required to counter such threats are still at the research stage.

Once inside a system, manipulation of data becomes easier, so overall vulnerability to attack increases. This problem could be exacerbated with the increased network sharing of transmission system availability data (e.g., the Internet-based Open Access Same-Time Information System, or OASIS) and operational control data for regional and interregional power flow.

Both cyber and physical attacks need to be considered.

Intrusion into information systems could have overt and covert effects. An information-based attack by terrorists or hostile powers, and the loss of information systems integrity from any number of possible threats, might cause widespread outages and be less risky than attempting physical attacks on the power infrastructure. It is feasible that blackouts, such as that which affected New York City in 1977, could be caused today through cyber attack. More subtle intrusions in the form of fraud and industrial espionage could be aimed at financial gain or, as a recent panel participant said, "We fail to take into account such consequences of events such as public panic and decline of public confidence".[2]

PROTECTION OF CRITICAL DATA SYSTEMS

Secured access to infrastructure information is critical to ensuring the integrity of operations and management.

The continuing increase in computer use for power system management means that protecting these computer systems from terrorist acts, and from other common risks to information systems, is particularly critical. The protection of information in this context means securing access to and ensuring integrity of the data and information used in the Electric Power Infrastructure's operation, maintenance, and overall management. This category of exposure is different from natural or system induced events because it entails a premeditated assault on specific, and possibly the most vulnerable, points of the system.

Security measures are not currently mandated by law.

PUCs normally allow utilities to cover security costs of providing physical security including measures such as fences, guards, and spare components. It is possible that commissions may not recognize the need for additional security. Reliability and liability are linked to regulatory policy and have not been set by law. Federal emergency preparedness and guidelines would make this more likely.

To protect information, it is important to understand where and how this information is used, the threats and vulnerabilities associated with its use, and to appropriately provide for the reliable operation of networks and computers that transport and process it. For example, control center computers may need special precautions such as a power source that is independent of the grid.

Information will become more of a target for criminal elements and the insider threat.

In addition, as information becomes more directly related to the economic performance and success of industry participants, it will become more of a target for criminal elements. In contrast to terrorist acts that are aimed at disruption to make a political statement, financial gain or revenge motivates criminals and disgruntled employees. In either case, the integrity of the power system can be undermined.

Many strategic decisions are tied to instantaneous access to confidential or critical data.

Confidentiality and appropriate use of information by authorized users is critical to retaining the confidence of individual consumers. Strategic business decisions, tactical operational decisions, and near instantaneous electronic trading decisions are all dependent on timely access to confidential information. Thus, to function efficiently, the energy market stakeholders will require utmost confidence in the transactions and integrity of information flows that are directly related to power trading. Today very little use of cryptography is made by the utilities to protect their information assets, but this is likely to change.

> It is the mutual dependence of electric power on computing systems and computers on electric power that lies at the heart of many of the major concerns addressed in this roadmap.

CROSS-INDUSTRY COLLABORATION

The emerging internal needs and challenges facing the utility industry make participants dependent on shared information and on each other's actions. However, future collaboration within the utility industry will be tempered by the competitive nature of the business environment, and there are antitrust issues to be considered. In some instances, competition can undermine overall reliability, which can only be achieved by considering integrated system performance, from generation in one region to retail customer delivery in another.

Even as the electric industry becomes more competitive, power reliability will require more cooperation among utilities.

Although traditional information sharing arrangements to deal with threats posed by weather, earthquakes, system stress, or single component failure will continue to be important, the safe and efficient operation of the Electric Power Infrastructure is also dependent on other infrastructures, namely, telecommunications, transportation, oil and gas, financial, and emergency services. For example, the telecommunications required to support power control and to provide essential means of communication is becoming increasingly important and is itself vulnerable to attack. Approximately a third of control traffic is carried on or though the Public Switched Network.[3]

The electric utility infrastructure is dependent on other highly complex systems.

To paraphrase Peter Neumann of the Stanford Research Institute, to a first approximation, every utility computer will be connected to every other computer. If in the future we reach a point where information management is dependent on the Internet, then bringing down the Internet could greatly impact the power grid. A move toward this power trading process is already taking place through implementation of OASIS.

All stakeholders share a common interest in deterrence, intrusion detection, security counter-measures, graceful degradation, and emergency back-up and recovery. In the future, it is likely that the electric power industry, as well as other related critical infrastructures, will benefit from government issued indications and warnings about impending events.

The Electric Power Infrastructure will benefit from an indications and warnings system.

> A major challenge is planning and executing information sharing arrangements and near real-time threat and intrusion alerts to assist in prevention and recovery from events that could present an unacceptable risk.

PLANNING FOR THE FUTURE

Transition to the future of market-based electricity requires a continued appraisal of the roles of the public and private sectors. The private interests of legitimate market participants will result in market mechanisms that provide economic levels of security against loss of revenue or confidence. For example, there are reliability criteria established by NERC and further reinforced by regional councils, such as the Western Systems Coordinating Council, that deal with high-consequence events.

Market forces will provide economic levels of security against losses.

Where the market cannot provide adequate protection, the government must provide support.

There are, nevertheless, situations where economic security may be insufficient for national security and the public good. A distributed and coordinated attack on utility physical or information systems is an example of a low-probability, high-consequence event. Where the market does not adequately plan for such contingencies, the government must provide market-supporting mechanisms, including new forms of public-private partnerships because of their high national consequence.

It is of interest to note that in a study of Private Sector vs. Public Sector Risk,[4] the probability of a terrorist attack is shown slightly lower than ice storms and slightly higher than hurricanes. It is predictable that the utility system of the future could become more vulnerable to information interception or corruption by skilled electronic intrusion originating both inside and outside the system. Threats from insiders are expected to be the most common.

The industry has more experience dealing with natural disasters than with threats to critical information.

The issues of physical vulnerabilities have been extensively studied (e.g., a study by the Office of Technology Assessment[5]). One conclusion reached is that "no plausible natural disaster should damage the bulk power system so badly as to cause widespread power outages for more than a few days if utilities have taken adequate precautions." Compared to dealing with physical and environmental events, the industry does not have equivalent studies or a long history of dealing with information threats. Planning ahead to acquire state-of-the-art knowledge of information security measures would contribute to a reduction in overall vulnerability.

Cost of new R&D on security can be reduced through public/private sharing.

Investments in long-term research and development (R&D) are already diminishing and may become insufficient for national security and the public good.[6] The depletion of R&D resources may not be felt immediately, but over time, the loss of a commitment to technology investment will reduce economic growth, impair international competitiveness, and erode technological and economic leadership. Through private sector-public sector cooperation on R&D, preparedness, and response, the cost to each sector can be reduced while the degree of risk mitigation is increased.

> A major challenge is assessing and reducing the vulnerability of the utility systems as a whole. Issues of jurisdictional accountability and the means to replace dwindling funds needed to maintain continuity of R&D for the longer term are of growing concern.

ROADMAP DEVELOPMENT

The electricity infrastructure is two tightly coupled networks: the power grid and the electric information network.

In assessing the uncertain impacts of market and technological change, it is convenient to view the electricity infrastructure as two tightly coupled networks. One is the physical network of power generation, distribution and use–the electric power grid. The other is the underlying data network and processing systems that are critical to safe and reliable management of the power grid–the electric information network.

In this roadmap, the issues of infrastructure assurance will be examined as the four closely interrelated areas of concern that have emerged.

I. PUBLIC ROLES AND RESPONSIBILITIES

- THE TRANSITION FROM A REGULATED, VERTICALLY INTEGRATED MONOPOLY TO A COMPETITIVE INDUSTRY DEMANDS A FRESH APPRAISAL OF THE ROLES AND RESPONSIBILITIES OF THE PRIVATE AND PUBLIC SECTORS, INCLUDING THE INTERRELATIONSHIPS OF FEDERAL AND STATE GOVERNMENT.

II. POWER SYSTEM MANAGEMENT

- THE GRAND SCALE AND COMPLEXITY OF THE POWER SYSTEM PROVIDES A CONTINUAL RELIABILITY CHALLENGE BECAUSE OF VULNERABILITIES UNDER NORMAL OPERATING CONDITIONS AND EVEN GREATER VULNERABILITIES AND INSTABILITIES DURING EMERGENCIES, WHETHER CAUSED BY ACTS OF NATURE OR BY DELIBERATE ACTS.

III. INFORMATION SYSTEM MANAGEMENT

- THE PERVASIVE DEPENDENCY ON INTERCONNECTED INFORMATION SYSTEMS AND COMMUNICATIONS NETWORKS BY THE ELECTRIC UTILITIES RAISES CONCERNS OVER INTRUSION AND THE SECURITY OF CRITICAL INFORMATION SYSTEMS AND DATA.

IV. INTERDEPENDENCIES

- THE ELECTRIC POWER INFRASTRUCTURE IS DEPENDENT ON THE SERVICES PROVIDED BY OTHER INFRASTRUCTURES AND VICE VERSA. FOREMOST AMONG THESE ARE THE TELECOMMUNICATIONS, FINANCIAL SERVICES, TRANSPORTATION, OIL AND GAS, AND EMERGENCY SERVICES SECTORS.

TECHNOLOGY AND POLICY OBJECTIVES

The technical and operational challenges are addressed in this roadmap as a related set of critical success objectives with associated technology and policy gap analysis and initiatives. Over the next 15 years, the objectives to address new market conditions, meet new quality standards, and counter threats are:

1. **BALANCE PUBLIC AND PRIVATE INTERESTS IN THE NATION'S ELECTRICITY SUPPLY. ENSURE THAT PUBLIC POLICY, ROLES, AND RESPONSIBILITIES WILL GUARANTEE THE PUBLIC GOOD WHILE PERMITTING FREE MARKET FORCES TO SERVE PRIVATE INTERESTS.**

2. **GUARANTEE THE SAFETY, AVAILABILITY, AND QUALITY OF THE NATION'S ELECTRIC POWER GRID. CONTINUE THE FUNDAMENTAL RESEARCH TO UNDERSTAND, CREATE, AND APPLY POWER TECHNOLOGY PRODUCTS AND MANAGEMENT TOOLS CRITICAL TO ASSURANCE OF THE POWER GRID.**

3. **GUARANTEE THE INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY OF THE INFORMATION NETWORK. RESEARCH, DEVELOP, AND APPLY SECURE, ROBUST, AND ADAPTIVE INFORMATION SYSTEMS, NETWORK TECHNOLOGIES, AND MANAGEMENT TOOLS.**

4. **INCREASE ASSURANCE OF INTERDEPENDENT INFRASTRUCTURES. INCREASE UNDERSTANDING OF WHAT EACH INFRASTRUCTURE OWNER/OPERATOR MUST KNOW ABOUT OTHER INFRASTRUCTURES TO ENABLE RATIONAL CONTINGENCY PLANNING. DEVELOP NEW COOPERATIVE AGREEMENTS WITHIN THE INDUSTRY AND BETWEEN INTERDEPENDENT PRIVATE AND PUBLIC SERVICE PROVIDERS.**

The global goal for the infrastructure is to fulfill the public trust by ensuring that the surety, availability, and quality of electricity are maintained by the future competitive marketplace.

TECHNOLOGY AND POLICY ROADMAPS

The driving requirements critical to achieving each of the four key objectives are presented in the text and tables that follow. The responsibilities are coded as FG-Federal Government, SG-State Government, LA-Local Authorities, EP-Energy Providers, SV-System Vendors, AC-Academia. The lead role is listed first.

OBJECTIVE 1: BALANCE PUBLIC AND PRIVATE INTERESTS IN THE NATION'S ELECTRICITY SUPPLY.

NATIONAL POLICIES AND ROLES (FG, SG)

Where market forces fail, government should take action at the levels closest to stakeholders.

The changing mix of stakeholder interests in the power system calls for a reexamination of the appropriate roles of government in a competitive market. A set of principles needs to be established (possibly based on the concept of subsidiarity[7]) that would require government action only if and insofar as objectives cannot be achieved through a system of open and competitive market forces. Further, actions should be taken at the level closest to the stakeholders, and the means employed should be commensurate with the aims to be achieved.

The central role for government (including national laboratories with pertinent expertise) is attention to issues and actions at the national level that are not amenable to resolution by industry participants. Panelists from private industry at a recent workshop felt that the concept of an integrated national electric transmission grid should receive the highest priority for federal R&D expenditures.[8] The same workshop envisaged an entity having overall responsibility for operation of a national electric grid, should wholesale market forces fail to meet expectations.

The protection of infrastructure must become a practical matter of agreeing on what government agencies need to do in key areas including:

- Allocating authority and accountability for the national electric grid
- Supporting R&D and leading by example
- Increasing public awareness in the absence of a catastrophe
- Providing incentives for business to do more
- Working with industry to develop power system assurance standards
- Improving the status of university technical programs
- Dealing with international and legal issues[9]

R&D ON POWER SYSTEM RISK ASSESSMENT AND DEFENSE (FG, EP)

The consequences of large-scale attacks need to be understood and quantified with models and simulations.

An understanding of the vulnerabilities, threats, and impacts and the deterrence and response to large-scale attacks in the context of the power system is needed. The economic and national security consequences of large-scale system failures need to be understood and quantified where possible. These consequences will help national policymakers decide the importance, urgency, and resources to be allocated to infrastructure defense. It is important for government to understand the risk and to inform industry about the possible motives and opportunities of potential attackers and about effective countermeasures and their costs. Needed are comprehensive models and simulations that will provide the basis for estimating the probabilities and impacts at a level requiring detailed understanding of system failures. Within the public sector, jurisdiction decisions are required on responsibilities for strategy, implementation, and compliance.

PRIVATE SECTOR AWARENESS AND EDUCATION (FG, SG, AC)

The public sector must share information with the private sector in order to raise the level of awareness.

A primary role of the public sector is dissemination of information to aid the private sector in thinking and acting defensively. New mechanisms are required to share the knowledge gained by government agencies and the military from their threat assessments and protective and recovery measures. Private sector awareness can be enhanced through practical system planning, engineering, simulation, probes, games, and exercises. A federally funded educational program at universities should be introduced to strengthen the areas of protection and recovery of complex systems in degree programs for the system engineering disciplines.

PROTECTION OF POWER FOR CONTINUITY OF GOVERNMENT AND ESSENTIAL SERVICES (FG, SG, LA, EP, SV)

Low-cost, on-site back-up power should be deployed.

In the near-term, federal, state, and local government and related essential services should have a back-up power reserve adequate to support critical functions. Low-cost, on-site electrical generation and storage technologies need to be made available by the marketplace, perhaps with government incentives.

Strong protection of electric utility power supplies to the key metropolitan areas, including the nation's capital, should be provided for by conducting system studies followed by implementation of necessary measures. Protection should encompass ways to strengthen the infrastructure against physical and man-made disasters and realistic cyber attacks. The federal government should fund the systems studies and should cost-share the implementation with state and local governments in the same proportion as the Federal Emergency Management Agency's (FEMA's) disaster mitigation grants (75% vs. 25%). Protective measures should be implemented in a modular, open systems fashion to take advantage of new technology as it becomes available.

OBJECTIVE 1: Balance public and private interests in the nation's electricity supply.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Develop clear national policies and roles	Clarity and adequacy of boundary definitions	Policies and roles defined for a regulated and terrorist-free era	Public-private sector conference on policies and roles Complete immediate action plan	Implement a transition plan	Public-private management of a national electric power system
Research power system risks and develop defensive measures	Risk/reward metrics and methods	Generally confined to physical protection	Simulate and assess large-scale attacks Estimate national security and macro-economic benefits of improved protection	Periodic testing and upgrades	Large-scale implementation of standards for resilient systems
Enhance private sector awareness and education	Public outreach programs and specialist degrees	Essentially none	Develop programs tailored to private and public sectors, including higher education	Refine and continue programs Fund academic achievement awards	Refine and continue programs
Strong protection of power for continuity of government, essential services, and major metropolitan areas	Impact assessments	Ad hoc attention except in rare cases	Survey back-up power supplies Set standards at FG, SG, LA levels Conduct metro area system studies	Implement standards. Secure public funding and implement	Conduct regular exercises
Plan to maintain generation and transmission reserve capacity	Stability margins	Excess resulting from rate base regulation. Margins decreasing	Review FERC and NERC authorities, introduce legislation	Maintain or increase reserve capacity per regulation or law	Worst-case simulations
Transfer of technology from the public to the private sector	Best practices, procurement specifications	Results not widely known in private industry	Transfer of model policies, practices and standards Transfer information surety technology	Ongoing development and transfer	Ongoing development and transfer
Manage funds allocated for emergency relief and recovery	Budgets	FEMA and LA budgets for natural events only	Introduce legislation for federal-state cost sharing following FEMA formula	Implement preventative mitigation measures	Funded comprehensive relief and recovery plan
Develop domestic and international frameworks for cooperation	Declarations on principles, laws, treaties	Many open issues on cyber-based crime and terrorism	Introduce legislation to correct deficiencies in authorities	Periodic international conferences	Periodic international conferences

MAINTAINING GENERATION AND TRANSMISSION RESERVE CAPACITY (FG, SG, EP)

Operating reserves may have to be mandated by Congress.

In a shared but competitive system such as the North American power grid, no one "owns" either the problems or the solutions. In the future, the electric power industry will have to serve the public good, but the means to do so are not clear. The administration of programs at a state level would likely not achieve the results needed for issues nationwide in scope. An entity such as the Federal Energy Regulatory Commission (FERC) should regulate, or the Congress should legislate, that generation and transmission capacities be maintained at a safe margin nationwide. NERC or some other independent agency charged with oversight should determine that the adequate operating reserves are being maintained.

Utility rate bases should be allowed to include cost of improving and securing transmission or adding essential capacity.

All PUCs and FERC should allow the costs of transmission capacity expansion necessary to meet this safety margin to be included in the rate base. There needs to be some allowance for the marketplace to determine whether generation or transmission should be built to meet the needs of the customer, but PUCs and FERC must allow transmission owning entities to recover investments through increases in the rate base to build or improve transmission to deliver essential capacity and energy to the load centers. Increased interconnection between regions, subregions or power pools should be considered an acceptable means of meeting the generation capacity safety margin. Generation size and location is extremely important in maintaining interconnected transmission capacity between subregions.

TRANSFER OF TECHNOLOGY FROM THE PUBLIC TO THE PRIVATE SECTOR (FG, SV)

Government can lead by example and encourage adoption of new technology.

Public agencies, such as the Department of Defense and the Department of Energy, by developing and protecting their own sites and systems, can lead by example and stimulate the development and transfer of advanced technology and know-how to the private sector. Government systems can be used as testbeds, and procurement policies can further serve to develop the market for new robust systems and to set de facto standards.

FUNDS FOR EMERGENCY PROTECTION, RELIEF, AND RECOVERY (FG, EP, SV)

Funding for infrastructure protection should be through a combination of public and private sources.

The choice between regulatory and market mechanisms to fund critical civilian infrastructure protection and relief is a public policy issue to be settled through political processes. Government financial support can be used, but requirements may increase if the frequency and impact of attacks grow. In addition, the federal government should plan to fund or provide incentives to the private sector to mitigate the effects of low probability, high consequence disasters or cyber attacks. The role of insurers also needs to be defined.

DOMESTIC AND INTERNATIONAL LEGAL FRAMEWORKS FOR COOPERATION (FG)

Cyber threats do not recognize borders. International cooperation is essential.

Cyber threats to US power supply information support systems are difficult to anticipate, counter, and prosecute. Because of the international issues involved in cyber threats to information systems, it would be useful for the government to review existing relevant laws, treaties, and protocols and take appropriate action. Leadership by the federal government is required to create an international environment that raises the level of understanding and encourages cooperation and coordinated action. Internationally agreed-upon statements of principle have an important influence. On the domestic front, the legal authorities of the Department of Justice, FBI, and CIA to trace, identify the source of, and neutralize cyber attacks within and across national borders should be reviewed for adequacy.

OBJECTIVE 2: GUARANTEE THE SAFETY, AVAILABILITY, AND QUALITY OF THE NATION'S ELECTRIC POWER GRID.

INVESTIGATE AND PREPARE FOR THE YEAR-2000 PROBLEM (FG, EP, SV)

Microcode embedded in control function chips could cause serious disruptions.

Preliminary studies of this subject by EPRI and others suggest that there may be a very large, dangerous, and costly situation with little time left for attending to it. The focus has now shifted from management information systems to concern for microcode embedded in a myriad of chips involved in control functions throughout the industry. The potential for serious disruption and major power system damage exists and demands immediate concerted efforts by industry stakeholders. Failure to take reasonable precautions would leave a utility open to charges of failure to prevent avoidable loss.

R&D AND TRANSFER OF TECHNOLOGIES FOR PUBLIC INTEREST ISSUES (FG)

R&D in electricity infrastructure has dropped significantly and will continue to fall as restructuring proceeds.

In addressing the need to secure R&D in the public interest, a highly respected leader in the electric power industry recently stated:

> The national utility industry objective has become unstable, and the industry may not continue to support R&D of this type in a competitive environment.
>
> Chauncy Starr, President Emeritus,
> EPRI Journal, December 1996

A General Accounting Office report on changes in electricity related R&D funding[10] concluded that investments by utilities dropped by about 33% during the calendar years 1993 through 1996 and that further reductions are expected. In 1992, the National Association of Regulatory Utility Commissioners recommended that utilities devote 1% of their revenues to R&D. This would have amounted to about $2.2 billion in 1996, whereas the actual amount was around $480 million, or 0.22% of revenues.

Certain parts of utility infrastructure R&D will require government support.

In keeping with the principles for public involvement, R&D will be required for key technologies that probably would not be developed without a government supported research program. One positive sign on the horizon is the preliminary recommendation of the President's Commission on Critical Infrastructure Protection that government supported R&D funding against threats to critical infrastructures be immediately doubled to $500 million in 1999 and increased thereafter until it reaches a level of $1 billion per year.[11] These technologies will be required to prevent disruption, mitigate threats, and minimize impacts and thus provide the basis for a more reliable power system. Continued improvements in protection and recovery of critical public power and information systems could provide the knowledge and technology base for protection of privately owned infrastructures.

OBJECTIVE 2: Guarantee the safety, availability, and quality of the nation's electric power grid.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Investigate and prepare for the "Year 2000" problem	Number of at-risk devices and affected power plant	Large number of at-risk devices and unpredictable consequences	Coordinate research efforts and information sharing Coordinate contingency and recovery planning		
R&D and transfer of technologies required to address public interest issues	Public money spent and value delivered to private sector	DOE funding at about $1B per year Value derived is unclear.	Fund as dictated by a risk and a defense assessment Introduce value metrics	Conduct periodic review of the risk-defense assessment	Conduct periodic review of the risk-defense assessment
R&D techniques and analysis tools for large-scale power system behavior and control	Scope and speed of tool capabilities	Stability analysis and projections taking 20 minutes at a regional level	1,000 fold increase in speed with subcycle state information	Devise accurate models and tools for the national grid	Develop new tools and techniques for decision support of real-time analysis
Develop commercial products for mid- to long-term deployment	Size of market for robust products	Loss of US leadership in key power technologies	Increase government-industry cost-shared R&D on energy storage, transmission and distribution, survivability and management	Transfer and implement R&D results Government procurements and incentives	Implement a self-sufficiency plan for robust products
Develop methods and facilities for testing and simulation	R&D budgets and head count	Conducted by many of the DOE labs Overall alignment of capabilities vs. needs is unclear	Rationalize public and private initiatives for testing and simulation Create a long range plan	Conduct periodic review of results and plans	Conduct periodic review of results and plans

There is a critical need to define a prioritized research agenda and create a new organizational framework for coordinating federal and state roles in funding and conducting research at a national level. This prioritization and coordination will provide organized direction and help avoid duplication of effort. The research agenda concerned with national and strategic issues is likely to include fault-tolerant architectures, high-speed computational resources and algorithms for dynamic security assessments, HVDC (high-voltage direct current) methods, high-power and high-speed semiconductors, FACTS (flexible AC transmission systems) devices, high-voltage metering, superconducting materials and applications, and superconducting magnetic energy storage.

> Government sponsored R&D should be managed in a manner that is well aligned with public sector goals and expedites technology transfer to the private sector, perhaps with an advisory structure involving EPRI, the national labs, and agencies of the federal government.

TECHNIQUES AND ANALYSIS TOOLS FOR LARGE-SCALE POWER SYSTEM CONTROL (FG, EP, SV)

Optimal power flow of large grids will eventually be self-organizing for maximum efficiency.

Current control technologies and practice rely largely on off-line assessments of the power system using steady-state analyses. Fully integrated on-line security assessment tools to facilitate real-time transient analysis and system control are under development, but require further research. Better software tools and models are required for human decision support. New knowledge and improvements are needed in state estimation, measurements, data collection, and adaptive control algorithms. An ongoing R&D project for system simulations aimed at optimal power flow on large power grids is the Wide Area Measurement System supported by the DOE, EPRI, Pacific Gas and Electric, the Bonneville Power Administration and the Western Area Power Administration.[12] The technology direction is for the power grid to become self-organizing by dynamically using information about demand and the current state of the underlying system to allocate resources for optimum efficiency.

MID- TO LONG-TERM COMMERCIAL R&D (FG, EP, SV)

Distributed resources and off-line energy storage could reduce risks and improve reliability.

R&D should be accelerated to improve energy generation, storage, and delivery options available to utilities and their customers. Distributed resources can improve reliability, and system studies should be conducted on how to quickly and reliably bring these resources, including independent power producers and cogenerators, on line when utility generation fails. High-energy-density batteries and inertial, gravitational, electric, and magnetic options for storing power generated during off-peak periods should be developed and deployed. Some of these options could be disconnected from the grid when not in use to prevent them from being damaged during natural and man-made disasters and electronic attack. Likewise, some information handling systems may warrant being disconnected from communication networks to avoid cyber attacks.

Since nearly 90% of all customer-affecting power outages are because of failures in the transmission and distribution system, R&D should also be focused on developing more capable energy management systems, survivable materials, structures, economical underground solutions, and

network architectures for transmission and distribution. For example, substation automation equipment that will transmit information between devices several orders of magnitude faster than currently possible will enable increases in economical and reliable power. Future energy management systems will use delivery network data to increase network capacity, transfer less-expensive power over longer distances, and ensure even greater levels of reliability despite the increased volume and complexity of transactions.

> It is yet to be determined how reliable and cost-effective distribution systems will emerge in the new competitive environment and what, if any, state regulatory involvement will be required in setting performance guidelines.

ORGANIZATION AND FACILITIES FOR TESTING AND SIMULATION (FG, AC)

DOE should take the lead role in establishing organizational structure and providing test facilities.

To carry out the policies requiring R&D on power system risk assessment and defense (mentioned in Objective 1), a multiparty organization, incentives, and resources will be required. The key to successful research and implementation of the technologies is to address broad stakeholder interests in the private and public sectors, including universities.

The DOE should have a lead role in establishing the organizational structure and funding mechanisms. The national laboratories and the National Energy Research Scientific Computing Center should play key roles in providing the physical facilities needed for testing and simulating the viability, reliability, and maintainability of new technologies. More attendance at exercises such as Prosperity Games™, the RAND Strategic Simulations, and the Vital Issues Process workshops should be encouraged to explore the state of readiness within the industry and with cross-industry dependencies.

OBJECTIVE 3: GUARANTEE THE INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY OF THE INFORMATION NETWORK.

Electric power communication and computer security is in its infancy.

An assessment of electric power control systems security[13] concluded that "Electric power communication and computer security is literally at its infancy. Most utilities do not have security measures in place at all and rely on a combination of private communication networks, proprietary protocols, and lack of knowledge of utility operations to provide what security there is. They are quite vulnerable to concerted attack and have little realization that this is true."

RESEARCH TO DEFINE OPERATIONAL REQUIREMENTS (FG, AC, SV)

This research will focus on utilities' internal operations and information networks to other related parties.

A structured information technology risk and impact assessment approach is required to develop independent information security requirements sets for the operations of electric utilities. An advanced information protection framework needs to be developed and implemented to clearly define, model, and describe the electric utility operations infrastructure from an information security perspective. These requirements will focus on utilities' internal operations and the information technology infrastructure for interconnected parties (e.g., power pools, marketing companies, billing services, etc.) and will consider state and federal laws that influence such requirements. With this understanding of the risks, a related R&D agenda and mitigation strategies can be described and prioritized.

RESEARCH IN THE BEHAVIOR OF COMPLEX INFORMATION SYSTEMS (FG, AC)

We need to understand large real-time networked systems down to the finest level of detail.

Similar to the need for a long-term power system R&D agenda, the critical need is to define a prioritized research agenda in the information technology domain. The need is to understand the theory, behavior, and means to control large distributed real-time networked systems at all levels, from an overall architecture view down to the finest level of detail in hardware and software.

A biological metaphor is often used to describe self-healing, adaptive immune systems and architectures. Research will likely be concentrated on trusted hardware and software design disciplines, adaptive fault-tolerant systems that minimize vulnerability, agents for real-time information management, decision support tools, and industry-specific data communication protocols.

Further research is needed on the dissemination of understandable information on the occurrence of faults. Similar needs exist in other infrastructures and cross-sector research should be coordinated wherever possible. The international standards for Open Distributed Processing[14] recommendations should be considered and adopted or adapted to meet the future needs of the industry.

OBJECTIVE 3: Guarantee the integrity, confidentiality, and availability of the information network.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Research to define operational requirements	Commonly accepted risk assessment methods and metrics	Infrequent and inadequate attempts to assess risk and requirements	Advanced information protection framework and high priority agenda defined	Fully funded and prioritized R&D agenda and means to monitor results	Continue development of mitigation measures
Long-term R&D in the behavior of complex systems	Synchronization of, and human interactions with, distributed data processes	Systems limited to simple filtering transactions and message passing	Develop "intelligent telemetry" concepts, architecture, and behavior modes	Develop breakthrough solutions to issues of human interaction Expansion of software component technologies	Convergence of network and systems management capabilities across industries
Develop management strategies and protective measures	Formal policies and practices	Frequently ill-defined policies and practices Low recognition of asset values	DoD and DOE fund R&D on defensive strategies Utilities establish best practices	Transfer R&D results on information security Institute commonly accepted principles	Continuation
Develop commercial products for mid- to long-term deployment	Market demand and supply	A growing generic product market but lacking utility specialization	DoD and DOE fund R&D on a robust internet and detection/protection systems and tools	Transfer R&D results to utility sector. Utility industry procurement standards	Continuation
Develop methods and facilities for testing and simulation	R&D budgets and head count	Conducted by many of the DOE labs Overall capabilities vs. needs is unclear	Rationalize public and private initiatives for testing and simulation Create a long-range test plan	Conduct joint government-industry exercises with annual review of results and plans Implement lessons learned	Annual review of results and plans
Information security requirements and standards	Probability of loss and cost of insurance	Concept of avoidable loss is untested Minimal acceptable levels are undefined	Establish security working groups within all utility standards setting groups	Develop and implement security standards and educational curricula	Establish and practice national standards of excellence

MANAGEMENT STRATEGIES AND PROTECTIVE MEASURES (EP, SV)

A strategy is required to achieve the objective of relating risks to individual electric utility operational data systems and to establish a prioritized set of protective initiatives. Utilities need the ability to independently analyze the security requirements for their information technology infrastructure protection and to determine the strategic approaches that they can apply to mitigate any risks that are found to be significant. Prudent utilities will incorporate information systems disaster recovery and contingency planning within their overall power systems emergency planning.

A model strategy, along with policies and practices, should be developed for information security management, including information security and recovery metrics and standards to span the functions of:

- Deterrence (monitor; identify, prosecute, and extradite attackers; international agreements),
- Counter-intelligence gathering (encryption, deception, detection),
- Confusing offensive strategic/tactical analysis (use unpredictability, deception, and redundancy),
- Hardening systems (find, close, or wall-off vulnerabilities),
- Intrusion detection (at both functional and technical levels),
- Reaction to attack (contain, gracefully degrade, adapt, and recover).

MID- TO LONG-TERM COMMERCIAL PRODUCT R&D (FG, EP, SV, OTHERS)

Utilities should be encouraged to invest in protective systems through positive regulatory action.

In recent testimony to the House Committee on Commerce,[15] Ralph Masiello, VP of Strategic Development at ABB, Inc., stated, "It can be expected that utilities will increase their information system capabilities as fast as capital investment and cost recovery allowed by regulatory bodies will permit. ABB believes that instead of just being 'permitted' to make investments, utilities should be encouraged to do so by positive regulatory action." Referring to California as setting the stage, Mr. Masiello went on to state that "the ISO [Independent System Operator] will end up with a transaction processing requirement as large as any used in American commerce today. Add to this the desire of FERC and the industry to immediately move to handling these requirements over the Internet, or at least with Internet technology, and you have one of the largest information technology challenges around today."

Accelerated R&D should focus on robust operating systems, software, and databases.

The utility industry should become a leader to accelerate R&D focused on providing robust operating systems, application software, databases, and Internet and associated standards and products that can improve the ability to secure vital information systems to appropriate degrees. Consideration should be given to using the Software Engineering Institute's Capability Maturity Model (CMM)[16] to provide the basis for improving the quality of software delivered to the utility industry. The concept of tamper-resistant devices may have many utility applications such as electronic metering. These devices erase sensitive data in their memories whenever improperly used and are designed to comply with the Federal Information Processing Standard 140-1.

The following categories of new, secure robust technologies, products, and tools should be developed or adapted for, and implemented on, critical information systems supporting the infrastructure.

- Decision support tools for risk, cost, impact, and benefit assessments
- Intrusion detection and protection systems and tools
- Malicious code detection and eradication
- Software integrity and verification
- Auditing and stress testing
- Monitoring, diagnostics, and forensics
- Encryption and access control

ORGANIZATION AND FACILITIES FOR TESTING AND SIMULATION (FG, EP, SV, AC)

Similar to the needs described in Objective 2, a multiparty organization, incentives, and resources will be required for testing and simulation of the behavior of large-scale data networks and systems. A report by the Center for Global Security Research[17] states that, "Ultimately, threats and vulnerabilities need to be tested on a working testbed, and research results that project hardening also need to be evaluated. Due to the expense of such a testbed, consideration must be given to developing a virtual testbed; in addition, there will be the need for several testbeds distributed throughout the country that can be accessed by researchers and implementors."

Consideration should be given to creating several virtual testbeds.

Once again, the key to successful research and implementation of the technologies is to include broad stakeholder interests in the private and public sectors, including universities. The DOE should have a lead role in establishing the organizational structure and funding mechanisms. The national laboratories, the National Energy Research Scientific Computing Center, and the National Science Foundation (NSF) should play key roles in providing the physical facilities needed. Simulated disaster back-up and recovery exercises should be carried out on a regular basis to train industry members and to explore the state of information readiness within the industry.

Broad stakeholder interest should be included in research and implementation.

INFORMATION SECURITY REQUIREMENTS AND STANDARDS (FG, SG, LA, EP)

Government leadership in encouraging the development of minimum acceptable information security standards associated with critical, essential, and sensitive electric utility data is important. These requirements will have to result in operating standards that are practical and economically effective. Such standards are typically based upon legal dictates and good business practices, perhaps similar to commonly accepted accounting principles used in financial auditing. An example of such a

Current standards have not kept pace with the evolution of network systems.

government-industry collaboration can be seen in the European Computer Manufacturers Association Standard ECMA-205,[18] which defines a minimum set of requirements for commercial applications. This is distinguished from other standards such as those in the US Trusted Computer System Evaluation Criteria or Orange Book 1983, which were tuned towards military and government requirements. Current standards have not kept pace with the evolution of network systems; however, considerable work is taking place to set standards for how information security can be specified and assessed in working systems. Details of this work can be found at <<http://csrc.nist.gov/nistpubs/cc/>>. Efforts by the Committee Consultative International Telegraph and Telecommunications (CCITT), an international communications standards organization, include work underway to support security in distributed applications and deserve more support from the US.

Standards should not become proprietary.

Encouraging and monitoring actions taken to secure the infrastructure is a proper role of state and local agencies. Standards should be voluntary except where national security is at stake. The federal government together with national standards bodies (e.g., ANSI, IETF) should ensure that standards, such as those for encryption key management, do not become proprietary or, at a minimum, that licensing costs remain affordable.

OBJECTIVE 4: INCREASE ASSURANCE OF INTERDEPENDENT INFRASTRUCTURES.

It is critical to have achieved an analysis of the risks to the power and information systems belonging to electric utilities, as outlined in Objective 1, and to develop a set of strategies that can mitigate the risks that are found in such related areas as fuel diversity. It is important to apply such analyses at the appropriate level and not to try to apply a general approach or set of requirements for the various operating levels (company specific, power pool, general applicability to the sector).

> The distribution of threat/vulnerability risk analysis and mitigation strategy documents should be appropriately restricted.

MINIMAL ESSENTIAL INFRASTRUCTURE (FG, EP)

An MEI-EP would provide minimum power for essential government services at all levels and military preparedness.

The concept of a Minimal Essential Infrastructure (MEI) is controversial and hard to define.[19] An MEI definition for electric power (MEI-EP) should be explored and must involve a combination of defined responsibilities, systems, procedures, laws, and tax incentives that directly and indirectly affect the assurance of the power system. An MEI-EP should include providing the minimum power necessary for the continuity of essential government services at local, state, and federal levels, including

OBJECTIVE 4: Increase assurance of interdependent infrastructures.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Plan for minimal essential infrastructure assurance	Quantitative and qualitative objectives	Proposals at a concept stage	Define a MEI for the electric power industry with multiparty consensus	Develop an interim strategy and implement key provisions	Fully develop MEI across industries
Manage public and private sector collaboration	Government/industry assessments Results of industry and essential services in action	Government roles need attention Private industry groups like NSTAC missing in the electric industry Insufficient cross-sector coordination	Create a National Infrastructure Assurance Council comprised of senior CEOs and selected Cabinet Officers Identify government leads for each area	Analyze actual events and conduct simulations	Refine analysis and projections based on actual events and conduct simulations
Develop joint preventative measures	Formal cross-sector agreements	Contingency planning is limited and has a physical emphasis	DoD and DOE develop and share results of intelligence Form a NSA/NIST/DOE information assurance partnership to speed certification of security products	Routine exchange of incident warnings and remedial actions	Cross-training programs in infrastructure protection
A strategic plan to limit impacts of interdependencies	Cross-sector interdependencies risk-impact studies	None in widespread use	Federal government in concert with national associations develops a cross-industry plan The electric power industry and DOE develop a recovery plan for fuel, communications, and transportation disruptions	Continue evolution of the plan in light of experience and changing circumstances	Continue evolution of the plan in light of experience and changing circumstances

maintaining military readiness. Government could encourage infrastructure strengthening and expansion through regulatory processes and tax incentives. Through regulation of insurers, government should continue to play a role in ensuring the financial health of insurers and assuring the public a minimum level of service.[20]

There are many issues surrounding the exact nature of an MEI that arise from the blurring of traditional boundaries between law enforcement, military, and civilian responsibilities. Two examples that will have a bearing on the future of integrity and privacy in electric power data exchange and transaction processing are the issues surrounding public key infrastructures[21] and payment systems security.[22]

PUBLIC AND PRIVATE SECTOR COLLABORATION (FG, SG, EP, SV)

Government can be the focal point for collaboration between public and private sectors.

Roles and responsibilities for government's state of readiness at department levels need to be exemplary. The only place within the entire electric power industry where disaster recovery plans are required by regulatory agencies is at nuclear power plants, identifying the need for reassessing government policies and procedures. Government will also be needed to facilitate multiparty collaboration within the public and private sectors.

> The situation calls for a focal point within the federal government, at the White House or National Security Council level, for continued critical infrastructure protection.

Examples of such leadership and collaboration are:

- A formal incident escalation reporting structure and process
- A repository of best practices, methods, and results
- Shared access to incident data and recovery experience
- Priority allocations of resources in emergencies
- Metrics to identify critical, essential, and sensitive information
- Joint recovery coordination exercises
- Increased public awareness of threats and system options
- Stocking of critical components
- Attacker identification and attack neutralization
- Incentives for infrastructure strengthening

PREVENTATIVE MEASURES (FG, EP, OTHER SECTORS)

Emphasis needs to be placed on cross-infrastructure and cross-industry protective measures.

Preventative measures to deal with high-risk threats and vulnerabilities will include critical node and cross-infrastructure scenario analysis and advanced indications and warnings from industry-wide and government centers. More emphasis needs to be placed on the front-end intelligence gathering and analysis that a sophisticated attacker must perform to mount a damaging attack. The traditional approach of harden, detect, react needs to continue, but with more emphasis placed on creative reactions to attacks (e.g., graceful degradation, adaptability). Examples of cross-sector and cross-industry protective measures are:

- Indications and warnings processes and systems
- Joint probes and auditing exercises

- Contingency planning, modeling, and simulations
- Generally accepted practices and regulations on avoidable loss
- Education and training of security personnel
- Testing and certification of security products
- Shared tools for management of multiple contingency events

STRATEGIES TO LIMIT IMPACTS OF INTERDEPENDENCIES (FG, EP, OTHER SECTORS)

Interdependencies require cross-industry mitigation plans to limit impacts.

Mitigation recommendations will be focused on understanding and limiting cross-industry vulnerabilities associated with the protection of the power supply infrastructure and its supporting information systems.

A cross-industry mitigation plan, at a strategic level, can be used for selecting tactics to lessen the risks to the continuity and integrity of electric utility power and information systems. Mitigation planning strategies can be addressed at national/generic levels, regional/power pool levels, and for the individual utilities where there is a high enough probability that there is a threat that can exploit any vulnerability.

Such strategic plans will define measures to limit impacts and recover from emergencies including, but not limited to, the following:

- Disruption of fuel supply
- Disruption of telecommunications
- Disruption of the power trading infrastructure
- The corruption of critical and essential control information

Modeling and simulation tools will be essential for identifying and analyzing vulnerabilities caused by interdependencies among infrastructures.

TECHNOLOGY AND POLICY DRIVERS

A summarized list of the principal technologies and technology-related policies that drive the success of the objectives is as follows:

- The clear definition of surety requirements for the operation and management of the restructured electric power industry.
- The development of modeling tools that can analyze the complexities of the national scale power grid and its interdependencies with other infrastructures.
- The education of the electric power industry regarding the need for increased information surety in the Electric Power Infrastructure.
- A commitment for long-term government and industry research funding to investigate the protection of the Electric Power Infrastructure and its interdependencies with other infrastructures.

OPPORTUNITIES AND SHOWSTOPPERS

OPPORTUNITIES

We must take advantage of the current momentum and national concern with the protection of the national infrastructures. In addition, many information technologies are still evolving, and now would be an opportune time to help direct their evolution to meet needs specific to the Electric Power Infrastructure. The Internet, for example, is one of the most used and least protected methods for transporting information. Its use is expanding and includes the transport of some Supervisory Control and Data Acquisition (SCADA) system data used in the electric power industry. However, it is very unlikely that SCADA-unique requirements are being considered in the development of Internet security.

SHOWSTOPPERS

Unless industry and government act immediately, infrastructure stakeholders may be lulled into complacency. An unfortunate reality is that an event resulting in a significant loss of money or lives must usually occur before industry will respond to a threat. The recently released President's Commission on Critical Infrastructure Protection report is still fresh in many people's minds, but until actions and funding are assigned, many stakeholders may be reluctant to act.

The 1998 Auckland, New Zealand, power outage is an example that should be studied and learned from to avoid a similar catastrophe.

NOTES

1 S. Gehl. Powering Progress, The Electricity Technology Roadmap Initiative. A Preliminary Vision of Opportunities. EPRI May 1997.

2 Report of Vital Issues Panel I: The North American Power Grid. Sandia National Laboratories. April 23, 1997.

3 Electric Power Information Risk Assessment. NSTAC. March 1997.

4 G. H. Copelan. Risk Sharing and Energy Emergency Preparedness. Department of Energy (DOE).

5 Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage. Office of Technology Assessment, PB90-253287.

6 Electric Power System Infrastructure Technology Research and Development Recommendations. DOE Task Group draft. July 3,1997.

7 A. Kelman. Developments in European Intellectual Property Law. The Seventh Conference on Computers, Freedom and Privacy, CFP 97.

8 Emerging Critical Issues and Technology Needs. Sandia National Laboratories report, SAND 97-1659. April 1997.

9 L.T. Greenberg. Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda. Stanford University. July 21-22, 1997.

10 Changes in Electricity-Related R&D Funding. General Accounting Office. GAO Report 96-203, August 1996.

11 Remarks by R. T. Marsh, Chairman of the President's Commission on Critical Infrastructure Protection at the Bankers Roundtable meeting, Sept. 11, 1997. www.pccip.gov/marsh_banker.html

NOTES (continued)

12 J. F Hauer et al. Information Functions and Architecture for Networked Monitoring of Wide Area Power System Dynamics. Pacific Northwest National Laboratory, draft. June 1997.

13 Dr. M.E. Agudo. Assessment of Electric Power Control Systems Security. Report by the Joint Program Office for Special Technology Countermeasures. September 30, 1996.

14 ISO standards for ODP ISO/IEC 10746 ITU X.900.

15 R. Masiello. Testimony Before the House Committee on Commerce. ABB Inc. September 5,1997.

16 Paulk, Mark et al. A Capability-Maturity Model for Software. CMU/SEI-91-TR-24, ADA 263403. 1993.

17 S. Trost. Tools for 21st Century Infrastructure Protection. Center for Global Security Research. July 1997.

18 Commercially Oriented Functionality Class for Security Evaluation. European Computer Manufacturers Association Standards, ECMA-205.

19 Roger Molander, Andrew Biddile, Peter Wilson. Strategic Information Warfare: A New Face of Warfare. RAND MR-661-OSD. 1996. <http://www.rand.org/publications/MR/MR661/MR661.pdf>

20 S. J. Lukasik. Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure. Center for International Security and Arms Control. Stanford University.

21 B. Biddle. Public Key Infrastructures and Digital Signature Legislation, 10 Public Policy Questions. The Seventh Conference on Computers, Freedom and Privacy, CFP 97.

22 S. D. Crocker. Payment Systems Security in Cyberspace. CyberCash, Inc.

glossary & acronyms

ANSI American National Standards Institute.

Availability Properties that specify limits on the extent of disruption of service.

CCITT Committee Consultative International Telegraph and Telecommunications - A committee of the United Nations which recommends international communications standards.

Confidentiality Properties that specify limits on access to information.

Control center An operational hub of the power system where decisions are made regarding which generation is scheduled and how high voltage transmission systems are to be operated.

Cyber The colloquial term for information networking.

DARPA Defense Advanced Research Projects Agency.

Distribution That portion of the power system that delivers power from a substation towards the customer usually in the range of 2 to 69 kV.

DoD US Department of Defense - The primary agency with responsibilities for military preparedness.

DOE US Department of Energy. The agency with responsibility for the nation's energy systems.

Encryption The technique for rendering plain communications indecipherable (Also see the word "key").

EPRI The Electric Power Research Institute - The primary entity who conducts research on behalf of the utility industry.

FACTS Flexible AC Transmission System - The name given to a family of high-voltage electronic controllers.

FEMA Federal Emergency Management Agency.

FERC Federal Energy Regulatory Commission - The primary agency responsible for the interstate aspects of the power system.

Generation The technologies involved in the conversion of some form of energy into electricity, includes fossil, nuclear, wind, solar, photovoltaic, and natural gas among others.

HVDC High-voltage direct current transmission.

IETF Internet Engineering Task Force - The organization that moderates the development of " standards" used by the Internet.

Integrity Properties that specify limits on modification of information.

Internet A worldwide network used for computer-to-computer communications that is rapidly growing as a ubiquitous utility for information access.

ISO Independent System Operator—In a restructured environment, the ISO manages power transactions to ensure power generation meets load demand requirements.

Key The code needed to decipher encrypted information.

Long term In this roadmap, 6 to 15 years.

MEI Minimum Essential Infrastructure - A concept that suggests that for each of the essential infrastructures of the nation there is a minimum configuration which is required for the public good.

Mid term In this roadmap, 3 to 6 years.

NERC North American Electric Reliability Council - An organization established by the utility companies to set recommended standards of reliability for the nation's power system as a whole.

glossary & acronyms

NIST National Institute of Standards and Technology.

NSA National Security Agency.

NSF National Science Foundation.

NSTAC National Security Telecommunications Advisory Committee.

OASIS Open Access Same-time Information System – A FERC mandated process and software application by which transmission system operators publish their available transfer capacity using internet technologies.

Open Open as applied to information systems are standards defined in such a way as to permit competitive use. Compare with system designs which give a vendor competitive advantage.

PCCIP President's Commission on Critical Infrastructure Protection - A commission established to recommend actions to protect eight critical infrastructures including the Electric Power Infrastructure.

Prosperity Games™ Exercises designed and operated by Sandia National Labs that explore strategic issues in a multiparty interactive setting.

Protocols When applied to information systems are the communications rules that enable heterogeneous systems to exchange data.

PUC Public Utility Commissions.

RAND A nonprofit institution that improves public policy through research and analysis.

Real time A general term used to mean that information can be acted on in a manner that can affect events as they occur.

SCADA Supervisory Control and Data Acquisition – An information system used to collect control and status data in the electric power, and oil and gas industries.

Security The protection of information when used in an information sense. The stability of the power system when used to describe power system operations.

Security policy A statement that governs acceptable system and human behaviors.

Subsidiarity A concept that determines the contemporary sharing of responsibilities and roles of government. <http://www.law.harvard.edu/groups/jmpapers/schill/>

Tools Software that uses advanced algorithms to augment human decision making.

Transmission The high-voltage part of the power system transmission network. Typically running between large generators and distribution substations and usually in the range of 69 to 765 kV.

WAMS Wide Area Measurements System - A joint research project between industry and the DOE to advance the state of real-time management of the grid in the Western states.

WSCC Western Systems Coordinating Council - The NERC western region council.

Year 2000 Refers to the anticipated malfunction in computer code that will occur when the date changes to the year 2000.

participants

To develop this roadmap a long list of volunteers gave freely of their time and expertise. The intention was to gain as many viewpoints as possible and to distill from them a representative document rather than a consensus. All views were expressed as individual contributions and not as official statements by their companies. Some individuals who contributed have chosen not to be listed as participants, which in no way diminishes the value of their input.

CHAMPION

Ronald L. Skelton, C.Eng. F.I.E.E.
Electric Power Research Institute

PARTICIPANTS

Robert H. Anderson, Ph.D.
RAND

Arnold B. Baker Ph.D.
Sandia National Laboratories

Judith A. Browne
Duke Power

Michael L. Cohen, M.S.,M.A.,Ph.D.(ABD)
The MITRE Corp.

Linda L. Folks CPA,CISA
Tennessee Valley Authority

Stephen Gehl, Ph.D.
Electric Power Research Institute

Ronald A. Gove, Ph.D.
Science Applications International Corp.

Ali Ipakchi
ABB Inc.

Karl Levitt
U.C. Davis

Teresa Lunt
DARPA

Roy Maxion
Carnegie Mellon University

I. Paul McCurley
Edison Electric Institute

Lee Metcalf
Houston Light and Power

Charlotte A. Quigley
Consolidated Edison of N.Y.

Robert B. Stuart
Pacific Gas & Electric

Fred H. Walsh
Tennessee Valley Authority

Stephen Walsh
Department of Defense

Richard E. Weiner, P.E.
Science Applications International Corp.

US Oil and Gas Infrastructure Strategic Roadmap

The US Oil and Gas Infrastructure is vital in supplying energy to all other critical infrastructures and to the American public. With estimated annual revenues totaling nearly $400 billion, the continued surety of this infrastructure is also of vital importance to our economy. Our reliance on the Oil and Gas Infrastructure is ever increasing for transportation and through our rapid evolution to a more technology dependent world. While technology continues to enhance our lives, it also increases our dependence on electric power, and thus on oil and natural gas as some of the fuels for electricity generation. Oil also continues to be widely used for other numerous industrial and commercial applications.

The Oil and Gas Infrastructure has experienced a variety of changes during the past few decades, including emerging new technologies, declines in domestic oil production, increased security risks, domestic reductions in crude oil and product inventory levels, and restructuring of the natural gas industry. Fortunately, the infrastructure has managed to avoid any significant repercussions from these changes. However, to better prepare the infrastructure for future challenges, we must identify and prioritize the risks to the Oil and Gas Infrastructure. Once this is accomplished, we can devise comprehensive surety strategies. This roadmap, therefore, is provided in this effort to preserve the surety of the Oil and Gas Infrastructure.

DESCRIPTION

The Oil and Gas Infrastructure is vital to the security, economic prosperity, and social well being of our nation.

The US Oil and Gas Infrastructure is a vital component in maintaining the security, economic prosperity, and social well being of our nation. It fuels the public and private sector motor vehicles needed to transport the people, products, and supplies that keep our economy and defense strong, and our communities close. It provides the fuels to generate some of the electric power used to run the enormous amount of electronic and computer equipment we rely upon. We rely on the Oil and Gas Infrastructure for producing, refining, distributing, and marketing end products such as diesel fuel, gasoline, jet fuel, distillate and residual fuel, petrochemicals and polymers, and petroleum products. Many of these products we have come to expect and rely on so much are often taken for granted.

INFRASTRUCTURE INTERDEPENDENCIES AND COMPLEXITIES

This infrastructure is vulnerable to physical and economic threats.

Historically, the US Oil and Gas Infrastructure has had two major categories of threats: physical and economic. Physical threats cover the spectrum, from malicious attacks to natural disasters to human error. Incidents from these threats have been rare, although sometimes the incidents have had profound public responses, such as oil tanker accidents. The most common physical threat to the Oil and Gas Infrastructure has been inadvertent damage to buried cables or pipelines, but this may not always be the case as energy supplies become more critical to all other infrastructures. Economic threats are intimately meshed with the stability of the top oil and gas producing countries and regions, as well as with the social, economic, and environmental priorities of the American public. Unfortunately, these threat categories are continually changing with the evolution of technology and increased system complexities, warranting a stakeholder-wide re-evaluation of the Oil and Gas Infrastructure's surety protection.

Massive amounts of critical data are sent over public networks, and surety must be evaluated.

The Oil and Gas Infrastructure's ever-increasing use of computers and information systems for managing and controlling industry assets has improved capabilities and efficiencies. However, the risks associated with the increased use of these information and control systems need to be evaluated. Massive amounts of industry information are routinely transferred over the Internet or other common communications media for routine business transactions. Critical control and status data is acquired over Supervisory Control and Data Acquisition (SCADA) systems utilizing proprietary communications networks and, in some cases, the Internet. These networks and information systems are even more critical because they are the only feasible way to effectively

control and monitor the industry's miles of pipeline and other vast resources. These information systems can often be vulnerable to malicious physical and cyber attacks, especially from insider threat. Information surety must be incorporated into these networks and information systems to better protect the Oil and Gas Infrastructure against these vulnerabilities.

The Transportation Infrastructure has always been critical to the movement of oil and gas commodities. Although pipelines distribute a considerable portion of oil and gas to users within the US, other transport means are also utilized to supply remote customers and to import these fuels from overseas. Furthermore, the Transportation Infrastructure is the biggest customer of oil products, putting even more emphasis on the importance of the interdependencies between these two infrastructures.

Transportation and Electric Power infrastructures are interdependent with the Oil and Gas Infrastructure.

The Electric Power Infrastructure is also mutually dependent with the Oil and Gas Infrastructure. Oil and gas are two important fuels for electric power generation. As the Oil and Gas Infrastructure increases its use of computer related technologies, its reliance on electricity, and therefore on the Electric Power Infrastructure, will continue to increase.

OIL SECTOR ISSUES

World oil demand is expected to grow substantially over the next 20 years. There are a range of predictions about the sufficiency of the world oil supply, but most forecasts point to a declining world oil production starting in the 2010 to 2015 time frame. In any case, the US has increasing vulnerability to oil supply disruption. The US consumes almost twice as much crude oil as it produces, and consumption and imports are projected to increase. Transportation fuels account for the majority of US petroleum use, and currently there is virtually no alternative. Our national dependence on oil has therefore made us a major oil importer and potentially vulnerable to the volatility of the world oil market.

Our national dependence on imported oil makes us vulnerable to world market fluctuations.

Today's worldwide crude oil infrastructure is increasingly dynamic with new suppliers from developing countries. A concern is that the governments of many of these new suppliers may become unstable, affecting production volumes and complicating assessments of the impact on the US Oil and Gas Infrastructure.

The instability of some foreign suppliers complicates production and supply assessments.

Technically recoverable crude oil reserves in the US are estimated to be about six times more than the proven reserves, offering some optimism for domestic oil production. While the US is the most intensely explored and developed oil-producing nation in the world, the US share of world oil reserves is only about 2 percent. The Gulf of Mexico and the Alaskan offshore reserves are the two primary reserves open to exploration.

The US share of world oil reserves is only 2 percent.

US refiners store oil and gas products to ensure a constant supply to consumers.

Over the last two decades, the number of US refineries has decreased significantly. Large, new refineries are not expected to be built in the US because of the current over-capacity of US refineries. Therefore, the cost of building new refineries within the US has not been economically justifiable. Refiners keep crude oil, distillate, and gasoline stocks on hand to ensure a constant flow of product to customers. The risks associated with not maintaining supplies include embargoes, strikes, and logistical problems in production, pipelines and tanker/barge movements. Inventory levels are currently guided by efforts to reduce life cycle cost through anticipation of market demands, reduction of storage, adjustment of feedstock supply streams due to seasonal and market variations, and reduction in storage costs.

The SPR effectively minimizes disruption.

The Strategic Petroleum Reserve (SPR) is one of the cornerstones of US energy policy and remains an effective policy tool in minimizing the dislocations to the US economy that would result from a sudden disruption in the international flow of oil. The presence of the SPR affords the administration important diplomatic flexibility to assess supply disruption in a calmer environment. Moreover, the mere presence of the SPR may prevent foreign government action aimed at the US.

NATURAL GAS SECTOR ISSUES

The extensive gas pipeline network depends on information systems and is vulnerable to cyber attacks.

The US depends on natural gas for approximately 24 percent of its energy requirements, with most of the fuel supply coming from domestic resources. This dependence is expected to continue increasing because of its affordability, ease of transport and distribution, and environmentally attractive combustion characteristics. Many of our northern states continue to rely on natural gas imported from Canada; pipeline connections from the gas-rich southwest and Gulf of Mexico regions are still expanding. In general, the extensive interconnectedness of natural gas pipelines allows for movements of large fuel supplies over vast areas while providing an inherent capability to recover quickly from major disruptions. However, this recovery capability increasingly relies on computerized monitoring and control, and information systems to manage an effective response, making the protection of cyber vulnerabilities critical to the surety of the infrastructure.

As a highly competitive industry, the gas infrastructure depends on information surety.

The natural gas sector has been undergoing regulatory restructuring for the past 20 years, similar to the transition now being experienced by the electric power industry. This transition has resulted in a competitive market that has influenced technology application, industry flexibility, and reduced prices, offering both benefits and disadvantages to the industry. Information is essential for the competitive market. Accurate and up-to-date information on weather, prices, supplies, consumption, and inventory is needed to make informed decisions on a daily basis. With millions of dollars being traded based on this information, lack of reliable, comprehensive data can be very costly.

TECHNOLOGY AND POLICY OBJECTIVES

The Department of Energy (DOE) Comprehensive National Energy Strategy (1998) proposes five major goals to secure the US energy, environmental, and economic futures. These goals are:

I. IMPROVE THE EFFICIENCY OF THE ENERGY SYSTEM

II. ENSURE AGAINST ENERGY DISRUPTIONS

III. PROMOTE ENERGY PRODUCTION AND USE IN WAYS THAT RESPECT HEALTH AND ENVIRONMENTAL VALUES

IV. EXPAND FUTURE ENERGY CHOICES

V. COOPERATE INTERNATIONALLY ON GLOBAL ISSUES

The following roadmap outlines key technology and policy objectives to be addressed over the next 15 years. This roadmap primarily addresses Goal II: Ensure Against Energy Disruptions, although some of the objectives crosscut all of the Comprehensive National Energy Strategy goals. In terms of assuring supply, DOE (1997) has described its research and development objectives for national oil and gas programs. These R&D objectives were used as a guide for defining the following technology and policy objectives.

1. REDUCE THE VULNERABILITY OF THE US ECONOMY TO DISRUPTION IN OIL SUPPLY.

2. ENSURE ENERGY SYSTEM RELIABILITY, FLEXIBILITY, EMERGENCY RESPONSE, AND EMERGENCY CAPACITY.

3. IMPLEMENT AN INDICATIONS AND WARNING SYSTEM FOR THE OIL AND GAS INFRASTRUCTURE.

TECHNOLOGY AND POLICY ROADMAPS

The requirements critical to achieving each of the objectives are described in the following tables and text.

OBJECTIVE 1: REDUCE THE VULNERABILITY OF THE US ECONOMY TO DISRUPTION IN OIL SUPPLY.

A variety of technologies can improve domestic oil production.

This objective should be met through a combination of strategic positioning and adoption of advanced technologies. This approach will allow us to maximize our domestic oil production efficiency and reduce the risks associated with importing oil.

A variety of technologies can be used to improve domestic oil production efficiency and capability. Developing a portfolio of these technologies must be a priority for industry and government so we can enhance domestic oil production in diverse and challenging geologic environments. Some examples of these technologies include:

- Improved computer imaging technologies for locating and identifying oil and gas reservoirs in geologically complex settings or in deeper and smaller compartmentalized reservoirs
- Advanced drilling and extraction technologies to boost recovery from mature reservoirs and reduce exploration costs
- Technologies that will help industry meet environmental regulations while reducing the cost for compliance
- Improved delivery and storage technologies to help ensure a safe, reliable, and cost-effective supply of gas and oil

Approximately 70% of the world's oil is produced in the Persian Gulf region. Diversification and proactive development of other sources would reduce risks and instabilities associated with a high dependence on one region. The Caspian Sea is one of the oil sources with great oil producing potential. Other sources should also be investigated.

OBJECTIVE 1: Reduce the vulnerability of the US economy to disruption in oil supply.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Improved imaging technologies Advanced drilling technologies and extraction technologies Environmental technologies Improved delivery and storage technologies	Domestic oil production maintained at the maximum efficient level	Exploration and development active for 1 to 5 years, limited long term R&D	Re-evaluate existing reserves using state-of-the-art technology Increased availability and use of subsurface geologic data Assist industry with developing a portfolio of technologies for production in diverse geologic environments	Develop, demonstrate, and deploy new technologies to reduce cost and improve productivity of oil and gas wells Increased use of advanced geophysical imaging to define drilling location Increased use of advanced logging and wellbore geophysics	Increased discoveries of new domestic oil and gas fields Increased reserve growth rate in existing fields Increased volume of "booked reserves" per new wells
Diversify sources of oil available to world markets	Stability of oil price and supply	70% of world oil production is in the Persian Gulf region 50% of the US imported oil is produced in the western hemisphere	Promote expansion of oil supply from other sources such as Caspian Sea	Development of regional energy cooperation agreement	Flexible portfolio of available oil and gas import sources
Maintain readiness to address threats and disruption to world oil and gas supplies	Minimal impacts from disruptions	SPR currently developed and monitored	Maintain the existing SPR sites and inventory in drawdown-ready conditions, including investments in the facility and equipment life-extension programs	Facility life-extension program complete	Equipment life-extension program complete

The US Oil and Gas Infrastructure stakeholders must maintain a coordinated readiness to address threats and disruptions to world oil and gas supplies. The SPR is a key tool in this effort. The SPR inventory must be kept at adequate levels and in drawdown-ready condition. Support of the facility and equipment life-extension programs will improve the existing capabilities offered by the SPR and by oil and gas reservoirs in general. These programs extend the life of drilling equipment and reservoirs, thereby reducing premature well abandonment and avoiding technical and financial challenges associated with locating and drilling new wells.

The SPR must be kept at adequate levels and drawdown-ready.

OBJECTIVE 2: ENSURE ENERGY SYSTEM RELIABILITY, FLEXIBILITY, EMERGENCY RESPONSE, AND EMERGENCY CAPACITY.

The Oil and Gas Infrastructure is an important element of the US energy system. We must therefore align the Oil and Gas Infrastructure objectives with national energy policy and technology objectives. This includes taking into account the relationship between oil and gas and electric power for improved surety of electricity generation. Three goals that will strive toward meeting this objective include:

- improving the reliability and flexibility of electricity generation, transmission, and distribution,
- improving the reliability and flexibility of domestic oil refining, transportation, and storage,
- improving the reliability and flexibility of natural gas transportation, and storage.

This objective also encompasses three additional important and integrated goals:

- conduct formal industry-wide consequence based risk assessments,
- protect vulnerable interdependencies with other infrastructures, and
- improve existing data collection systems

CONDUCT FORMAL INDUSTRY-WIDE CONSEQUENCE-BASED RISK ASSESSMENTS

A formal, comprehensive assessment is needed to evaluate potential vulnerabilities and consequences at all levels.

Risks to the Oil and Gas Infrastructure must be captured using a structured qualitative risk assessment process. Impacts to the US infrastructure should be analyzed in terms of both near- and long-term effects and consequences, addressing risk mitigation and prevention recommendations. Although some informal risk assessments are currently conducted at the industry, international, national, state, county and municipal levels, there is no risk assessment that involves stakeholder members at all levels. A formal, comprehensive assessment is needed to evaluate potential vulnerabilities and consequence scenarios at all levels of the infrastructure. Protection options can then be more effectively prioritized and selected. Economic impacts should be the focus to provide incentives for industry participation and support. However, environmental and legal issues must also be of high priority.

With the advance of technology, and corresponding automation and remote monitoring, major facilities are run during nights and weekends with minimal personnel, resulting in a need for increased security monitoring. Threat profiles in risk evaluation must include insider threat, sabotage, environmental terrorism, financial manipulation, and political posturing using oil and gas as a tool or weapon. These threat categories are critical.

OBJECTIVE 2: Ensure energy system reliability, flexibility, emergency response, and emergency capacity.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Improve the reliability and flexibility of electrical generation, transmission, and distribution	Stability of price and supply of electrical power	Electric power industry undergoing restructuring	Reliability standards established	Reliability standards enforced	Flexibility in sources including renewable, nonrenewable, etc. Reducing environmental impact through improved efficiency and new technologies
Improve the reliability and flexibility of domestic oil refining, transportation and storage	Stability of price and supply for electrical power	DOE has an unique suite of oil, gas, and programmatic models	Maintain existing simulation capabilities Best approaches to enhance security selected	New processing and low emission technologies to lower environmental costs Models to analyze impact of oil and related environmental programs on production and utilization Coordinated effort to protect the infrastructure initiated	Integration of DOE's oil and gas models Coordinated effort to protect the infrastructure in place
Improve the reliability and flexibility of natural gas transportation and storage	Stability of price and supply for electrical power	DOE has an unique suite of oil, gas, and programmatic models	Develop improved gas flow measurement and energy measurement technologies Best approaches to enhance security selected	Improve methods and lower costs for storage Emission detection technologies developed and demonstrated Models to analyze impact of gas and related environmental programs on production and utilization Coordinated effort to protect the infrastructure initiated	Develop advanced storage to meet the needs of industrial and power generation markets Integration of DOE's oil and gas models Coordinated effort to protect the infrastructure in place
Conduct formal industry-wide consequence-based risk assessments	Industry-wide acceptance and participation in assessments	DOT, DOE, USGS, MMS, and industry groups have made assessments Some data available	Assemble industry-wide risk assessment team Define risk criteria Begin high level risk assessments	Perform detailed level risk assessments Prioritize industry-wide risk protection Identify collaborations and funding	Implement risk protection plan Periodically update risk assessments

PROTECT VULNERABLE INTERDEPENDENCIES WITH OTHER INFRASTRUCTURES

Computer modeling and simulation will be needed to assess the complex interdependencies between critical infrastructures.

Interdependencies between infrastructures have not been addressed in the past. However, these ever-increasing complexities are becoming cause for concern. An industry-based assessment is needed to identify interdependencies within the infrastructure. This should then be followed by a multi-infrastructure assessment to identify interdependencies between and among the critical US infrastructures. Collaborations and alliances can then be formed to develop a strategy for protecting those interdependencies that are found to be critical and vulnerable. The historic lack of knowledge about interdependency issues will require the development and assembly of a suite of modeling and simulation tools that can be used to model various disruption scenarios and protection options.

IMPROVE EXISTING DATA COLLECTION SYSTEMS

Although considerable data are gathered, new metrics need to be formed to assess risks.

The Mineral Management Service (MMS), US Geologic Survey (USGS), Department of Transportation (DOT), DOE Energy Information Administration (EIA), American Petroleum Institute (API) and other industry groups currently have metrics to collect, correlate, and publish considerable data on the worldwide Oil and Gas Infrastructure, including reserves, production, consumption, and imports. The adequacy of these current methods needs to be evaluated. An adequate system would include structured and timely notification when significant Oil and Gas Infrastructure risks appear. We must develop new metrics and redefine and categorize existing metrics so that quantification of risks to the Oil and Gas Infrastructure can be statistically and objectively determined and correlated. These risk assessment metrics should be incorporated into the existing EIA oil and gas measurement system with predetermined, timely, congressional notification when these metrics indicate that significant risks to the Oil and Gas Infrastructure are anticipated. An application where risk metrics and thresholds are needed is in monitoring the rate of domestic oil production coupled with the rate of imports and consumption. When these rates reach predetermined levels, appropriate actions could be selected from a preplanned portfolio of options. Options could include congressional and/or presidential briefings by the Secretary of Energy, or the implementation of predetermined consumption constraints.

OBJECTIVE 2: Ensure energy system reliability, flexibility, emergency response, and emergency capacity (continued).

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Protect vulnerable interdependencies with other infrastructures	Widespread industry knowledge and protection of interdependencies	Very little knowledge or protection of interdependencies	Perform high level analysis Identify areas needing further analysis Specify modeling and simulation tools needed for further analysis Form an industry-based interdependencies forum	Collaborate with other infrastructures to protect vulnerable interdependencies Develop modeling and simulation tools	Conduct periodic assessments of interdependencies Use modeling and simulation tools
Improve existing data collection systems	Widespread use of data collection metrics	DOT, DOE, USGS, MMS, and industry groups have made assessments; systems not adequate	Set standards for data collection systems	Link quality assurance to continued legislative action	Implementation and continuous improvement of all risk assessment data systems and criteria

OBJECTIVE 3: IMPLEMENT AN INDICATIONS AND WARNING SYSTEM FOR THE OIL AND GAS INFRASTRUCTURE.

DESIGN AN INFRASTRUCTURE-WIDE INDICATIONS AND WARNING ARCHITECTURE

A new communications structure needs to be developed for real-time assessments.

The existing Oil and Gas Infrastructure does not share information well. Instead, communication and information systems have tended to be custom designed, and in some cases proprietary. Furthermore, high-level information databases have traditionally been assembled through survey forms distributed by the DOE EIA. This type of database accommodates long-term planning and trend identification, but does not address more real-time concerns like pipeline leaks or oil tanker accidents. An indications and warning architecture is needed to facilitate information sharing and industry coordination on a more timely basis. Such an architecture could also facilitate correlation of industry-wide events for identifying and locating malevolent threats.

IMPLEMENT INDUSTRY-WIDE INFORMATION SURETY STANDARDS

Standards would improve communications with other infrastructures.

There is a need for industry to share secure information on a frequent basis to be able to conduct daily business and address infrastructure-wide threats in a more coordinated and timely manner. This could prove especially useful in communicating with other infrastructures. At a minimum, information surety standards for consistent protection of vital infrastructure information must be implemented. SCADA systems could benefit immediately. These systems are widely used in the industry to pass control and status information; however, adequate surety has not necessarily been included in their design. Secure SCADA protocol and authentication standards would greatly enhance information and infrastructure surety.

IMPLEMENT TECHNOLOGIES FOR IMPROVED INFRASTRUCTURE SURETY

Advanced sensor and monitoring technologies would be highly useful for pipeline protection.

The sheer size of the Oil and Gas Infrastructure and its many miles of pipelines make it physically impossible to know the status of all of its critical nodes without the aid of technology. More advanced and sophisticated technologies are needed to gather and correlate information and to prevent and clean up environmental hazards. In particular, the implementation of advanced sensor and monitoring technologies would be very beneficial to pipeline protection. In addition, advanced environmental clean-up technologies are needed to better contain and clean spills and hazards, and to minimize impacts to the environment.

OBJECTIVE 3: Implement an indications and warning system for the Oil and Gas Infrastructure.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Design an infrastructure-wide indications and warning architecture	Widespread use and acceptance of architecture	Proprietary, nonstandard systems used by industry	Obtain industry support Identify information requirements	Begin implementation of information standards Integrate regional level indications and warning systems	Integrate national level indications and warning system
Implement industry-wide information surety standards	Information surety standards widely accepted and used	None exists	Identify information surety requirements Begin defining information surety standards	Information surety standards completed and industry use begins	Information surety standards widely accepted and used Continue updating surety standards as needed
Implement technologies for improved infrastructure surety	Widespread use of surety technologies	Limited use of surety technologies	Identify surety requirements Identify existing technologies Implement applicable technologies Specify requirements for new technologies	Develop new surety technologies as needed Incorporate surety specifications in the long-term infrastructure development	Widespread use of surety technologies Continually incorporate surety into infrastructure development

TECHNOLOGY AND POLICY DRIVERS

This roadmap, along with roadmaps by DOE Fossil Energy and Energy Research, describes approaches to address several of the DOE Comprehensive National Energy Strategy goals. Some fundamental drivers that will help meet these goals and that are critical to the future surety of the Oil and Gas Infrastructure follow:

- Implementation of additional information surety technologies and standards. Computer and communication systems are some of the most critical assets in managing the Oil and Gas Infrastructure, yet their vulnerabilities are some of the least understood and least protected. The infrastructure's reliance on these systems will only increase, requiring that attention and protection options be carefully evaluated in this area.
- More investments in the US Oil and Gas Infrastructure by the oil industry. The numbers are staggering in terms of the disparity between money spent by oil companies on development and investment overseas compared to domestic investment. Economic incentives are needed to divert more of industry's interest to infrastructure surety.
- A petroleum industry risk management process. There is no codified or structured petroleum industry risk management process upon which to evaluate risks to the petroleum infrastructure.

OPPORTUNITIES AND SHOWSTOPPERS

There are many opportunities to improve the surety of the Oil and Gas Infrastructure and very few showstoppers.

OPPORTUNITIES

- Use national and international environmental policies to more effectively guide the infrastructure. In the Kyoto Protocol of early December 1997, US delegates agreed to a 7 percent cut in the 1990 levels of greenhouse gases by the years 2008 to 2012. If the treaty is approved and implemented, it could have a major impact on the Oil and Gas Infrastructure by possibly re-evaluating the appropriate mix of fuel types for the generation of electrical power, encouraging development of more fuel-efficient automobiles, petro-chemical and greenhouse gas producing plants moving to developing countries not participating in the treaty, and ending subsidies that keep fossil fuel costs low. We must take full advantage of policies like this to strengthen and guide the infrastructure, rather than respond to them as obstacles and oppositions.
- Review, evaluate, benchmark, and re-engineer, as appropriate, existing regulations, policies, laws and codes to promote conservation of petroleum products. Many of the existing regulations, policies, laws and codes were enacted when petroleum imports were lower, and without benefit of new technological advances. Approximately two-thirds of the US petroleum products are consumed in transportation. A periodic review and update may reduce the vulnerability to the Oil and Gas Infrastructure by facilitating conservation. We can propose these changes in the form of revisions to, or new, regulations, policies, laws, and codes, as appropriate.
- Develop a baseline infrastructure surety policy suitable for national and/or international adoption. There are no formally structured systems or existing metrics to objectively quantify surety risks to the Oil and Gas Infrastructure. Wide variation exists in similar US petroleum facilities because they are largely dependent on resident expertise and allocated budgets; no consensus standards exist.

SHOWSTOPPERS

- Industry does not seem to be convinced that improved infrastructure surety is a major concern. Furthermore, investments in infrastructure surety must be economically attractive, either as near-term preventive measures or as long-term cost savings investments. Government has been leading the infrastructure surety effort and must make an economic case to industry to obtain better support and buy-in.

SOURCES

DOE. *Comprehensive National Energy Strategy: National Energy Policy Plan, Pursuant to Section 01 of the Department of Energy Organization Act.* Washington, DC. April 1998.

DOE. *Oil and Gas R&D Programs: Securing the U.S. Energy Environmental and Economic Future, Office of Fossil Energy, Office of Natural Gas and Petroleum Technology,* Washington, DC. March 1997.

Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. October 1997.

American Petroleum Institute publications

- *International Comparisons of Energy - Gross GNP Ratios.* R31108.
- *World Petroleum Supply, history, prospects, and policy issues.* R80010.
- *Are We Running Out of Oil?* R00135.
- *Oil Industry Participation in Emergency Planning.* R52800.

US Strategic Petroleum Reserve More Important Than Ever/Risks to Global Crude Oil Flow Sustain Need for Strategic Reserve. Oil and Gas Journal. Vol. 95, No. 37, pp. 20. September 15, 1997.

US DOE Energy Information Administration publications

- *Petroleum 1996: Issues and Trends, Office of Oil and Gas.* September 1997.
- *Natural Gas 1996: Issues and Trends, Office of Oil and Gas.* September 1997.
- *Natural Gas Monthly, Office of Oil and Gas.* January 1997.

Strategic Petroleum Reserve Annual Report for Calendar Year 1996. US DOE Assistant Secretary for Fossil Energy, Office of Strategic Petroleum Reserve.

Strategic Petroleum Reserve Annual Report for Calendar Year 1997. US DOE Assistant Secretary for Fossil Energy, Office of Strategic Petroleum Reserve.

glossary & acronyms

API	American Petroleum Institute
API gravity	Measures crude oil density or specific gravity. A high gravity crude is "light" and a low gravity crude is "heavy." A light crude yields more light products than heavy crude.
BPD	Barrels per day
CQI	Continuous Quality Improvement, or Total Quality Management (TQM)
DOE	Department of Energy
DOT	Department of Transportation
EA	Environmental Assessment
EIA	US DOE Energy Information Administration
EIS	Environmental Impact Statement
MMBD	Million barrels per day
MMB	Million barrels
MMS	Mineral Management Service
NYMEX	New York Mercantile Exchange
OPEC	Organization of Petroleum Exporting Countries
QA	Quality Assurance
SCADA	Supervisory Control and Data Acquisition
SPR	Strategic Petroleum Reserve
USGS	US Geologic Survey

participants

Mr. Tom Allen
SCIENTECH, Inc.
Vice President

Mr. Patrick Ward
SCIENTECH, Inc.
Project Manager

Mr. James K. Edwards, P.E.
SCIENTECH, Inc.
Consultant - Principal Investigator

Mr. Harry Leith
SCIENTECH, Inc.
Consultant

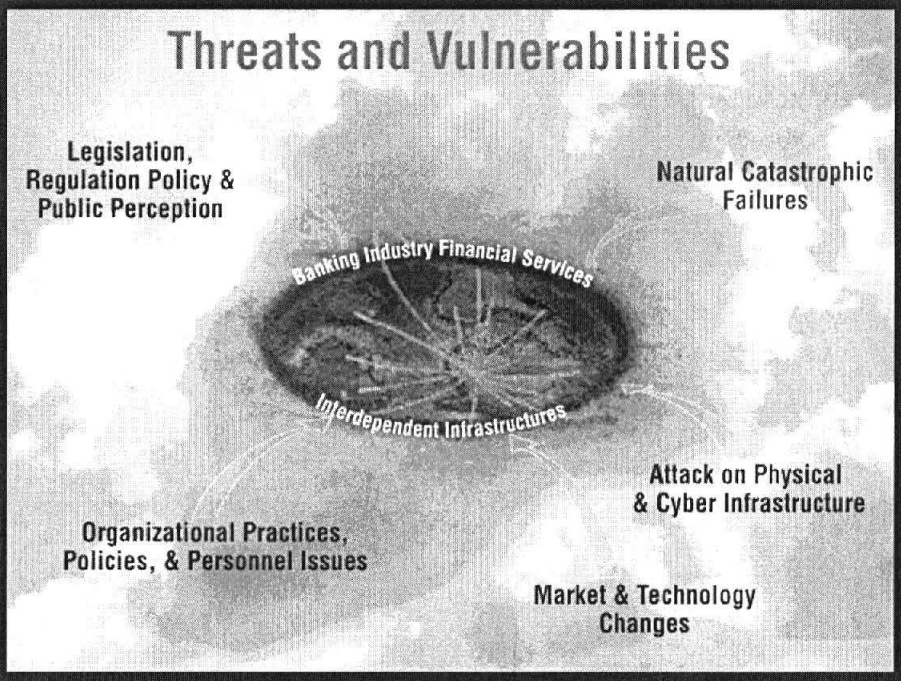
Mr. C. Curtis Johnson
CEO, DynMcDermott Petroleum
Operations Company

Mr. Charles L. Steinkamp, P.E.
Crude Oil Consultant

Mr. David Borns
Principal Member of Technical Staff
Sandia National Laboratories

US Banking Industry Financial Services Strategic Roadmap

Technology developments have had a profound impact on the US banking industry. Driven largely by competition, consumer acceptance, and cost reduction opportunities, the use of electronic means for information and value exchange is rapidly increasing. The ability to transact banking business anytime and anywhere is becoming a requirement for businesses and consumers alike. Electronic exchange through local area networks, wide area networks, and the Internet has created new possibilities and provides global access to banking information and services for business and consumers.



The US banking industry is simultaneously undergoing change caused by industry consolidations, increased competition, and increased reliance on suppliers of services such as telecommunications, third-party service providers, utilities, and transportation. All of these developments will create new risks for which the industry must be prepared.

The following technology and policy roadmap addresses the threats and vulnerabilities that could face the US electronic banking industry and offers solutions over the next 15 years to continue to ensure the industry's safety, soundness, and to maintain public confidence in it.

DESCRIPTION

The banking industry relies on advanced systems and processes.

It is recognized that the banking industry sector is among the most advanced in security measures of all the industry sectors. Its systems and processes protect operations from disturbances such as system failures, fraud and other crime, and internal and external attacks. Sustaining public trust in the safety of the banking system depends largely on these protections.

The current trend of mergers and acquisitions creates additional risks for both traditional banking and electronic commerce.

In the move toward electronic commerce, there are new threats and vulnerabilities that require assessment to safeguard this public trust. Increased dependence on suppliers such as third-party service providers, telecommunications networks, and the electric power industry, is one such new threat and vulnerability. Unknowns resulting from restructuring the electric power industry add ambiguity to dependence on this infrastructure. In addition, increased reliance on key technical personnel, as more business processes are computerized, creates potential exposure to insider attack. Changes underway in the industry's structure, including the current trend of mergers, acquisitions, and consolidation of operations centers, create additional risks for traditional banking in general and the electronic banking infrastructure in particular. Opportunities exist to identify solutions beyond traditional risk management methods, while continuously leveraging existing security architecture, where appropriate, to provide solutions that are cost-effective relative to the value of the systems being protected.

While current assessments show that the industry is prepared to handle these security challenges, efforts must continue to ensure ongoing interoperability, efficient and secure transaction handoff from one party to another, and overall safety and soundness of the electronic infrastructure. In addition, challenges resulting from new infrastructure features, dependence on technology providers, energy providers, the networks themselves, and transnational threats of all kinds need to be addressed in coordination with government and private sector organizations to ensure effective risk management.

To address these critical issues, Sandia National Laboratories engaged the Banking Industry Technology Secretariat (BITS), a subsidiary of The Bankers Roundtable, whose membership is reserved for the senior executives of the 125 largest bank holding companies in the US. BITS assembled a team of key stakeholders with expertise in critical areas of electronic banking, security, and computer technology to identify the threats and vulnerabilities facing the industry and to develop a roadmap to create strategies for action in the protection of US electronic banking infrastructure. Four major objectives, critically linked and interrelated, were identified and outlined in this report and appear here in priority order. It was agreed that coordinated efforts between government and private industry represented the most important step in successfully addressing the threats and vulnerabilities.

Coordinated steps between government and private industry are essential for effective risk management.

CURRENT INDUSTRY EFFORTS

Various government and private sector organizations are addressing security issues facing the US banking and finance industry. These include but are not limited to: the American Bankers Association (ABA), American National Standards Institute (ANSI), the American Society for Industrial Security (ASIS), BITS, the Computer Emergency Response Team (CERT), the Federal Reserve System, Internet Engineering Task Force (IETF), the National Security Telecommunications Advisory Committee (NSTAC), the Financial Services Technology Consortium (FSTC), and the President's Commission on Critical Infrastructure Protection (PCCIP). The Forum of Incident Response and Security Teams (FIRST) is an umbrella organization. See http://www.first.org/team-info/ for a directory of many allied groups.

Other efforts have been implemented to address the secure transmission of transactions over open networks such as the Internet. For example, Visa, MasterCard, and the vendor community produced the Secure Electronic Transmission Protocol (SET) standard that uses digital certificate technology to authenticate the parties in a payment transaction. Major banks and technology providers are collaborating to develop open standards, such as the Open Financial Exchange (OFX), for bill presentment, on-line bill payment, and other services. Standards for automatic teller machines (ATMs) are also being pursued.

Many major banks and technology providers are collaborating to develop open standards for secured transactions.

TECHNOLOGY AND POLICY OBJECTIVES

To derive the technology and policy objectives, it is important to define the risks that could impact the industry. The defined categories and corresponding threats and vulnerabilities are identified below:

THREATS AND VULNERABILITIES

Category 1. Natural or catastrophic failure:

- Earthquakes, floods or other natural disasters
- Failure of telecommunications networks and utilities

Category 2. Attack on physical and cyber infrastructure:

- Vandalism, sabotage, bombs, external or insider attack
- Viruses in telecommunications networks and computers
- Hackers accessing systems through the network

Category 3. Impact of market changes on the banking industry:

- Failure of suppliers
- Mergers and acquisitions
- Inability to respond to changes in a timely manner
- Unregulated entrants not meeting industry security standards

Category 4. Technology risk management:

- Inadequate end-to-end testing, including certification of unregulated service providers
- Technology changes, such as movement to distributed systems
- Lack of interoperability resulting from ambiguity among currently existing standards
- Not adapting legacy systems to meet new infrastructure requirements and other changes (e.g., year 2000 issues)

Category 5. Organizational practices, policies, and personnel issues for the changing environment:

- Not maintaining state-of-the art approaches to security
- Not integrating traditional physical security and systems security issues and practices
- Not ensuring adequate training and retention of personnel

- Not addressing personnel issues associated with external and internal security, insider attack, and impact of state laws/privacy issues
- Not standardizing security practices across bank branches, offices, and departments

Category 6. Legislation, regulation, policy, and preserving the public trust:

- Not maintaining consumer/public confidence and trust
- Not promoting appropriate legislation in banking and in other unregulated financial institutions

The resulting objectives developed to address these threats and vulnerabilities over the next 15 years are:

1. **DEVELOP A CRITICAL INFRASTRUCTURE INDICATIONS AND WARNING (I&W) CENTER. THIS CENTER SHOULD UNITE THE GOVERNMENT AND THE PRIVATE SECTOR TO COLLECT, ANALYZE, AND DISSEMINATE THREAT INFORMATION AND SECURITY LAPSES AND TO ESTABLISH SECURE COMMUNICATIONS CHANNELS TO MANAGE CATASTROPHIC FAILURES CAUSED BY NATURAL DISASTERS OR INTENTIONAL MALICIOUS ACTS. (THIS OBJECTIVE ADDRESSES THREATS AND VULNERABILITIES, CATEGORIES 1 AND 2.)**

2. **IMPROVE INTEROPERABILITY AND RISK MANAGEMENT ASSOCIATED WITH, AND IN ANTICIPATION OF, RAPID TECHNOLOGICAL AND MARKET CHANGES. SECURITY INTEROPERABILITY SHOULD BE INCLUDED WITH THIS OBJECTIVE. (THIS OBJECTIVE ADDRESSES THREATS AND VULNERABILITIES, CATEGORIES 3 AND 4.)**

3. **PREPARE BANKING INDUSTRY PERSONNEL FOR THE EVOLVING INDUSTRY. THIS SHOULD BE ACCOMPLISHED BY ESTABLISHING ADAPTABLE, EFFECTIVE SECURITY POLICIES AND PRACTICES AND BY PROVIDING APPROPRIATE TECHNICAL TRAINING. (THIS OBJECTIVE ADDRESSES THREATS AND VULNERABILITIES, CATEGORY 5.)**

4. **MAINTAIN SAFETY AND PUBLIC TRUST IN THE BANKING INDUSTRY. WORK WITH INDUSTRY PARTICIPANTS, REGULATORS, AND CONSUMER GROUPS TO ENSURE APPROPRIATE POLICIES AND PRACTICES ARE IN PLACE TO MAINTAIN SAFETY AND PUBLIC TRUST USING COST-EFFECTIVE SOLUTIONS. (THIS OBJECTIVE ADDRESSES THREATS AND VULNERABILITIES, CATEGORY 6.)**

TECHNOLOGY AND POLICY ROADMAPS

A list of the requirements and drivers that are necessary to meet the objectives in the near (0 to 3 years), intermediate (3 to 6 years), and far (6 to 15 years) term are presented in the tables that follow.

OBJECTIVE 1: DEVELOP A CRITICAL INFRASTRUCTURE INDICATIONS AND WARNING (I&W) CENTER.

Although rare, most industries face the risk of disruption of operations arising from natural disasters or intentional malicious acts against the cyber and physical infrastructures on which they rely. Because the banking industry is so dependent on outside resources, such as telecommunications, utilities, and transportation, additional steps should be taken to protect the industry from disruptions at these sources.

OBJECTIVE 1: Develop a critical infrastructure indications and warning (I&W) center.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Identify and evaluate the vulnerabilities of critical external infrastructure and internal resources	Interdependencies on external infrastructure identified Dependencies on internal resources identified Vulnerabilities identified and evaluated	President's Commission on Critical Infrastructure Protection (PCCIP) Infrastructure Protection Task Force (IPTF) Public sector efforts (e.g., FBI/DOJ, DOE) Private sector efforts (CERT, InfraGard)	Further development of government initiatives to cover all areas and infrastructure Facilitate formal and informal information sharing among multiple industries Conduct industry-wide study to evaluate existing resources, infrastructures, and interdependencies Evaluate and respond to the Presidential Commission Report recommendations Establish public/private sector working group to evaluate vulnerabilities, internal trends, resources and interdependencies in the banking industry	Public/private sector committee fully established and functional	Establish joint public/private sector methodology to collect, analyze and disseminate threat and vulnerability information

OBJECTIVE 1: Develop a critical infrastructure indications and warning (I&W) center (continued).

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Detect, collect, and analyze incident information or data	Standardized reporting system established Risk assessment completed Central indications and warning facility to compile and analyze data Trends identified Risk detection improved	Suspicious Activity Report (SAR) FBI - CIITAC IPTF NSTAC Air Force - ASIMS Formal and informal computer hardware and software industry and user groups	Achieve consensus between public/private sector on general infrastructure threats Establish industry anonymous database containing incident and vulnerability reports Develop computer anomaly detection tools Standardize reporting criteria of cyber intrusions in SARs	Establish joint public/private sector clearinghouse to collect, analyze and disseminate threat and vulnerability information	Automate communication process, improve intrusion detection process, and formalize analysis process
Disseminate threat information to industry to allow development of protection plans and communication with other infrastructure I&W centers	Industry-wide coverage achieved Protection for sensitive or classified information improved Communication channels among government and industry established Industry protection plan established Increased deterrence of incidents through prosecution	CERT Advisory System NSTAC InfraGard National Computer Security Association	Expand InfraGard or InfraGard-type organizations Establish private sector points of contact for disseminating information Review law enforcement policies that restrict threat information sharing Build secure communications channels with existing I&W centers Develop consequence models to help bring in protection planning	Establish joint public/private sector I&W centers to collect, analyze and disseminate information Change policies to facilitate sharing	Expand communications channels to include the international arena National cross-infrastructure indications and warning center established
Contingency planning and crisis management for critical infrastructure elements	Network components identified Central recovery capability established Expertise database established Alternate resource availabilities identified Emergency Response Team created Diversification plan in place	FEMA NTA NSEP	Develop plan for continuity of banking that identifies crisis management structure, roles, likely threats and contingencies, resources, expert data base, and next steps Study existing backup operations and identify potential weaknesses Coordinate with government efforts currently underway	Create robust infrastructure-wide crisis management plan Identify and establish recovery routing and resource alternatives	Continually revise continuity plans based on new technologies and standards Conduct disaster drills

This system will provide real-time indications and long-term trend information about disruptions.

A multi-industry I&W system would identify and classify threats and provide adequate information to industries to allow them to develop countermeasures to prevent, detect, and recover from cyber intrusions and physical attacks. In addition, this system would provide assistance and resources to halt, contain, and recover from a catastrophic event. Both real-time indications and long-term trend and correlation information about infrastructure attacks and disruptions are needed.

As indicated in the Strategic Roadmap, Objective 1 table, there are many technical attributes that will drive the success of this objective:

- Identification and evaluation of the vulnerabilities of interdependencies with other infrastructures, as well as identification of vulnerabilities to internal resources. This task will uncover the complexities resulting from the ever-increasing interdependencies on other infrastructures.
- Detection, collection, and analysis of incident information or data. Detection technologies and information systems will be key in providing the ability to acquire accurate, complete, and timely information regarding infrastructure attacks and disruptions. This information must then be organized and correlated for effective dissemination and response.
- Dissemination of threat information to industry to allow development of protection plans and communication with other infrastructure I&W centers. Timely dissemination of information will be critical to the success of this effort.
- Provision of contingency and crisis management plans. Cooperation among industry participants, as well as with government, is needed for effective preparedness planning.

OBJECTIVE 2: IMPROVE INTEROPERABILITY AND RISK MANAGEMENT ASSOCIATED WITH, AND IN ANTICIPATION OF, RAPID TECHNOLOGICAL AND MARKET CHANGES.

Security controls are struggling to keep up with rapid changes in banking and financial services.

Rapid technological changes can have profound and sometimes unexpected impacts on all aspects of the financial services industry. These changes include movement to open technologies, distributed systems, and virtually unlimited access, while system administrator and security controls in new operating systems struggle to keep up.

Rush-to-market could introduce flawed or inadequately tested systems.

Rapid market changes, such as banking industry mergers and acquisitions, can affect the national banking infrastructure. Rush-to-market and/or unmanaged change in critical infrastructure may introduce systems that may not be adequately tested or may not meet accepted security and

OBJECTIVE 2: Improve interoperability and risk management associated with, and in anticipation of, rapid technological and market changes.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Monitor changes in critical markets	Business environment changes identified and recognized	Individual industry efforts	Use public/private sector I&W centers to identify and report changes affecting the industry and infrastructure	Perform risk assessment and business impact of physical and cyber infrastructure threats	Improved monitoring techniques and ongoing assessment of changes
More timely development and heightened support of open security standards	Agreement on open security standards for new technologies before multiple variations are implemented in products in the marketplace Standards adopted that address, support or meet banking security requirements	ATM Forum T1S1 Internet Engineering Task Force World Wide Web Consortium SET Standard OECD standards NIST, NSA standards under development	Increase banking industry commitment of resources and participation in the national and international standards processes Develop industry criteria to guide development of market driven or de facto open standards Identify appropriate standards bodies to take on infrastructure issues (e.g., TFPC) Develop open/modular network architecture for the financial services industry	Improve collaboration among standards committees to speed issuance of open standards Develop banking regulations that promote open/extensible security standards	Increase collaboration among standards committees to expediently issue open standards Large-scale deployment of banking regulations that promote open/extensible security standards
Develop security criteria and guidelines for third-party suppliers	Comprehensive set of criteria established	Common Criteria CCS/SS7 security baseline Automotive industry action group requirements No industry-wide process; individual institution response	Evaluate current processes Expand on existing criteria and develop new ones as necessary Educate industry participants and third-party suppliers and promote criteria	Evaluate the criteria in terms of the evolution of technology and adjust as appropriate	Large-scale adoption of financial criteria
Verify compliance with criteria and open standards for banking organizations and third-party vendors	Degree of adoption and compliance	Various certification programs for security and interoperability	Survey existing programs Identify missing security criteria and open standards Include security requirements in contracts with vendors	Develop levels of compliance that institutions can select (e.g., self-certification, outside audit, guarantees) Cross-certification across industries	Refine and enhance compliance programs Large-scale compliance with criteria and open standards Investigate liability loss allocation schemes
Develop testing methodologies that successfully reduce security vulnerabilities and consequences	Fewer security vulnerabilities discovered in released networks and systems products	Somewhat ad hoc testing methodologies based on legacy systems Integration testing that tests for functionality, but not specifically for fewer vulnerabilities in new products or networks and in end-to-end service management AICPA	Institutionalize security vulnerability testing as part of normal system acceptance Establish industry-wide and cross industry testing mechanism, to certify information systems products Establish R&D to develop better network security design principles, including analysis of consequences	Develop automated testing and secure design methodologies for distributed systems Develop standardized security testing methodologies Implement security accreditation practices	Implement artificial intelligence and structured testing methodologies Develop certification of product design processes similar to ISO 9000
Build flexibility into technology to enhance security and to speed implementation of security features	Timely adaptation to new requirements and technologies	Some technology resources have limited flexibility in adapting to new technologies, banking requirements, and the pace of changes	Survey current development processes Identify opportunities to enhance these processes Promote modularity and Application Program Interfaces (APIs) Work with other industry associations and agencies to investigate paths forward	Continuous adaptation and movement toward more flexible and modular designs Develop open network interfaces and supporting formalized network security design principles Work with other industry associations and agencies to investigate paths forward	Consumer capability to select, install, configure, and securely administer components for financial transactions Work with other industry associations and agencies to investigate further avenues for improvement of security implementation

performance standards. This can lead to unexpected consequences, inability to incorporate legacy systems, and divergence from open standards or multiple options within a standard that affects interoperability and could ultimately impact consumer confidence.

Introducing and managing change requires constant technical improvement.

Resolution of these issues requires continuous improvement of methodologies for introducing and managing change. This includes more timely development of open standards, testing methodologies, and certification programs.

In order to adequately plan and prioritize production investments for various infrastructure assets, it will be crucial to have an understanding of consequences for various disruption scenarios, including capturing the effects of interdependencies with other infrastructures. Infrastructure interdependencies have never been considered in planning security investments. However, as all of the US critical infrastructures continue to evolve, their interdependencies appear to be increasing. These interdependencies may make way for knew and unforeseen vulnerabilities.

Technical attributes that will drive the success of this objective are:

- Monitoring changes in critical markets. The effects of various threats and protection strategies on critical markets must be monitored to gauge strategy effectiveness.

- Timely development of open security standards. Open security standards are critical to forming a unified front to strengthen security.
- Development of security criteria and guidelines for third-party suppliers. It will be critical that all suppliers follow a standard set of guidelines for effective implementation in the financial services industry.
- Verification of compliance with security criteria and guidelines. Certification programs for compliance will be necessary in assuring that standards and guidelines are being followed.
- Development of testing methodologies that successfully reduce security vulnerabilities. Standard and stringent test methodologies must be developed to ensure that the latest vulnerabilities are being evaluated. This is crucial, as technologies and procedures will constantly be evolving.
- Building flexibility into design to speed installation of security enhancements. When possible, flexibility and portability of systems and technologies must be inherent in their design. This will minimize cost and complexity as systems and technology evolve over time.

OBJECTIVE 3: PREPARE BANKING INDUSTRY PERSONNEL FOR THE EVOLVING INDUSTRY.

Meeting the challenges of an evolving industry needs to be an integral part of corporate culture.

New technology, interdependencies, risks, and market environments require organizational practices to adapt to meet the challenges of change. Banking and financial organizations should review and update risk management practices, technology systems management and personnel policies, and train employees to be prepared for these changes. In particular, system administrators need to be trained and constantly made aware of the latest security vulnerabilities. Banks and financial organizations should keep current with new developments to mitigate and overcome potential security vulnerabilities. An organization's physical and information systems security should employ an effective, integrated approach. Threats from insiders and outsiders should be addressed by personnel security measures, in the systems' designs, testing, implementation, and through proactive senior management oversight and periodic audits.

Technical attributes that will drive the success of this objective are as follows:

- Technical training and awareness. Awareness of the latest threats and the latest security tools and systems will be a continual process.
- Security practices and adaptation. The proper and complete adaptation of security practices will require buy-in by all industry participants and security providers.
- Security screening for information systems personnel. Strict screening of personnel having access to information systems is imperative in reducing insider threat.

OBJECTIVE 3: Prepare banking industry personnel for the evolving industry.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Technical training and awareness	Technical competency assessment survey	Varies with vendors, users, and technologies; limited security training, some applications training	Improve third-party service provider, vendor, and user training in both applications and security	Integrate threat data into training through government and private cooperation Use of technology to improve delivery of training	Achieve dynamic integration of security and operational training and awareness
Security practices and adaptation	Risk reduction of successful infrastructure attacks Results of independent audits against benchmarked security criteria in information security policies	Limited coordination and communication between the bank's physical security and systems security departments Limited information sharing across disciplines and government/private entities Some impediments to use security information in personnel decision-making Minimal audit standards for security requirements	Encourage internal coordination and education Increased information sharing between the bank's physical security and systems security departments Facilitate information sharing Identify and mitigate impediments to use of security information in personnel decision-making Examine security policies that impact use of security information Work with AICPA to design and implement enhanced audits	Security requirements integrated into systems operations Publish and distribute relevant security information to bank's organizational and systems security areas Improve scope and depth of audit standards	Continually improve coordination, information sharing, and use of security information across bank departments Coordinated sharing among banks Evolve to coordination across industries
Security screening of information systems personnel	Reduction of the insider attacks	Personnel criteria vary widely by organization including criticality of information systems positions Standards for systems and network security procedures vary in third-party information system providers Local employment and defamation law inhibits sharing derogatory personnel information	Establish guidelines based on job criticality Establish guidelines for contract clauses for critical information systems personnel Review state, local, and federal laws and recommend changes to allow appropriate data sharing and other personnel security measures Define professional accreditation requirements and design program	Apply guidelines to internal and external information systems personnel Establish or enact regulations permitting better security screening for information systems personnel Roll out accreditation program	Implement advanced behavior systems to screen personnel Institute regular personnel information sharing Monitor percentage of accredited participants

OBJECTIVE 4: MAINTAIN SAFETY AND PUBLIC TRUST IN THE BANKING INDUSTRY.

Banking enjoys a high level of public trust, which must be maintained.

Public trust is an important differentiator of the banking industry relative to other service providers. Maintenance of this trust is critical to the ongoing faith in the banking system. Security concerns, whether perceived or real, can significantly impact trust levels. Ensuring that public trust is maintained in balance without costly and complicated regulatory and legislative controls requires extensive education and cross-industry participation. Collaboration among bank executive management, regulators, legislatures, consumers/public, business, and press is required to ensure that security, integrity, availability, and reliability of industry services are maintained. This includes extensive communication and coordination among the various participants, both internal (bank-to-bank, bank-owned entities, and outsourcers) and external to the industry, including its dependencies on service providers. Establishing the same level of trust in new cyber banking services, such as electronic commerce, that currently exists in the physical world is an important challenge in the next several years.

When considering solutions, special attention must be given to understanding any costs involved. Certain legislative and regulatory requirements and certification and service mark programs carry substantial overhead. These costs must be weighed against the value of the assets being protected and the invaluable trust that the public places in banking institutions.

Technical attributes that will drive the success of this objective are:

- Educational programs tailored to legislators, regulators, consumer public, businesses, investor community, and the press, regarding the value of the banking industry financial services (e.g., payment systems), risks to be managed, and the value of risk management practices.
- Shape/influence domestic and international legislative and regulatory initiatives that are focused on information sharing, nationally focused security infrastructures, and security technology.
- Cross-industry communication and coordination focused on industry infrastructure issues, including bank-to-bank, third-party and bank-owned service provider arrangements, and across external dependencies.
- Leadership in developing and implementing voluntary self-regulatory programs.

OBJECTIVE 4: Maintain safety and public trust in the banking industry.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Develop and implement educational programs tailored to legislators, regulators, consumer public, businesses, investor community, and press regarding the value of the banking industry financial services (e.g., payment systems), risks to be managed, and the value of risk management practices	Consumer opinion polls Regulatory and legislative results Public understanding and acceptance of service marks	Several loosely or uncoordinated, individual efforts Numerous newly announced programs (e-trust, AICPA, Global Chip Card Alliance)	Survey current practices Evaluate effectiveness; review and endorsement by stakeholders Develop and coordinate strategy Identify useful metrics	Ongoing public awareness programs Promote value of service marks to engender public trust	International coordination Continually refine programs
Help shape/influence domestic/international legislative and regulatory initiatives	Effective but minimal legislation/regulation for banking functions Industry self-monitored programs and practices Consistent application to all parties	Lack of consensus on legislative issues dilutes effectiveness Effective association involvement with regulatory bodies, but no control over nonbank entrants	Identify and implement self-regulatory programs Promote application of domestic laws by function and across sectors to address nonbank participants Use contracts to ensure sound risk management and liability definition	Introduce appropriate legislation	Focus on international coordination
Ensure cross-industry communication and coordination focused on industry infrastructure issues including bank-to-bank, third-party and bank-owned service provider arrangements	Multi-industry coordinated efforts Third-party adoption of practices	Various associations, forums, independent efforts Service providers that serve groups, banks, and businesses (e.g., credit cards, electronic commerce)	Coordinate work groups to document existing policies and practices of interbank and bank-owned service providers Develop framework and criteria to evaluate third-party service providers' security arrangements	Establish Bank Council to review third-party initiatives	Promote the value of existing service marks to engender public trust
Take leadership in identifying and developing voluntary self-regulatory programs	Adoption of self-regulation Adoption of service marks Contract provisions enforcing good practices	Independent industry/vendor controlled programs Redundancy among industry associations	Inventory existing programs Develop necessary bank programs and charters Promote sound civil enforcement of good practices by contract law	Affected participant education and communication Civil court action against insecure and irresponsible parties that impact critical banking infrastructure	Continually refine programs Develop cross industry programs

TECHNOLOGY AND POLICY DRIVERS

A summarized list of the principal technologies and technology-related policies that drive the success of the objectives are:

- Promotion of existing service marks and development of additional open standards certified through acceptable testing methods for emerging technologies and interoperability of all stakeholder systems and processes
- Development of a multi-infrastructure early warning system/dialogue that monitors cross-infrastructure dynamics/vulnerabilities and supports cross-infrastructure-based contingency planning
- Initiation of cross-infrastructure practices and training for technical/skills certification and personnel security practices
- Public awareness; influence of regulatory and legislative bodies in support of practices

OPPORTUNITIES AND SHOWSTOPPERS

OPPORTUNITIES

- Convergence of IT and telecommunications permits banks to extend their product and service portfolio through multiple delivery channels and improve responsiveness to customers (i.e., time-to-market).
- Generation of procedures for industry/government information sharing on potential threats focuses effort and minimizes resource costs while reducing fraud, service outages, and errors.
- Opportunity to accelerate successful consumer adoption of secure electronic banking, with mutual benefits to banks and consumers, vs. prolonged rollout period of high costs and low volumes.
- Ability to use multi-industry consortia to:
    1. Establish efficient, cost-effective interoperability open standards, service mark, and training bodies for securely transmitting information and money flows before widespread fragmentation occurs.
    2. Expand capacity and/or establish restoration priorities for geographically concentrated catastrophic failures. Effectively coordinate financial service industry objectives and messages, and disseminate these objectives and messages to legislators, regulatory agencies, the press, and the public. Continuing the trust relationship permits banks to leverage their critical role in the electronic-commerce and electronic money evolution.
    3. Coordinate disaster recovery and crisis management from a high-level industry perspective to ensure interfaces, interdependencies, and other impacted areas are considered and addressed.
    4. Coordinate international standards and cooperation, leveraging established commercial practice and civil law.
    5. Leverage and influence of third-party assurance services to minimize consumer confusion and maximize bank effectiveness.

SHOWSTOPPERS

- Difficulty of industry and government to specify new cyber risks and to share threat histories because of fear of sharing competitive information or divulging sensitive information does not permit industry to maximize resources and realistically protect the infrastructure. This can lead to delay of industry-wide recovery planning strategies.
- Legal constraints and liability concerns limits banks' ability to fully perform security checks and share information about suspects.
- Government regulation must be structured to encourage incorporation of security in products. In addition, legislation and differing/conflicting banking requirements must foster an environment that will support creative solutions and the ability to manage risk. Legislation/regulation must also support cost-effective solutions that will not negatively impact the ability of banks to compete against unregulated non-bank competitors.
- Lack of consensus on globally acceptable security certification and/or encryption techniques creates weak links in infrastructure resulting in higher likelihood of attacks.
- Increasing pace of installing multiple security devices and different protocols impacts interoperability.
- Liability issues that will arise with new technologies and services may reduce the motivation for providing and using various types of services.

REFERENCES

Daly, P. President's Commission on Critical Infrastructure Protection Report. 1997.

NSTAC Financial Services Assessment Report, 1997.

Sound Practices Guidance on Information Security for Networks. Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation, SR 97-32 (SUP).

Testimony of Ken Lieberman, SVP, VISA USA. Visa's plans and experience in the use of digital signature technology. Hearings before the Subcommittee on Technology, of the House Committee on Science, 105th Congress. October 28, 1997.

glossary & acronyms

ABA American Bankers Association

AICPA American Institute of Certified Public Accountants

ANSI American National Standards Institute

API Application Program Interfaces

ASIMS Aeromedical Services Information Management System

ASIS American Society for Industrial Security

ATM Automatic Teller Machine

ATM Forum The ATM Forum is an international non-profit organization formed with the objective of accelerating the use of ATM products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

BITS Banking Industry Technology Secretariat

CCS/SS7 Common Channel Signaling/Signaling System 7

CERT Computer Emergency Response Team. The CERT Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania. SEI was established in 1984 as a federally funded research and development center in response to "software crisis." Operated by Carnegie Mellon and sponsored by the Department of Defense (DoD), the SEI concentrates on technology transition to improve software engineering practice. The CERT/CC is part of the SEI Networked Systems Survivability (NSS) program. The principal goal of the NSS is to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks. (www.cert.org)

CIITAC Computer Incident and Infrastructure Threat Assessment Center

DoD Department of Defense

DOE Department of Energy

DOJ Department of Justice

FBI Federal Bureau of Investigation

FEMA Federal Emergency Management Agency

FIRST Forum of Incident Response and Security Teams

FSTC Financial Services Technology Consortium

I&W Indication and Warning

IETF Internet Engineering Task Force

InfraGard InfraGard is a group of computer professionals brought together by the FBI in 1996 to address computer crime problems. The group is developing an intrusion alert system to keep businesses informed about computer hacking incidents. (http://www.businesstoday.com/archive/topstories/hackers11.htm)

IPTF Infrastructure Protection Task Force

ISO International Organization for Standardization

IT Information Technology

NIST National Institute of Standards and Technology

NSA National Security Agency

NSS Networked Systems Survivability (program)

NSTAC National Security Telecommunications Advisory Committee

NTA NSEP National Telecommunications Alliance/National Security Emergency Preparedness

glossary & acronyms

OECD Organization for Economic Cooperation and Development

OFX Open Financial Exchange

PCCIP President's Commission on Critical Infrastructure Protection

R&D Research and Development

SAR Suspicious Activity Report

SEI Software Engineering Institute

Secure Electronic Transaction Protocol (SET Standard) Protocol developed by Visa, MasterCard and technology vendors for securely conducting payment transactions over insecure networks like the Internet. SET uses digital signatures to tie a payment transaction to the party and ensure that the payment information was not altered.

Security Security describes mechanisms, policy, and procedures used to protect corporate assets from misuse, alteration, disclosure, or theft. In general, security practices are designed to ensure that computers, data networks, applications, and information are protected from use or misuse by unauthorized personnel and available for use by authorized personnel.

SET Secure Electronic Transaction

Stakeholder Stakeholder refers to participants from the banking industry financial services, its dependent suppliers such as telecommunications and utilities and its vendors.

Suspicious Activity Report All insured depository institutions are required to file Suspicious Activity Reports (SAR) with FinCen, an arm of the Treasury Department, when an employee, customer or other person engages in suspicious activities involving the institution that are not related to a legitimate business purpose. Areas of particular interest include: employee misconduct, money laundering, offshore transactions, wire transfers, third-party obligations, credit cards, and electronic funds transfers. FinCen inputs the SARs into a database, which can be accessed by law enforcement and banking regulatory agencies.

Threat Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification or data, and/or denial of service. (NCSC-WA-001-85)

T1S1 ANSI T1 subcommittee that addresses the Common Channel Signaling Protocol

TFPC Toll Fraud Prevention Committee

Vulnerability A weakness in system security procedures, hardware design, internal controls, etc., which could be exploited to gain unauthorized access to classified or sensitive information. (NCSC - WA - 001 - 85)

participants

CHAMPIONS

William Randle
Executive Vice President
Huntington Bancshares, Inc.

Kit Needham
Senior Director
Banking Industry Technology Secretariat (BITS)

PARTICIPANTS

Edward Appel
Vice President
CertCo

Robert Dabbs
Assistant Vice President
Federal Reserve Bank of New York

Kawika Daguio
Federal Representative
American Bankers Association

Jim Dempster
Senior VP, Technology Strategy
M&I Data Service

Arnold DuPont
Project Manager
Bellcore

Henry E. Gittleman
Supervisor, Special Agent
FBI

Mitch Hadley
Vice President
NationsBank

Susan Koeppen
Trial Attorney
Department of Justice

Ken Lieberman
Senior Vice President
Visa

Dan Lynch
Vice President, Manager of Internal Controls
Mellon Bank

Gabe Maznick
INFOSE
National Security Agency

C. T. Montgomery
Vice President, Crypto Group
CertCo

Sam Schaen
Principal Engineer
MITRE Corporation

Dori Shimoda
Vice President, Strategic Planning
NYCE Corporation

Frank A. Sydor
Vice President
First Chicago, NBD

Randy Till
Director, Business Continuation
MasterCard

participants

PROJECT MANAGER

Dr. George Stratis
Director, Strategic Market Planning
Bellcore

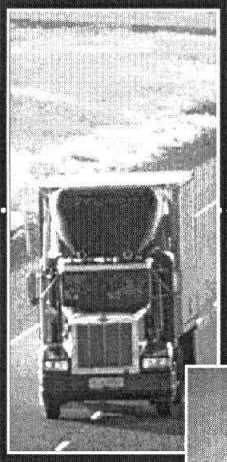
PROJECT SUPPORT

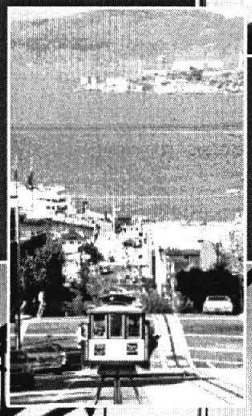
Peggy Lipps
Technical Writer
Service Quality Solutions

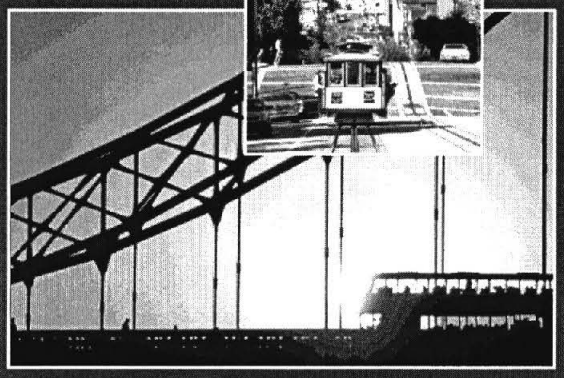
Beth Nave
Change Management Consultant
Bellcore

Pete Pawelko
Technical Director, Professional Services
Bellcore

US Transportation Infrastructure Strategic Roadmap







As a major component of our national economy and defense, the US Transportation Infrastructure is critical to the nation. We are also reliant on it as individuals to meet many of our personal, social, and economic needs. This infrastructure continues to evolve, taking advantage of the latest technologies and practices. However, this evolution is making the infrastructure more dependent on information technologies and the transfer of information to provide its services. In order to assure the effectiveness of the infrastructure and preserve the security and economic well being of the nation, we must devise a well-coordinated strategy to address its evolving threats and vulnerabilities. This roadmap proposes approaches to address these issues so that the surety of the US Transportation Infrastructure can be preserved as we enter the next millennium.

DESCRIPTION

The US Transportation Infrastructure comprises publicly and privately owned passenger and freight transportation assets. These assets encompass all modes of transportation and include:

MODAL TRAVELWAYS

- highways
- railways
- pipelines
- waterways

TERMINALS

- airports
- marine ports
- rail terminals

TRANSPORTATION FLEET

- automobiles
- trucks
- buses
- rolling stock
- airplanes
- ships

Infrastructure assets include those centers ancillary to, but necessary for, the maintenance and operation of the US Transportation System. The centers include maintenance areas, traffic control centers, and dispatch centers. Certain assets in the US Transportation Infrastructure are also part of the global transportation infrastructure, such as the US Merchant Marine, US Flag Air Carriers, and international terminals and ports of entry.

While the transportation infrastructure is mostly owned by federal and state government, the transportation fleet of all forms is almost entirely privately owned.

The Transportation Infrastructure is not owned or operated by a single national entity. Most of the Transportation Infrastructure facilities in the US, which include highways, airports, and seaports, are owned and operated by individual state and local public sector authorities. Most of the civil fleet, which includes automobiles and trucks, rolling stock, aircraft, and the merchant marine, is owned and operated by the private sector. Notable exceptions to this pattern are the transit fleet, which is primarily owned and operated by local public-sector agencies, and the railroad and pipeline industries, where the physical plant is owned and operated by private-sector companies. Although the federal government finances highways, transit systems, and airports, the only transportation system that it operates directly is the air traffic control system.

The transportation system gives unlimited personal mobility to millions of people and is the logistical backbone of our national security.

The Transportation Infrastructure, therefore, contains a set of modally distinct, highly independent and redundant transportation infrastructures that are regulated by the federal and state governments, but are controlled by thousands of local and regional public and private sector owner/operators.

The Transportation Infrastructure is critical to every aspect of life in the US.[1] The transportation system ensures the food supply, delivers energy resources, provides raw materials to manufacturing plants,

imports products for local consumption, exports goods to global markets, moves defense materiel and armed forces personnel, and provides access to emergency services. Perhaps the most important need the infrastructure fulfills is unlimited mobility to millions of Americans to exercise their personal, economic, social, recreational, and religious freedoms, while simultaneously supplying the logistics backbone necessary for our national security and defense.

TRANSPORTATION TRENDS AND CONCERNS

Transportation is viewed as essential, and communities and industry revolve around its availability.

Over the past 50 years, the needs and interconnections of communities and industry in the US have become so diverse and intense that it is impossible to have self-sustaining populations, manufacturing, or military centers. Technologies have evolved to the point that some form of transportation is affordable and available to all. Furthermore, transportation has become such an integral part of our lives that we come to view it as an essential capability and service and often take it for granted. Communities and industry continue to evolve around the availability of transportation, resulting in the following consequences:

- There will continue to be a greater connectivity between communities;
- There will continue to be a greater reliance on the transportation infrastructure;
- Disrupting fundamental transportation connections puts communities, industry, and our national security at great risk.

Even a short-term disruption of transportation results in significant losses.

Even a localized, short-term loss of transportation services, whether caused by natural or inimical forces, results in significant economic losses to companies and individuals and threatens the health and welfare of immobilized citizens. In addition, abrupt cessation of transportation operations can cause injury and death. Airplane crashes, bridge collapses, and rail signal failures are examples of such short-term loss of services. Broader scale and more lengthy service losses may have dire implications for US international policy, global economic power, and national defense.[2] The transportation industry, recognizing that loss of service is a high-consequence event, has developed comprehensive emergency operations responses for a variety of scenarios, such as winter storms, hurricanes, major crashes, earthquakes, and civil defense measures.

Transportation consolidations, while economically necessary, create a potentially more vulnerable infrastructure.

However, the transportation industry is undergoing a dramatic transformation. To begin with, many regions have seen a marked consolidation of transportation services, particularly in the private sector. For example, rail service in many communities has been discontinued, leaving them with only highway access. The rail industry itself went through a tumultuous period in the late 1980s and early 1990s, when many railroads were consolidated or went bankrupt, leaving fewer, larger railroad

providers of predominately freight transportation. These survivors redefined and repositioned themselves as providers of intermodal logistics services competing in new market niches. This same trend was seen in the maritime and aviation industries, with fewer national or even international intermodal operators dominating the transportation marketplace. Although this consolidation of transportation services was economically justified and necessary, one unintended consequence of a more interconnected, less independent transportation system controlled by fewer operators is a potentially more vulnerable infrastructure.

Public funding issues could result in privatization of previously government-controlled operations.

The same economic pressures that are driving private sector consolidation of service providers are producing other challenges to public-sector transportation assets. Chronic underfunding of physical infrastructure maintenance and rehabilitation activities, particularly of publicly owned assets, is creating severe service deficiencies in some areas. The current federal fiscal policy of keeping significant funds in both the Highway Trust Fund and the Aviation Trust Fund for budget reduction purposes has worsened this situation. Similarly, many state governments are finding it difficult to finance necessary pavement and bridge improvement projects. These public funding issues are likely to result in the privatization of highways, the transit fleet, and airports, effectively removing them from direct government operational control.

Military and public dual-use of civil transportation may require upgrading those assets of strategic importance to the military. Fiscal responsibility will need to be decided.

The US military's reliance on the civil transportation infrastructure continues to increase. Using the merchant marine and the civilian air fleet instead of dedicated military assets is a cost-saving strategy. However, this dual-use strategy places additional demands on the transportation infrastructure. Military transportation demands could conflict with the demands of the country's economic activity, which includes the military's own industrial base. The military's strategy for using civil transportation also increases the potential for political, military, and strategic civilian assets, such as civil aviation centers and civilian seaports, to become more attractive targets for aggressor nation states, terrorist groups, and others. The dual-use policy, therefore, raises a difficult issue. Should certain parts of the civilian transportation infrastructure be made more reliable, safer, and secure as a consequence of strategic importance to the military? If so, who is responsible for paying the difference between ensuring individual and commercial surety and the presumably greater costs necessary to provide for national security?

INFRASTRUCTURE INTERDEPENDENCIES

Although transportation has always been highly interdependent with the Energy, Emergency Services, and Financial Infrastructures, it is also now becoming increasingly dependent on the Communications and Information Infrastructure. For years, electric power and fossil fuels have formed the staples necessary to provide transportation services throughout the modern world, and now communication and information systems are also playing a key role in the operation of the Transportation Infrastructure. This interdependency forms more intimate links with the Electric Power Infrastructure because of the electricity demands of communication and information systems. Another indirect relation with the Oil and Gas Infrastructure is also formed because fossil fuels are commonly used to generate power.

The Transportation Infrastructure is interdependent with the other critical US infrastructures, increasingly with the Communications and Information Infrastructure.

The key point is that the Transportation Infrastructure is becoming increasingly interdependent on other infrastructures without widespread industry or government knowledge about the consequences, and without protection strategies. What this implies is that the Transportation Infrastructure can potentially be disrupted by events in other infrastructures. For example, shipping, trucking, and rail transport can all be crippled through their scheduling and coordination systems. Theft of proprietary logistics data can result in economic losses and may contribute to criminal activities (e.g., smuggling, hijacking, theft). Air, rail, and motor vehicle traffic can become gridlocked if traffic control systems or traffic signaling systems are destroyed or disabled. A disruption in fossil fuels can affect the transportation fleet or the supply of electricity.

These infrastructure interdependencies are becoming more complex and more vulnerable.

Joint government and industry leadership is needed to assign responsibilities for maintaining the surety of the Transportation Infrastructure. No organizational structure currently exists that assigns ownership or leadership for addressing the evolving threats and vulnerabilities of the infrastructure. However, this is expected to change when the Department of Transportation is assigned responsibility for assurance of the Transportation Infrastructure under a new Presidential Decision Directive. Industry is not likely to take action unless there is an economic benefit to their investment or there is an incident involving a loss of life. Although it may not currently be feasible to take down a significant component of the infrastructure through the Communications Infrastructure, the possibility of this happening is increasing as the Transportation Infrastructure becomes more reliant on computer and network technology.

Transportation Infrastructure surety needs to be managed by joint government and industry leadership.

All infrastructures need to be part of a coordinated effort to address surety issues.

A coordinated front among all infrastructures is needed to address infrastructure interdependency issues. This will require information sharing across and within the various critical infrastructures. Information on threats, disruptions, and vulnerabilities must be collected and properly disseminated in a timely manner. This is a formidable task because competitors may be reluctant to share information for fear of losing a competitive advantage. In addition, an information use structure must be defined in order to identify the type of data needed and who must see it.

DEPENDENCE ON THE TRANSPORTATION INFORMATION INFRASTRUCTURE

There is increasing dependence upon the Transportation Information Infrastructure, and surety issues must be assessed.

The growing dependence of transportation on communication and information systems warrants special attention. Some of these systems are substitutes for capital investments to increase system capacity, efficiency or profitability, while others are used to plan system enhancements and allocate capital. For surface transportation infrastructures, highways and railroads, for example, environmental, political, or financial constraints preclude adding additional physical capacity, so capacity gains come from using the existing infrastructure more efficiently and effectively. For the aviation and maritime industries, sophisticated capacity management technologies are better investments than capital investments (i.e., buying more planes or ships). Global manufacturing and retailing practices place additional demands for better real-time transportation information using advanced tracking, information systems and telecommunication technologies. Multimodal transport link availability and vehicle/shipment status are vitally important information flows for route planning, dispatch, traffic operations and incident response activities. These surface transport operations technologies are the Intelligent Transportation System (ITS). An analogous system, the National Airspace System (NAS), is being developed for aviation. For the purposes of this Roadmap, the aggregate set of all transportation information assets, that is, the hardware, software and data, is defined as the US Transportation Information Infrastructure (TII).

Unfortunately, the rapidly increasing amount of interconnected and interoperable information represented by the TII has also added to the overall transportation system's vulnerability. Although the use of computer systems and the Internet for transportation system management may add some efficiencies, it may also open the infrastructure to a wide variety of cyber threats, including malicious attacks, software bugs, or even the Year 2000 problem.

More use of computer systems for information management gains efficiencies, and opens the infrastructure to a wider variety of threats.

A significant aspect of the TII is that the real value is contained in its databases, rather than in its technology base. Information surety is the critical factor necessary and sufficient for widespread diffusion of the TII. Users of the TII will demand guaranteed information integrity, availability and confidentiality. This means that the owners of the TII must protect against information theft, unauthorized data modification, and the unauthorized destruction of both data and information technology. The TII needs to be open, interpretable, and easily accessible, yet also safe, secure, and reliable.

The TII needs to be open and easily accessible, yet also safe and secure.

Fortunately, the TII is still in its infancy. The transportation sector is not yet dependent on information technologies to the degree that the telecommunications and financial sectors are. Many of the new technical architectures in the TII, such as ITS, are still in the planning and prototype stages. Other systems like the Global Positioning System (GPS), however, are already deployed and available for radio navigation and aircraft landing guidance systems. Vulnerabilities in these systems must be better understood before we fully transition to them.

The TII development needs to be assessed to build in surety from the beginning.

Most owner/operators have not yet connected to the TII, whose specifications are still evolving. As a consequence, the US has an opportunity to build information surety into the TII from the very beginning. This advantage will evaporate quickly, however, in the absence of a comprehensive, focused strategy.

TECHNOLOGY AND POLICY OBJECTIVES

The surety objectives of the US Transportation Infrastructure over the next 15 years are to:

1. **CLARIFY AND ASSIGN ROLES, RESPONSIBILITIES, AND LIABILITIES FOR PRESERVING THE SURETY OF THE TRANSPORTATION INFRASTRUCTURE.**

2. **DEVELOP AN INDUSTRY-WIDE CONSEQUENCE MANAGEMENT ARCHITECTURE FOR THE TRANSPORTATION INFRASTRUCTURE.**

3. **SPECIFY AND DEPLOY APPROPRIATE INFORMATION SURETY METHODS, TOOLS AND TECHNOLOGIES.**

4. **IDENTIFY AND PROTECT VULNERABILITIES THAT MAY RESULT FROM INTERDEPENDENCIES WITH OTHER INFRASTRUCTURES.**

TECHNOLOGY AND POLICY ROADMAPS

The requirements necessary to meet the objectives are outlined in the following roadmaps.

OBJECTIVE 1: CLARIFY AND ASSIGN ROLES, RESPONSIBILITIES, AND LIABILITIES FOR PRESERVING THE SURETY OF THE TRANSPORTATION INFRASTRUCTURE.

Unlike the electric power, telecommunications, finance, and banking infrastructure sectors, the transportation sector comprises tens of thousands of individual operators, loosely associated along mainly modal lines, many of whom are likely to use the TII. Indeed, there are over 40,000 units of government alone that have policy and financing authority over some transportation assets. Adding to this institutional complexity is the emerging global nature of the industry. That is, many Transportation Infrastructure owner/operators are foreign organizations and not subject to the same level of scrutiny or regulation that domestic operators are. As a result, no single agency, association, or operator is able to dictate a single infrastructure surety policy.

No single agency or association, public or private, is able to dictate a single infrastructure surety policy.

OBJECTIVE 1: Clarify and assign roles, responsibilities, and liabilities for preserving the surety of the Transportation Infrastructure.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Stakeholder consensus and buy-in	Enacted policy or regulations in place	No explicit statutory roles, responsibilities, or liabilities for infrastructure assurance	Strengthen legal mechanisms for assigning responsibility to systems owners Define explicit responsibilities for owners and government agencies	Assess responsibility structure for effectiveness	Update responsibility structure according to state of the infrastructure
Federal leadership	Regulatory modification	No security emphasis in existing capital projects planning process	Add surety to the set of transportation planning factors	Modify regulations for systems with public consequences	Continue long-term support and funding for infrastructure surety
Industry awareness	Industry participation	No industry-wide initiatives; very low level of industry awareness	Determine infrastructure vulnerabilities Develop and present TII surety briefing	Establish industry forum for infrastructure and information surety	Infrastructure surety forum keeps industry informed on surety issues and standards
Private/public partnerships	Industry led consortia	Legal impediments to partnering exist	Establish industry-wide policy goals and objectives	Major operators adopt goals and objectives	All operators adopt goals and objectives

The best role for the government is as a leader and facilitator

A more effective policy is for the federal government to act as a leader and facilitator of a new infrastructure-wide surety culture. Appropriate responses that affect the surety of the Transportation Infrastructure arise out of the general attitudes and approaches of all participants, including industry management, workers, and government regulators. If the threats and risks to the infrastructure are genuine, then the government has a legitimate responsibility to energize the industry out of its current complacency. The need and justification for infrastructure surety will have to come from its customers. The Departments of Defense (DoD) and Energy (DOE) are key customers of the civilian transportation infrastructure and have the most stringent surety requirements. Not surprisingly, these customers also have surety experience that would be invaluable to the transportation sector.

This policy objective arises out of these observations:

1. Transportation systems owners and users have not taken sufficient initiative to protect themselves independent of government intervention.
2. Most of the transportation is under nonfederal-government control. Because its owners will suffer the consequences and costs of systems failure, they have the most incentives to protect against such failure.
3. The failure of certain transportation systems carries severe public consequences. Protecting against these consequences is a legitimate role for the federal government.
4. The government has only a limited ability to influence systems owners, using regulation and technology assistance.

Once roles are defined, it becomes the responsibility of infrastructure operators to protect against system failures.

Meeting this objective involves the government sponsoring the forums where infrastructure risks, responsibilities, and liabilities are defined. Once defined, it becomes the responsibility of infrastructure operators to protect against systems failure. This responsibility should be reinforced by assigning specific liabilities to infrastructure owners for the secondary consequences of ignoring threats.

Unfortunately, the lack of solid risk knowledge coupled with the independence of systems operators precludes identifying any definitive strategy for years 6-15.

In summary, successful implementation of this objective will require:

- Consensus and buy-in from transportation stakeholders
- Strong Federal leadership
- Increased industry awareness of infrastructure vulnerabilities
- Formation of private/public partnerships

OBJECTIVE 2: DEVELOP AN INDUSTRY-WIDE CONSEQUENCE MANAGEMENT ARCHITECTURE FOR THE TRANSPORTATION INFRASTRUCTURE.

A robust consequence management approach to Transportation Infrastructure surety must be both continual and iterative. This approach consists of three major steps: threat identification, threat management, and consequence mitigation. Where necessary, the transportation sector is assumed to be willing to cooperate and collaborate with other infrastructure sectors to meet this objective.

Robust management of infrastructure surety must include threat identification, threat management, and consequence mitigation.

OBJECTIVE 2: Develop an industry-wide consequence management architecture for the Transportation Infrastructure.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Threat identification	Increased threat awareness by industry and government	No ability to identify and classify events	Declassify infrastructure threat intelligence Establish Threat Information Forum	Prototype automated Threat Information Forum	Fully automate TII
Implement threat management policies, processes, and technologies	Effective threat management controls	No control architecture exists	Develop architectural specs Identify applicable technologies, funding sources and responsibilities	Prototype architecture	Deploy architecture
Effective consequence mitigation	Loss of service impacts	Unknown	Develop draft contingency plans for most likely threats Implement consequence analysis tools	Test contingency plans Identify long-term protection investment options and funding sources	Refine contingency plans Implement long-term protection investment plan

THREAT IDENTIFICATION

Threats to the Transportation Infrastructure may come from malevolent sources such as hackers, terrorists, and hostile nation states, or from benign sources, such as a breakdown of the telecommunications system. Transportation system operators working with governmental agencies must systematically recognize significant threats, categorize threat effects and levels (i.e., risk of death, injury, economic loss, and system damage), and determine threat likelihood and the probable costs associated with the consequences of a successful threat. Threat identification includes finding both causal factors and agents. The single most important benefit is the dissemination of threat knowledge to all potentially affected system operators (and perhaps to the public as well). Because threats to the

Threat identification includes finding causal factors and agents.

Transportation Infrastructure are likely to threaten other infrastructures, the Threat Information Forum should have representatives from all infrastructures plus appropriate members of the intelligence, defense, law enforcement, and computer security communities.

THREAT MANAGEMENT

An integrated information system architecture containing threat controls is essential.

A method of implementing preventive or corrective measures to reduce either the likelihood or the severity of threats to the Transportation Infrastructure is needed. This implies that deploying an integrated information system architecture containing appropriate threat controls is essential. This architecture is a coherent combination of people, procedures, and technology.[3] Funding sources to deploy such an architecture must also be identified. One option could be for government to provide economic incentives for industry participation. Although enforced legislation could also be used, industry may be more resentful and less cooperative.

Building safety and hazard controls into technologies at their development stage is more effective than adopting them after the fact.

Threat management is a structured approach to eliminating, reducing, and controlling threats and includes approaches for minimizing damage caused by threat-induced system failures. Experience in other risk sensitive industries suggests that incorporating safety and other hazard controls seamlessly into operational technologies during their original developmental phase is far more efficient and effective than trying to adopt such controls after the fact. This experience has also highlighted the critical role of top management in risk avoidance.

Surety policies that are not clearly articulated are in themselves a surety threat.

Policies and procedures for crisis mitigation and response must be well defined and understood by all infrastructure stakeholders, especially in events that can impact other infrastructures or that are life threatening. Surety policies that are not clearly articulated are in themselves surety threats. This will help form a competent and unified front, resulting in increased response and mitigation effectiveness.

CONSEQUENCE MITIGATION

Failures within the Transportation Infrastructure are also tied to emergency management functions.

The transportation community has a long tradition of responding to system outages, failures, and accidents. In addition, transportation has always been an integral part of both national defense and local emergency management plans and operations. Mitigating the consequences of disruptions or failures of the Transportation Infrastructure is both analogous and interrelated to these physical emergency management functions. In addition, where system failure, disruption, or compromise is determined to have a causal agent, appropriate civil, criminal, and national defense responses need to be initiated.

OBJECTIVE 3: SPECIFY AND DEPLOY INFORMATION SURETY METHODS, TOOLS, AND TECHNOLOGIES.

Transportation Infrastructure information surety will be accomplished by balancing the needs of its customers with the capabilities of its service or technology provider. Multiple levels of surety, each appropriate to a specific user of a specific service, will emerge from this approach.

Surety will be accomplished by balancing the needs of customers with capabilities of service providers at appropriate levels.

SPECIFY SURETY REQUIREMENTS

The transportation sector has historically been on the trailing edge of information technology development and deployment. That is, most new information technology is developed for some other market sector and then adapted for transportation purposes. Consequently, it is unlikely that surety technologies unique to the TII are necessary, possible, or desirable. However, development of fitness-for-use criteria usable by both technology providers and TII operators that map off-the-shelf components onto specific needs of the transportation sector is valuable and can be achieved. Specific requirements are likely to encompass authentication, encryption, hardened sites and components, wired and wireless network surety, and so on.

Specific criteria in surety standards for the transportation sector are highly useful.

TII METADATA

Like the physical Transportation Infrastructure, the TII is considered to be a public good. As such, it must be ubiquitous, easily accessible, and usable by millions of highly mobile, legitimate users who demand anonymity or privacy. However, levels of privacy, accessibility, and data integrity among TII subsystems are apt to be inconsistent or contradictory because of the idiosyncratic nature of the TII development process. Therefore, uniform data standards are needed.

The Transportation Information infrastructure must be accessible, useful and secure.

OBJECTIVE 3: Specify and deploy information surety methods, tools, and technologies.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Specify TII surety requirements	Surety standard specifications	None exist	Develop draft fitness specifications	Add to ITS Architecture	Refine and expand to all TII data users
Develop TII metadata	TII data truth-in-labeling standards	No national TII data standards	Develop truth-in-labeling specifications	Release metadata for critical TII data	Refine and expand to all TII data collectors

OBJECTIVE 4: IDENTIFY AND PROTECT VULNERABILITIES THAT MAY RESULT FROM INTERDEPENDENCIES WITH OTHER INFRASTRUCTURES.

Intermeshing of infrastructures may blur the boundaries of responsibility.

Our lack of knowledge about vulnerabilities and protection of infrastructure interdependencies necessitates that we focus more on this area. The increasing intermeshing of the US infrastructures may blur boundaries of responsibility for disruptions and increase the complexity of identifying vulnerabilities. We must also have more information regarding economic consequences of disruptions from interdependencies to acquire industry support.

COORDINATE INTERDEPENDENCY EFFORT WITH OTHER INFRASTRUCTURES

Government leadership is necessary because government has overall responsibility for protecting US infrastructures.

The first step in addressing interdependency issues is to assemble a forum of experts and stakeholders from the different infrastructures. This forum should include both government and industry members who are willing to address mutual and individual vulnerability information. Government leadership at this forum is necessary because it has overall responsibility for protection of the national infrastructures. Effective protection of interdependency vulnerabilities will require a cooperative effort of all infrastructure stakeholders.

DEVELOP ANALYSIS TOOLS THAT HELP IDENTIFY INTERDEPENDENCIES AND THEIR VULNERABILITIES

Computer simulation and modeling of infrastructure interdependencies will be required for analysis.

Analysis tools are needed to identify the effects of interdependencies between infrastructures. This is especially important now that the transportation infrastructure is becoming so reliant on the Communications and Information Infrastructure. Data on economic impacts for various disruption scenarios can be used to select options from protection portfolios. High-power computational capabilities will be required to model the complexities inherent in this spectrum of problem scenarios.

OBJECTIVE 4: Identify and protect vulnerabilities that may result from interdependencies with other infrastructures.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Coordinate interdependency efforts with other infrastructures	US infrastructure assurance forum established	None exists	Develop charter and membership for forum	Assemble forum on periodic basis to address immediate concerns Plan long-term goals for interdependencies protection	Take action on long-term goals Periodically review and update forum's charter and membership
Develop analysis tools that help identify interdependencies and their vulnerabilities	Effective and usable analysis tools developed	None exist	Identify funding sources for tools Identify existing analysis tools Specify requirements for technology gaps Begin prototyping unavailable tools	Deploy suite of analysis tools Identify vulnerabilities in interdependencies Develop vulnerability protection plan	Develop vulnerability protection plan Continually update vulnerability protection plan

TECHNOLOGY AND POLICY DRIVERS

The following technology and policy developments are critical in order to achieve the roadmap objectives:

- . Information on threats to the Transportation Infrastructure must be declassified and made available to the transportation sector. To achieve industry buy-in, the transportation sector must be privy to government information on their infrastructure's vulnerabilities. Supporting information would also be helpful in achieving credibility.

- Advances in surety technologies will need to be made and reflected in public policy. Encryption and authentication technology standards, for example, must be better defined, recognized, and accepted.

- . Effective public/private sector partnerships will require policy and legislative reforms, especially for antitrust and Freedom of Information Act areas. This action will reduce legal constraints that could hinder vital partnerships.

OPPORTUNITIES AND SHOWSTOPPERS

OPPORTUNITIES

- The fact that the Transportation Information Infrastructure is in its infancy offers an opportunity to direct and incorporate surety concepts from the ground up, rather than attempting to add them in later. A specific example of where we must be expeditious is GPS. We must take advantage of incorporating surety in the use of GPS before the full transition to this system for radio navigation is complete by 2010.
- Opportunities for partnering and synergism exist with members of other infrastructures. Many of these partnerships may not be obvious until analysis of infrastructure interdependencies is begun. These partnerships can present excellent opportunities for joint ventures and for sharing expense burdens.

SHOWSTOPPERS

- Although various arguments for greater efficiency through information sharing will be made, the cultural divide between the public and private sectors, reinforced by the natural isolation among private sector competitors, will preclude a single, nationally consistent, interoperable TII within the transportation sector. While this situation may be less desirable from an academic perspective, it may actually be more resistant to strategic disruption. That is, the effects of compromising a single information asset could remain isolated and local to that asset.
- The lack of an industry policy on infrastructure surety will be more likely to continue in the absence of some defining event or incident, or until there is government involvement. Until one of these events take place, the likely consequences will be:
  1. Senior managers and policymakers have little knowledge about industry-wide surety issues. Without a significant surety disaster, they have little incentive to learn more. Also, in the absence of a national transportation surety emergency, few resources will be devoted to ensuring (and insuring) against such a disaster.[4]
  2. National surety issues may not be considered in continued planning of the Transportation Infrastructure.
  3. If transportation organizations will not explicitly specify transportation information surety requirements, they will end up with prevailing industry standards. It is unknown whether these will be sufficient to deter all but the most determined and technically proficient aggressors.

NOTES

1 The nation is strategically interdependent on the global Oil and Gas, Financial, Telecommunications, and Transportation Infrastructures. Our national vulnerability stems in part from the global exposure of these infrastructures.

2 While there have been many disruptions of local transportation services, primarily because of natural disasters, current US civil defense doctrine holds that conventional bombing by an aggressor nation-state is the only strategic way to disrupt the US Transportation Infrastructure. This event has never occurred.

3 While threat management is the focus of this roadmap, it should more properly be operationalized as a subset of system safety management. There are obviously many hazards inherent in the Transportation Infrastructure in addition to threats. All of these need to be assessed and controlled in the same process.

4 US transportation safety policy has been tombstone motivated. That is, a certain number of deaths are required before the industry adopts reform. Unfortunately, this pattern is likely to repeat itself to motivate cyberspace reform.

SOURCES

Nancy G. Leveson. *Safeware: System Safety and Computers.* Addison Wesley, Reading, MA. 1995.

Martin Libicki. *Defending Cyberspace and Other Metaphor.* NDU Press Book, National Defense University. 1997.

Winn Schwartau. *Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age.* 2nd ed., Thunder's Mouth Press, New York, New York, 1996. The "Dummy's Guide" to cyber-threats.

Volpe Transportation Center. "Emerging Issues in Transportation Information Infrastructure Security," Proceedings. May 1996.

glossary & acronyms

DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
GPS	Global Positioning System
Information Surety	A measure of the integrity, confidentiality, and accessibility of information.
ITS	Intelligent Transportation Service
NAS	National Airspace System
TII	The Transportation Information Infrastructure, consisting of transportation data, software, hardware, and communication technologies.

participants

CHAMPION

David Fletcher
Alliance for Transportation Research Institute
University of New Mexico

US Emergency Services Infrastructure Strategic Roadmap

The Nation's Emergency Services Infrastructure is rapidly changing to provide for an increasing array of challenges. Change is being driven by issues resulting from social, economic, and technological innovations and globalization forces. Within the current environment, and to prepare for the future, the stakeholders of this Infrastructure must ensure its continued reliability while adding new capabilities. This roadmap addresses the significant drivers and objectives that we must focus on over the next 15 years to ensure effective and reliable operation of the Emergency Services Infrastructure.

DESCRIPTION

The ESI provides services that respond to a wide range of emergencies.

The Emergency Services Infrastructure (ESI) supports the public health and safety of the residents of our nation's communities. Services provided include response to day-to-day situations such as medical emergencies caused by car accidents, heart attacks, trauma, fires, and crimes in progress. ESI agencies also respond to natural disasters (hurricanes, floods, earthquakes, tornadoes), technological disasters (transportation accidents and hazardous materials incidents), and intentional disasters caused by sabotage or terrorism.

The ESI interacts with all other US infrastructures.

The ESI's great breadth of stakeholders is the first line of emergency response in crisis situations. The unpredictable possibilities of emergency scenarios require that ESI support agencies interact with all other US infrastructures, either as responders or consumers of their services. For example, state and local agencies are largely dependent upon utilities (electric power, oil and gas, and telecommunications providers) to fulfill their missions during routine and emergent situations. Additionally, when these infrastructures experience disruptions, ESI agencies are called upon to help mitigate the impact of these outages on the community.

Services are provided by government, private and volunteer agencies.

Emergency services in the US have always been provided by a combination of federal, state, and local government resources in partnership with nongovernmental private and volunteer agencies. Responsibilities of ESI agencies are varied and include providing law enforcement, fire, emergency medical service (EMS), rescue, public health, emergency communications, and emergency planning and management services. Effective communication among all members of the ESI is crucial to an effective incident response.

Government agencies support local resources when necessary.

Responding to and managing the consequences of natural, technological, and intentional disasters are primarily state and local functions. Federal agencies are called in for support when state and local resources are unable to effectively cope with the disaster situation. Federal emergency services are generally provided through emergency support functions (ESFs) coordinated by the Federal Emergency Management Agency (FEMA). ESFs are functional area-of-response activities established within the Federal Response Plan to facilitate the delivery of federal assistance during the immediate response phase of disaster.

Examples of federal providers of emergency services include:

- FEMA
- United States Coast Guard

- Military forces operating under provisions for military support to civil authorities
- United States Forest Service
- National Park Service
- Department of Veteran's Affairs hospitals
- National Disaster Medical Service (NDMS)
- Federal Bureau of Investigation (FBI)
- Bureau of Alcohol, Tobacco, and Firearms
- Department of Energy

State and local providers of emergency services include:

- State law enforcement
- Local law enforcement (police and sheriff's departments)
- National Guard
- Fire departments
- Various local agencies (public works, etc.)
- Health or public health departments
- Emergency management agencies

Quasi-public/private providers include:

- Civil defense organizations
- Volunteer fire and rescue squads
- Transit agencies

Private providers include:

- Medical doctors
- Nurses
- Emergency medical technicians (EMTs)
- Hospitals and clinics
- Utilities
- Numerous nongovernmental or nonprofit agencies such as:
  - American Red Cross
  - CARE
  - Salvation Army

ESFs support the nongovernmental services with a variety of agencies.

ESFs are designed to enhance the protection of lives, property, public health, and the maintenance of public safety. During malevolent attacks, such as terrorism, the FBI is responsible for crisis management, and consequence management is coordinated by FEMA and delivered by a lead federal agency for each ESF. Agencies delivering such services include the Environmental Protection Agency, the Department of Health and Human Services, and the Department of Transportation. Many services are also related to the

federal agencies that oversee and regulate public health and safety, such as the Department of Health and Human Services, Food and Drug Administration (FDA), Environmental Protection Agency, Department of Transportation, Department of Defense, and the Center for Disease Control.

Emergency service agencies coordinate response to emergencies.

Emergency service agencies act as coordinators of local response to disasters and infrastructural outages (e.g., power or water outages or service interruptions). Typical emergency service tasks include rescue, evacuation, security, hazard suppression, hazard mitigation, recovery, and restoration. For example, if power or water to an area within a city is interrupted, a local emergency operations center (EOC) may be established to monitor the situation and any secondary impact. In the case of a power outage, entrapped persons may be rescued from elevators, and police may direct traffic at critical intersections and provide enhanced patrols to limit disorder. In water shortages, fire and police agencies may collaborate with planning efforts to ensure public access to potable water pending restoration by the utility. Joint information centers, comprised of public information officers from various local, state, and federal agencies, are responsible for coordinating information provided by a variety of official sources, including EOCs.

THE FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

FEMA is the central point of contact for a wide range of emergency management activities.

FEMA serves as the central point of contact within the federal government for a wide range of emergency management activities in both peace and war. FEMA is tasked to work with the emergency management community to achieve a realistic state of preparedness. FEMA's activities include, but are not limited to:

- ensuring continuity of government and coordinating mobilization of resources during national security emergencies;
- supporting state and local governments in a wide range of disaster planning, preparedness, mitigation, response, and recovery efforts;
- coordinating federal aid for presidential-declared major disasters and emergencies;
- administering the National Flood Insurance Program;
- coordinating civil radiological preparedness for defense, power plant accidents, and nuclear accidents;
- providing training and education to enhance the professional and technical development of federal, state, and local emergency management personnel;
- coordinating a national network of urban search and rescue teams that are able to respond to building collapses caused by natural disasters such as earthquakes or intentional disasters such as terrorist bombings.

Because no single city or state can be fully prepared for large natural or manmade disasters, the NDMS was created by the Emergency Mobilization Preparedness Board in 1981. The NDMS is a cooperative asset-sharing partnership among the Department of Health and Human Services, the Department of Defense, the Department of Veterans Affairs, FEMA, state and local governments, and the private sector. The purpose of the NDMS is not to replace local disaster planning efforts but to supplement and assist when local resources are overwhelmed. The NDMS includes deployable medical response capability to the disaster site or receiving location, a medical evacuation system, and more than 110,000 precommitted nonfederal acute-care hospital beds in more than 1,800 hospitals throughout the country.

The NDMS was created to supplement and assist overwhelmed local resources.

The NDMS also augments the ESI through the provision of disaster medical assistance teams (DMATs), disaster mortuary teams (DMORTs), and national medical response teams (NMRTs). These specialized NDMS assets are coordinated through the United States Public Health Service, Office of Emergency Preparedness within the Department of Health and Human Services. DMATs provide disaster medical support to a wide variety of disaster situations, while DMORTs augment the ability to manage mass fatality situations. The three NMRTs, located in Los Angeles, Denver, and Winston-Salem, provide an enhanced ability to manage the medical consequences of chemical, biological, and nuclear terrorist events both in field and in hospital.

The NDMS also provides specialized disaster teams.

SERVICE GAPS AND INTERDEPENDENCIES WITH OTHER INFRASTRUCTURES

The web of organizations providing emergency services is complex and diverse. As a result, there are large variations in service quality and availability. As an example, one of the largest service gaps is in rural emergency medical and fire response. One quarter of the US population lives in rural areas, which amounts to 80% of the US land area. Although many regional and state emergency systems have helped to coordinate delivery of services, some of the more successful initiatives, such as 911 service, are still not widely available. Another example is punctuated by the dramatic decline in federal support for EMS. A 1973 EMS Systems Act provided $30 million annually to states until 1981. Since 1981, EMS services have increasingly become a state responsibility. The federal role in EMS has become mainly a supporting role for training EMS providers, facilitating guidelines and standards, funding demonstration projects, and offering technical assistance.

Emergency services vary in quality and availability.

There has been growing awareness of the interdependency of emergency services with other national infrastructures. For example, the ESI is very dependent upon the US Telecommunications and Energy Infrastructures. If communications were disrupted or information systems destroyed during an emergency, the effective coordination and delivery of services to the impacted populace could be

US infrastructures are interdependent.

imperiled. If fuel is not available, emergency service vehicles at impacted sites could become immobilized. If the transportation infrastructure is disrupted, critical supplies could be delayed in reaching the impacted site.

Utilities, such as energy, and telecommunications are also dependent upon the ESI during outages. For example, during power outages caused by civil disorder, utility personnel may require escorts by law enforcement agencies to safely conduct restoration activities. Similarly, utility personnel may require escorts through areas threatened by large-scale wildland fires or similar natural emergencies.

EXAMPLES OF EMERGING THREATS

Emerging threats include terrorist use of chemical, biological, and nuclear weapons.

Until the notorious Sarin attack against the Tokyo subway by the Aum Shinrikyo cult, terrorism involving the use of chemical, biological, nuclear or radiological agents had been widely discounted. Although cases in the open literature noted rare occasions where terrorist groups were found with chemical or biological agents, the terrorist employment of such agents was considered unlikely. The Aum Shinrikyo attack on the Tokyo subway injured approximately 5,500 persons and left 12 dead. Various reports emphasize the cult's willingness to use or attempts to obtain other lethal weapons, including perhaps the deadly Ebola virus.[1] Similarly, while the technical capacity to craft a nuclear weapon was acknowledged to exist, the necessary access to fissile material was considered highly unlikely. Recent events, however, have required a reassessment of our ability to protect against and manage the low-probability, high-consequence potentials of such events.[2]

The former Director of the Central Intelligence Agency, John Deutch, observed that terrorists seeking to administer punishment or revenge might embrace chemical or biological tactics if their present tactics should become ineffective. While observing that the use of nuclear materials was less likely, Deutch noted that Chechen rebels planted radiological materials in a Moscow park in December 1995.[3]

Twenty-five nations can produce chemical weapons, and 17 are thought to be able to produce biological weapons.

Since the end of the Cold War, the potential for acts of terrorism has increased. Nuclear leakage, the growth of criminal gangs, and economic instability have contributed to the potential proliferation of chemical, biological, and nuclear devices.[4] The proliferation threat is not limited solely to the former Soviet Union. Over 25 nations have chemical weapons or the ability to produce them, and 17 are suspected of biological warfare development, including Iran, Iraq, Libya, Syria, and North Korea (nations that have shown militant- and terrorist-supporting behavior at various times[5]). Recent nuclear weapons testing by India and Pakistan has also become great cause for concern.

A threat to interests within the US also exists. According to a *London Telegraph* news brief, the Aum Supreme Truth Cult planned to release 20 tons of Sarin nerve agent in the US. A former follower,

Yoshihiro Inoue, the Aum Intelligence Minister stated, "If things had gone as planned, the Aum would have released 50 tons of Sarin in Tokyo, and 10 tons each in Washington and New York".[6]

Threats to the US can be domestic and foreign.

Domestic threats are also an area of continuing concern. For example, John Sopko[7] noted the following cases. In December 1995, a man with alleged ties to survivalist groups attempted to smuggle 130 grams of ricin into the US. In May 1995, a sometime associate of the Aryan Nation was arrested in Ohio after ordering bubonic plague organisms. In March 1995, two members of the Minnesota Patriots Council were convicted of trying to assassinate federal agents by employing ricin.

Biological terrorism was the subject of a special JAMA issue.

The threat of biological terrorism was addressed in the August 6, 1997, issue of *JAMA*, The Journal of The American Medical Association.[8] The series of articles in this specially themed issue reinforces the assessment of scientists and policymakers that there is good reason for the US to be concerned about an attack by terrorists using biological agents. Danzig and Berkowsky have written that small groups of people with modest finances and basic training in biology and engineering can develop an effective biological weapons capability.[9] R. Danzig, now a lawyer in Washington, D.C., was undersecretary of the US Navy from November 1993 through May 1997. P. B. Berkowsky is now a special assistant in the Office of the US Secretary of Defense. Other contributors to this special issue of *JAMA* point out that not only is biological warfare possible, it has serious and complex consequences. For example, Jeffrey Simon notes that biological weapons can be used to threaten civilian populations, create mass panic, and thus achieve military goals by undercutting the civilian support necessary for military operations or by holding civilians hostage to prevent military operations.[10]

The economic impact of biological warfare has been explored.

Since only modest microbiologic skills are needed to weaponize biological agents for terrorist use, the threat of biologic weapons warrants significant concern. The cost of producing biologic weapons is minimal. Combined with the ease of aerosol dissemination using commercial, off-the-shelf devices and the ability to select targets and attack from a position of obscurity, terrorists can release fresh, viable, and virulent biologic agents without the constraints of precise targeting. In order to assess the potential impact of a biological attack, three epidemiologists from the Centers for Disease Control and Prevention in Atlanta constructed a model that compares attacks using three classic biological agents on a suburban area.[11] The agents considered were *bacillus anthracis* (anthrax), *brucella melitensis* (brucellosis), and *francisella tularensis* (tularemia). The study found that the economic impact of a bio-attack could range from $477.7 million per 100,000 persons (brucellosis scenario) to $26.2 billion per 100,000 persons exposed (anthrax scenario). Rapid implementation of a post-attack prophylaxis program was found to be the single most effective way of reducing these losses.

Preparedness against attack can be economical.

In all three cases, high rates of injury and death were projected. For example, in the anthrax scenario for each 100,000 persons exposed, 50,000 cases of inhalation anthrax were expected, causing 32,875 deaths. Early implementation of prophylaxis was found to be an effective way of limiting both mortality and economic loss. As a result of their actuarial economic analysis of intervention, the authors demonstrated that preparedness for biologic terrorism is economically beneficial. They also suggest that a larger portion of a preparedness budget (derived from loss savings) should be allocated to measures that enhance rapid response to attacks. Suggested preparedness measures include developing and maintaining laboratory capabilities for clinical and diagnostic testing and environmental sampling, developing and maintaining drug stockpiles, and developing and practicing local response plans.[12]

Cyber and novel threats are becoming more of a cause for concern.

In addition to chemical, biological and nuclear (or radiological dispersal) scenarios, potential threats such as cyber attack (information warfare), or novel threats such as radio frequency weapons (RFW) attacks can yield results ranging from jamming and disruption to destruction of electronic systems. Such attacks could include the use of directed energy weapons such as flux compression generators to disrupt aviation systems or direct electrical contact to compromise a power grid. Emergency services agencies could be impacted also if terrorists used such devices to disrupt essential communications capabilities. The final, long-term potential is the threat of hybrid attack that combines more than one type of threat. As new technology becomes better integrated with our day-to-day lives, these now-exotic potentials may become of greater concern.

Although steps have been taken to improve preparedness and response capabilities for chemical and biological attacks, greater emphasis needs to be placed on developing and enhancing federal, state, and local emergency services capabilities to detect, respond to, and manage the entire range of potential attacks.

TECHNOLOGY AND POLICY OBJECTIVES

Objectives for the protection of the US Emergency Services Infrastructure provide a strategic plan to ensure synergy among organizations addressing national infrastructural issues. The objectives over the next 15 years are:

1. **DEVELOP A COLLABORATIVE INDICATIONS AND WARNING SYSTEM FOR THE CRITICAL INFRASTRUCTURES.**

2. **DEVELOP AN IMPROVED RISK ASSESSMENT PROCESS FOR THE EMERGENCY SERVICES INFRASTRUCTURE.**

3. **IMPROVE THE NATION'S CAPABILITIES TO ADDRESS CHEMICAL, BIOLOGICAL, CYBER AND INFORMATION WARFARE ATTACKS.**

4. **IMPROVE THE NATION'S EMERGENCY MEDICAL SERVICES SYSTEMS.**

TECHNOLOGY AND POLICY ROADMAPS

The requirements necessary to meet the objectives for the US Emergency Services Infrastructure in the near (0 to 3 years), intermediate (3 to 6 years), and far (6 to 15 years) terms are described below.

OBJECTIVE 1: DEVELOP A COLLABORATIVE INDICATIONS AND WARNING SYSTEM FOR THE CRITICAL INFRASTRUCTURES.

US infrastructures are increasingly interconnected and vulnerable.

US critical infrastructures are becoming increasingly vulnerable to attack as their interconnectivity and interdependencies increase. In order to ensure the viability of the minimal essential infrastructures in the US, an indications and warning (I&W) system should be developed among emergency services, electric power, telecommunications stakeholders, and key members of the federal law enforcement agencies. The FBI was tasked in Presidential Decision Directive (PDD) 63 to expand its current organization to a full-scale National Infrastructure Protection Center.

An effective I&W network is necessary to protect US infrastructures.

The cornerstone of infrastructure protection efforts is the development and coordination of an effective and reliable I&W network. Such a capability needs to be built both from the top down with a National Threat Center and from the bottom up with local/regional threat warning groups or centers. By integrating both local/regional and national capabilities, a robust and rapid warning system with the capacity for a wide range of threats can be created. The warning process can be based upon the collection and analysis data obtained through open-source collections to identify trends and potential threats. Open-source materials can be obtained from the Internet and news sources and can provide valuable information for guiding planning, training, and preparedness efforts for managing the consequences of infrastructural attacks.

A net assessment of threats combined with real-time situation status can be a powerful tool.

Collection and analysis of open-source data include scanning to discover trends and potential or possible threats, monitoring specific threat information during periods of heightened concern, and forecasting potential future target selection or tactical developments. Trends and potentials can be combined with traditional criminal intelligence, which essentially evaluates capabilities and intentions of specific groups for crisis management purposes, to provide command personnel with the information necessary to manage an incident in progress. The synthesis of trends and potentials with capabilities and intention constitutes a net assessment. When combined with real-time situation status, these are powerful tools for guiding incident response and defining the event horizon.

OBJECTIVE 1: Develop a collaborative indications and warning system for the critical infrastructures.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
National information and threat center and network	Robust, accurate, and timely alerts Forecasting future threats Effective information exchange	Limited crisis and threat coordination centers	Begin establishing regional centers	Regional centers operational Begin establishing national center and interacting with regional centers	National center fully operational and interacting with regional centers Effective coordination of crisis and consequence management efforts Near real-time situation status of critical events to guide response Expanded user base
Regional threat warning centers	Robust, accurate, and timely alerts Forecasting future threats Effective information exchange	Limited capability	Establish regional threat warning capability Regional centers active and interacting with national center and all local infrastructures	Operational regional threat warning centers linked with national center and with each other to form robust indications and warning network	Threat and warning network is fully integrated with crisis and consequence management efforts Near real-time situation status of critical events to guide response
Establish emergency management response plans for infrastructural and potential threats	Operational effectiveness Revision of law to address new threats Incentives for planning and mitigation are defined and in place	Some limited plans in place, refinement of others in early phases Required as part of Presidential Decision Directive (PDD) 39 Exist, but are not fully embraced or understood	National Security Council (NSC) coordinated information partnership established Analysis of threat and vulnerability data through integrated emergency management concepts of preparedness-response-recovery-mitigation New law and policy developed for cyber and emerging threats	Successful response to complex emergencies Successful mitigation efforts underway Increased awareness of trends and potentials among emergency management staff Revised law and policies to reflect threat posture Evaluate success of incentives and maximize their use	Emergency management efforts fully integrated into infrastructural protection efforts Scanning of events to assess trends and potentials Monitoring situation status and forecasting emerging threats and vulnerabilities
Coordinated national infrastructure assurance policies	Acceptance by ESI communities Mutually supporting public/private sector efforts Mitigation or prevention of cascading effects Overall reduction in costs Increased mitigation activities	Current efforts are primarily reactionary Mitigation and infrastructure assurance policies are fragmented or sector specific Limited electronic civil defense for cyber threats No integration of cyber and physical protection efforts	Develop awareness of threat and make protective tools available to meet evolving threats Develop model practices Initiate user groups to formulate protective options Initiate a systems approach to assurance and mitigation efforts	Implement mitigation efforts Evolve standards Define federal, state, and local roles on assurance of national infrastructure systems Synchronize public/private efforts Establish grants and low interest loans for security enhancement	Proactive electronic and physical civil defense strategies and refined tools to meet evolving threats Measurable cost reduction due to mitigation efforts Minimal cascading effects experienced

Information surety is critical to an indications and warning system.

Information surety will be critical to an indications and warning system in providing effective crisis response and mitigation. Advanced information technologies are needed to organize, filter, correlate, and disseminate massive amounts of data in an efficient, timely and secure manner. Continuous improvements and development of sensor technologies are also necessary for more effective warning and identification of natural disasters and malevolent attacks, especially for the detection of chemical and biological agents.

I&W information must be disseminated to a variety of users including emergency response teams and managers. It will therefore be most effective to include I&W information as an integral part of management response plans. Existing plans must be re-evaluated to identify areas requiring improvement or areas that can take advantage of the latest I&W technologies or information.

A coordinated effort will be key to success.

Coordination of the critical infrastructure owners and operators will be key to an effective indications and warning system. A critical first step is the precise definition of roles and responsibilities. Policies and guidelines must effectively outline the chains of command, lines of communication, procedures, and strategies to be used in diverse cross-infrastructure emergency response.

Objective 2: Develop an improved risk assessment process for the emergency services infrastructure.

Emergency services providers must develop an improved risk assessment process.

This objective requires the coordination of state, local, and federal emergency services organizations to develop an improved risk assessment process. A top-down systems approach is necessary to effectively align risks, strategies, and investment priorities for all levels of the ESI. Consequence-based risk assessment tools would be extremely useful in this process.

A national threat center can coordinate a state and local services network.

Risk assessment for local regions should be the lead responsibility of the state and local emergency services sector. Such processes rely upon a systems approach, broadband detection capabilities, integrated response, and deliberate preplanning. Regional threat warning groups or centers could be formed at the county or state level and be integrated into a network, coordinated, but not directed by a national threat center.

Capabilities and requirements need to be assessed.

An assessment of equipment and response requirements must be conducted to determine existing capabilities and requirements that must be filled to address a broad spectrum of threats. These requirements should be developed from a needs assessment, surveys of users, and information obtained from ongoing efforts such as the Chemical Biological Defense Command's Domestic Preparedness Program. This program is training local responders from 120 cities in response to chemical/biological threats.

Playbooks and target folders can be useful aides.

Deliberate planning could be aided by the development of response decision-making tools. Such tools could include playbooks, which guide response to a class of threats at a general class of

OBJECTIVE 2: Develop an improved risk assessment process for the Emergency Services Infrastructure.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Develop an effective systems approach to risk assessment	Reduced frequency of event occurrences Consequences and cascading effects decreased	Too narrowly focused No standard hazard, risk or vulnerability assessment models Lack of consensus regarding systems approach	Acquire, assess, and disseminate threat, vulnerability, hazard, and risk data Coordinate risk assessment model(s) via FEMA, NCCEM, NEMA, and fire and law enforcement	Conduct risk assessments for priority prototype scenarios Integrate assessment results for standards certification and technology needs	Coordinate risk assessment for interdependent US infrastructures
Develop detection and response capability for a broad spectra of threats (chemical, biological, nuclear, cyber, hybrid, and novel threats)	Timely mobilization and response to critical incidents	Limited, fragmented, minimal real-time or near-real-time detection or situation status monitoring capability Emerging recognition of need and early efforts underway	Reinforce the value of detection and response capabilities for chemical, biological, and nuclear threats Build an awareness of cyber threats and vulnerability of strategic ESI communication nodes	Integrate detection and response capabilities into regional early warning efforts Build and expand capabilities of specialized response teams Coordinate public/ private efforts, coordinate efforts among levels of government	Participation of key players from water, power, telecom, emergency management, police, fire, EMS and public health sectors
Develop playbooks and target folders to guide response to infrastructural threats	Operational effectiveness enhanced Exercise effectiveness enhanced	Some limited examples in place or under development Efforts are for single threat, event, or target class	Playbooks to guide general response to a range of threats initiated, target folders enhancing response capacity to key infrastructural targets initiated	Automation of playbooks and target folders underway in key metropolitan areas Initial efforts to integrate playbooks and target folders with detection and response capabilities are underway Integration of gaming and simulation to enhance response and emergency preparedness	Real-time or near-real-time situation status and modeling capability is integrated with sensor and detector capability and incorporated into playbooks and target folders in key metropolitan areas

targets, and target folders, which provide detailed information on the layout, unique hazards, intermodal linkages, systemic effects, geography, weather conditions, and typical response resources for a specific high profile target. However, these training aids are only useful if incorporated in an effective training curriculum.

OBJECTIVE 3: IMPROVE THE NATION'S CAPABILITIES TO ADDRESS CHEMICAL, BIOLOGICAL, CYBER AND INFORMATION WARFARE ATTACKS.

A domestic preparedness capability needs to be developed.

This objective involves the development of a comprehensive domestic preparedness capability for both current and future high-consequence threats. These threats include chemical and biological warfare agents used in terrorist scenarios, the potential for cyber terrorism or information warfare (either cyber attacks, i.e., against systems; or virtual attacks, i.e., using systems to cause damage at a physical target), and the resulting need for electronic civil defense.

Training for responders will be necessary.

Future threats of potential concern also include the use of advanced, less-lethal technology, such as high-energy or radio-frequency weapons (some are on the market within the former Soviet Union) and the potential of hybrid varieties of attack. For all of these threats, a capable and appropriately equipped response force is needed. These responders will come from local police, fire, EMS, and emergency management agencies. As a result, new and expanded training is needed, and new and more effective personal protective equipment (PPE) needs to be developed and deployed. However, chemical and biological training should build upon existing hazmat training levels as much as possible.

Using available technology can make training exercises cost-effective.

Cost-effective exercises should be developed for responders to demonstrate and evaluate the effectiveness of their planning and training. Whenever possible, full advantage should be taken of available technology such as video teleconferencing, medical computer networking, and interactive simulation exercises. Using these technologies in exercises will help integrate local, state, and federal participation while allowing them to remain at their home stations.

The MMSTS has been developed to augment first-response teams.

In addition to the cities receiving domestic preparedness training through Nunn-Lugar-Domenici stimulated efforts, the United States Public Health Service has initiated the development of the Metropolitan Medical Strike Team System (MMSTS). Key cities have been identified and prioritized to begin implementation of these enhanced local capabilities. However, it should be noted that the MMSTs, like military speciality teams, or the NDMS-sponsored NMRTs are supplementary assets (not first-responders). As a result, while they are necessary, the most impact toward mitigating the effects of a chemical attack can be gained by first-responders. Similarly, the greatest impact on mitigation for a bio-attack is derived by enhanced awareness of physicians and hospital staff. Additional efforts are needed to bolster capabilities in these areas. These include tools and technology for mass casualty decontamination and for differential diagnosis.

OBJECTIVE 3: Improve the nation's capabilities to address chemical, biological, cyber and information warfare attacks.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Chemical warfare (CW) sensors	Robust, accurate, real-time, cost-effective devices	Some devices available, some placement considered	Needs and siting assessments initiated	Pilot placement at key sites	Key targets protected by sensors, special events by portable devices
Biological warfare (BW) sensors	Robust, accurate, real-time or near-real-time, cost-effective devices	Some limited capability devices available, enhanced devices in research phases	Test and deploy prototype devices	Needs and siting assessments initiated	Key targets protected by sensors, special events by portable devices
Information warfare (IW) sensors	Robust, accurate, real-time, cost-effective devices	Physical separation, firewalls Limited software developed	Develop awareness of threat and make protective tools available to meet evolving threat	Proactive electronic civil defense strategies and refined tools to meet evolving threat	Proactive electronic civil defense strategies and refined tools to meet evolving threat
Specialty training for first-responders	Solid foundation of chemical, biological, and nuclear terrorism response skills	Limited initial train-the-trainer indoctrination programs underway	Completion of initial indoctrination training programs Develop cost-effectiveness exercises	Initiation of curricula development for advanced training Conduct periodic and unscheduled exercises	Provision of advanced training
Enhanced PPE for first-responders	Low cost, multithreat, practical PPE (simple to use, durable, quick, and easy to don)	Limited availability of effective gear among first responders, existing gear contributes to performance decrements and limits operational effectiveness	Develop and field test new prototypes	Allocation of enhanced PPE in major target areas	Broad-based availability of enhanced PPE

OBJECTIVE 4: IMPROVE THE NATION'S EMERGENCY MEDICAL SERVICES SYSTEMS.

EMS systems should be integrated.

The EMS professionals will be faced with many demanding challenges and opportunities during the next 10-15 years. Over this same time period, technological advances will also provide new products and offer innovative ideas to address pre-hospitalization care. Effective EMS systems should be integrated to increase operations efficiency in order to maintain the public's expectation of emergency medical care quality and quantity of services at the same time that some emergency response budgets are being reduced.

An area of growing concern is chemical or biological attacks by terrorists. We are currently ill-prepared to handle large-scale mass decontamination. An operational concept and tools must be developed to better prepare for this threat. This effort should include education and awareness programs for EMS and hospital staff on threats, diagnosis, tools, and procedures.

The availability of antidotes (e.g., atropine) and antitoxins is also crucial to maximizing response outcomes. Civilian agencies need access to military medical capabilities (e.g., MARK-I auto injectors) and to such devices for children and the elderly. The military autoinjectors, available in the US, are designed for healthy 80-90 kg males, not pediatric or geriatric patients. A similar need is the availability of portable, multipatient ventilators to manage nerve agent casualties.

Simon, in his recent *JAMA* article,[8] departs from the philosophy that, with the right mix of policies, security measures, and intelligence gathering, a major biological warfare terrorist attack can be prevented. He suggests instead that the history of conventional terrorism indicates that such efforts are not entirely sufficient, and "the greatest payoff in combating biological terrorism lies in focusing on how best to respond to a terrorist attack."

Simon further emphasizes that the medical and emergency service communities will play the most important role in the response process. He states, "Ensuring that they are trained to recognize the symptoms of diseases caused by biological warfare agents and have Critical Incident Stress Debriefing teams available to help them cope with the emotional aspects of treating exposed survivors should be part of contingency planning. By improving our readiness to respond to biological terrorism, many lives can be saved and terrorists denied their goal of creating panic and crisis throughout the country."[8]

Secure communications systems need to be developed.

While interoperability of electronic equipment is also needed and should be addressed, a more pressing need is the development of interactive communications capabilities. Not only do hospital staff need to be linked to ambulances and paramedic or EMT personnel, but police and fire responders need to be linked with each other as well as EMS personnel. Responses to complex emergencies, such as those

OBJECTIVE 4: Improve the nations's emergency medical services systems.

Technical and policy attributes that drive the success of this objective	Measures of Effectiveness	Current Status	Near Term (0 to 3 years)	Intermediate Term (3 to 6 years)	Far Term (6 to 15 years)
Tools and operational concept for mass decontamination	Ability to provide effective and rapid decontamination for ambulatory and nonambulatory patients in a mass casualty situation	Mass decontamination is problematic, no real solution is available given current technology	Develop potential tools and operational concept	Implement enhanced mass decontamination techniques	Refinement and broad knowledge of enhanced techniques
Tools for differential diagnosis of CW/BW agents	Ability to quickly and accurately determine agent employed in attack	Limited knowledge base, experience, and awareness	Broaden awareness of CW/BW issues among EMS and hospital staff	Development of expert decision-aids using advanced information technology	Broad-based usage of expert decision aids
Enhanced availability of antidotes and antitoxins	Access to sufficient antidotes and antitoxins for mass casualty situations	Limited availability, efforts toward enhanced access, caching	Determine scope of antidote and antitoxin needs	Sufficient caches of antidotes and antitoxins for key metro areas	Regional antidote and antitoxin availability commensurate with needs
Develop antidote autoinjector capability for children and the elderly	Availability of "MARK-I" type autoinjectors for pediatric and geriatric patients	No devices available for use in the US	Determine autoinjector needs, obtain FDA approval of devices, stimulate commercial production	Distribution of dose appropriate autoinjectors to key metropolitan areas	Broad-based availability of dose appropriate autoinjectors
Enhance ability to provide mass ventilation to nerve agent casualties	Availability of sufficient mechanical ventilators	Unknown, but limited quantity	Assess need, stimulate research on portable multipatient devices	Increased ventilation capacity in key metropolitan areas	Increased ventilation capacity nationwide
Implement and develop advanced technology for communications, training and simulation, and telemedicine	Broad-based use of virtual reality simulation for training and response rehearsal Improved secure communications	Limited application, enhanced practical systems being researched and developed Communication systems not always interoperable	Field test virtual reality simulations for CW/BW response and treatment in key metropolitan areas Provide telemedicine options Coordinate and standardize communication systems	Refined virtual reality simulation capability Refined telemedicine options Expand secure communications capability	Broad-based availability of virtual reality simulation as a training and response rehearsal tool Availability of telemedicine Highly effective secure communications used interactively among all ESI responders
Enhanced epidemiological surveillance for bio-threats	Robust, integrated local and national bio-surveillance	Effective capability challenged by fiscal restraints	Bolster existing efforts, increase funding to local epidemiologic efforts	Expanded epidemiological surveillance for bio-threats	Continued robust system with ongoing funding

resulting from infrastructure disruption or attack by weapons of mass destruction (WMD), require a high degree of interaction between police, fire, and EMS responders. Technical advice from off-scene advisors (virtual reachback) is also needed. Toward this end, interactive, encrypted, digital communications capabilities for voice and data (e.g., web-based data) must be developed and deployed.

Fiscal constraints reduce incentive for special capabilities.

The constraint on these communications technologies and on treatment technologies is largely fiscal. The cost of providing street medicine (which in many cases is provided to persons with no or marginal insurance) places a fiscal strain on health care facilities, thus reducing the incentive to develop or sustain the specialty capabilities most needed to effectively deliver field or disaster medicine.

All ESI communications centers (including 911 public safety answering points and EOCs) are vulnerable to strategic-level attack. Such attacks could originate through the public-switched networks or in the future by a radio frequency weapons attack. Efforts to protect against and manage these potentials should be integrated into a broader national electronic civil defense effort.

VR capabilities could be valuable tools.

Virtual reality (VR) capabilities have the potential to become a powerful tool for training EMS (as well as police and fire responders) in a number of skills. VR capabilities would be particularly useful in preparing personnel to perform time-critical procedures in hostile or austere environments. VR capabilities would also be valuable tools in crisis and response rehearsal for hazardous tasks (e.g., hostage rescue, hazmat, chemical/biological agent response).

Telemedicine, the use of telecommunications and information technology to provide health services at a distance, may serve to ameliorate many of the problems endemic to the health care system. Because the technology is essentially distance insensitive, telemedicine is likely to improve the delivery of care by eliminating inequities in the distribution of providers and specialized services.

Epidemics have long been a concern of densely populated areas. The current bio-threats highlight the need for improving our efforts and funding for enhanced epidemiological surveillance. In the past, an effective epidemiological surveillance capability has been hindered by fiscal constraints. Only a change in budgetary priorities will strengthen our mitigation and response to this threat.

TECHNOLOGY AND POLICY DRIVERS

A summarized list of the principal technologies, policies, and process issues that will drive the success of the above objectives follows.

- Continued development of an affordable, ubiquitous, high-capacity, national telecommunications network guarded with information surety. Communication is essential to warning and responding to crisis scenarios.
- Education and awareness of emergency services personnel to the threats and vulnerabilities of interdependent infrastructures and to emerging threats. We must also train emergency service personnel to better recognize the symptoms of diseases caused by chemical and biological agents.
- Effective government leadership to initiate infrastructure assurance efforts. Roles and responsibilities must be clearly defined for all managers and operators of the ESI.
- Adequate allocation of funding for near-term infrastructure surety and long-term surety research activities. The government and other ESI stakeholders must make financial commitments for improved infrastructure surety.

OPPORTUNITIES AND SHOWSTOPPERS

CHALLENGES

- Ensuring the capability to manage and contain incidents by having adequate capacity; access to incident sites; field identification of chemical, biological, and radiological agents; adequate protective gear; sufficient amounts of atropine and antidotes, and effective communications.
- Developing and implementing a communications plan to be used during a crisis to coordinate services and reassure the public by disseminating accurate and timely information.
- Predicting and preventing the cascading effect of failures (e.g., the failure of a water processing plant leading to lack of clean water, leading to large outbreak of illness, leading to an overload on doctors and hospitals, etc.).
- Understanding the complexity of US infrastructure interdependencies with the Emergency Services Infrastructure.
- Preventing and responding to deliberate or inadvertent threats such as: industrial chemicals; pesticides; herbicides; radioactive isotopes; heavy metals; bacteria; viruses; and parasites; and attacks against information systems using physical, high energy, or cyber means.
- Recognizing information warfare attacks and distinguishing intentional acts from inadvertent outages or breakdowns.
- Protecting our water systems. Needs for central water systems and expanding water sources stem from growing residential development, expanding population, and the need to protect public health and safety (e.g., firefighting).
- Addressing issues of manufacturer certification and liability for PPE.

OPPORTUNITIES

- Continue to build on the effective, locally based services now in place.
- Invest in building additional service capacity and service redundancy (where appropriate) to address potential strategic scenarios.

- Plan communication/service delivery in a variety of worst-case scenarios, and recommend solutions on the local, state, and federal level.
- Continue to appeal to the general public's volunteerism and mobilize them through education, training, and awareness.
- Use the current emergency planning organizations to expand understanding of the complexity and interdependencies of the US infrastructures.
- Extend the National Medical Disaster System model (i.e., decentralizing direct services and operations and centralizing information and communications) to a variety of emergency services systems.
- Develop and deploy strategies for preventing and mitigating the impacts of emerging threats such as information warfare or chemical and biological threats like antibiotic-resistant bacteria and mutating or resurging viruses that could contaminate the water supply.
- Develop real-time or near-real-time situation status assessment capabilities to scan and monitor systems and direct resources or to block attacks.

SHOWSTOPPERS

- All of these efforts require federal assistance because of the scarcity of resources and competing needs. Enhanced state and local funding is needed to build effective immediate-response capabilities. Consequence management is largely a state and local function. Firefighting and law enforcement (police and sheriffs) are local entities with major roles in response to infrastructural or WMD attacks, yet the overwhelming bulk of funding to date has been allocated to federal agencies. Rapid response, which limits morbidity and mortality, is dependent upon local accessibility of capable responders and systems. Accordingly, effective response and infrastructural defense require funding for enhanced indications and warning, decision-making tools, and first-responder capabilities at the local level. Furthermore, participation of first responders in capabilities assessments and requirements definitions will be crucial to the development and deployment of new technologies. Otherwise, new equipment may not meet the needs or expectations of first responders.

NOTES

1 Global Proliferation of Weapons of Mass Destruction, *Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs*. United States Senate, One Hundred Fourth Congress, Second Session, March 27, 1996, United States Government Printing Office, Washington, D.C. 1996.

2 Jonathan B. Tucker. Policy Approaches to Chemical and Biological Terrorism. Brad Roberts (ed.), Terrorism with Chemical and Biological Weapons: Calibrating Risks and Responses. Washington, D.C. Chemical and Biological Arms Control Institute. 1997.

3 John Deutch. Worldwide Threat Assessment Brief to the Senate Select Committee on Intelligence. Statement for the Record. pp. 16-18. February 22, 1996.

4 John F. Sopko. The Changing Proliferation Threat. *Foreign Policy*, Number 105, Winter 1996-97.

5 Leonard A. Cole. *The Eleventh Plague: The Politics of Biological and Chemical Warfare*. New York: W.H. Freeman and Company. 1996.

Louise K. Comfort (ed.). *Managing Disaster: Strategies and Policy Perspectives*. Durham, NC: Duke University Press. 1988.

6 "Aum 'planned to gas US'," *London Telegraph*, Issue 673. March 29, 1997.

7 Sopko. 1996-97.

8 J. D. Simon, PhD. *"Biological Terrorism: Preparing to Meet the Threat," Journal of the American Medical Association (JAMA)*, 1997;278:428-430. August 6, 1997.

9 R. Danzig, J.D., D.Phil., P. B. Berkowsky, M.A.L.D. Preparations Against Biological Warfare Should Be Higher Priority. Washington, DC; *Journal of the American Medical Association (JAMA)*, 1997;278:431-432. August 6, 1997.

10 Simon. 1997.

11 Arnold F. Kaufmann, Martin I. Meltzer, and George P. Schmid. The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable? *Emerging Infectious Diseases*, Vol. 3, No. 2. April-June 1997.

12 Kaufmann et al. 1997.

glossary & acronyms

Antiterrorism Defensive measures used to reduce the vulnerability of individuals and property to terrorist attacks.

Attack Sabotage or the use of bombs, chemical or biological agents, nuclear or radiological materials, armed assault with firearms or other weapons, or an electronic (or high-energy) attack on a computer system or the information infrastructure by a terrorist or quasi-terrorist actor that may cause substantial damage or injury to persons, property, or information systems in any manner. Attacks can involve physical means, either conventional or those involving chemical, biological or nuclear agents, or informational warfare including virtual and cyber attacks. See conventional, cyber, hybrid, physical, and virtual attack.

BW Biological Warfare

Capabilities and Intentions The portion of the intelligence cycle for infrastructure protection which deals with the specific operational capability or capacity (capabilities) and objectives (intentions) of a terrorist or quasi-terrorist group to conduct an attack. This portion of the intelligence cycle includes criminal intelligence. See trends and potentials and net assessment.

Consequence Management Measures to alleviate the damage, loss, hardship or suffering caused by emergencies. These include measures to restore essential government services, protect public health or safety, and provide emergency relief to affected entities. Consequence management response is primarily a responsibility of the affected state and local governments. Federal agencies support local efforts under the coordination of the Federal Emergency Management Agency (FEMA).

Conventional Attack Physical attacks using conventional means such as bombings, sabotage or armed assault.

Counterterrorism Offensive measures to deter and respond to terrorism. Traditionally, counterterrorism described covert activities directed toward specific groups; however, in broader usage it refers to efforts to respond to and the impact of terrorist attack.

Crisis The impact on an organization and its ability to cope with or respond to an extraordinary incident or event.

Crisis Management In terms of terrorism, measures to resolve the hostile situation, investigate, and prepare a criminal case for prosecution under federal law. Crisis management response is under the primary jurisdiction of the federal government with the Federal Bureau of Investigation acting as lead agency. Crisis management response includes measures to confirm the threat, investigate and locate the terrorist and their weapons, and capture the terrorists.

Criticality The level of impact of an attack or interruption caused by a natural or technological event upon people or a system.

CW Chemical Warfare

Cyber Attack Attacks against electronic information or data systems achieved through the use of an information based technology. Examples include hacking, denial of service, intrusion, etc.

DMAT Disaster Medical Assistance Teams

DMORT Disaster Mortuary Teams

glossary & acronyms

Emergency	Any event, human-caused or natural, that requires responsive action to protect life or property.
Emergency Support Functions (ESFs)	Functional area-of-response activities designed to facilitate the delivery of federal assistance in the immediate response phase of a disaster. Protection of lives, property, and public health, and the maintenance of public safety are the goals of these activities.
EMS	Emergency Medical Service
EMT	Emergency Medical Technician
EOC	Emergency Operations Center
ESF 1 Transportation	This function coordinates federal transportation support to state and local government entities, voluntary organizations, and federal agencies during an event requiring federal response.
ESF 2 Communications	This ESF assures the provision of federal telecommunications support to federal, state and local response efforts in the aftermath of a presidentially declared emergency, major disaster, or other situation per the Federal Response Plan.
ESF 3 Public Works and Engineering	Technical advice and evaluations, engineering services, and construction management and inspection are included in this ESF.
ESF 4 Firefighting	This ESF provides for the detection and suppression of wildland, rural and urban fires resulting from or occurring coincidentally with a catastrophic event requiring federal assistance.
ESF 5 Information and Planning	The information ESF is used to collect, process and disseminate information about a potential or actual emergency or disaster to facilitate federal response.
ESF 6 Mass Care	Coordinates efforts to provide shelter, food, and emergency first aid at major events requiring federal assistance.
ESF 7 Resource Support	This ESF provides logistical/resource support in events requiring a federal response, including relief supplies, space, office equipment, contracting equipment, and personnel to support immediate response activities.
ESF 8 Health and Medical Services	Provides coordinated assistance to supplement state and local resources for public health and medical care needs following significant natural or human-caused disasters.
ESF 9 Urban Search and Rescue	Provides Urban Search and Rescue efforts, which include location, extrication and provision of immediate medical treatment for victims trapped in collapsed structures.
ESF 10 Hazardous Materials	The Hazmat function provides federal support to state and local governments in response to an actual or potential discharge and/or release of hazardous materials following an incident requiring federal response.
ESF 11 Food:	Identifies, secures, and arranges for the transportation of food to areas affected by disaster.
ESF 12 Energy	This ESF facilitates restoration of US energy systems in the aftermath of a disaster which requires federal assistance.
ESI	Emergency Services Infrastructure

glossary & acronyms

Event Horizon The event horizon is the foreseeable future within a crisis or emergency incident. The impact of the event and its consequences can be interpreted as the event horizon based upon an understanding of what occurred, the resources available to manage the event, and the impact of response and mitigation actions during the course of response activities.

FBI Federal Bureau of Investigation

FDA Food and Drug Administration

Federal Response Plan (FRP) Developed under the leadership of the Federal Emergency Management Agency, this interdepartmental planning mechanism is the federal government's method of preparing for and responding to the consequences of disasters. Federal planning and response are coordinated on a functional basis, known as emergency support functions (ESFs), with designated lead and support agencies for each identified functional area.

FEMA Federal Emergency Management Agency

Forecasting Dissemination of threat information derived from an analysis of trends and potentials or through a net assessment to guide response or protective actions. See trends and potentials and net assessment.

Hybrid Attack An attack involving a combination of conventional and chemical, biological or nuclear agents (Conventional + CBN), or an attack combining conventional or chemical, biological or nuclear agents with an information warfare attack (Conventional/CBN + IW).

Incident A specific emergency event that requires a response to correct the situation, restore order, or protect life or property.

Incident Commander The person responsible for the command and direction of a functions at the field response level.

Indications and Warning (I&W) Intelligence (from a variety of sources, both open and classified) which is intended to provide warning of potential or imminent attacks against targets and infrastructure.

Information Warfare (IW) Actions taken to achieve information superiority or to influence sociopolitical or economic discourse gained by attacking or manipulating information infrastructure through physical, virtual, or cyber attack. Includes attacks against information systems or virtual attacks against physical targets by disrupting or manipulating information based processes.

MMSTS Metropolitan Medical Strike Team System

Monitoring The active search for, collection of, and assessment of information on terrorist activity which has been identified through scanning efforts as having direct local implications. See trends and potentials, scanning and forecasting.

NCCEM National Coordinating Council on Emergency Management. A national organization dedicated to supporting the emergency management (EM) community by reducing the risk to life and property in times of disaster; functioning as a clearinghouse for comprehensive EM issues; fostering creative problem solving; maintaining and expanding dedication to professional standards; influencing public policy and fostering commitment to global collaboration on EM issues.

NDMS National Disaster Medical System

NEMA National Emergency Management Association.

glossary & acronyms

Net Assessment The synthesis and fusion of trends and potentials and capabilities and intentions which is provided to an incident commander or decision-maker to aid crisis decision-making and emergency management actions by forecasting the likely event horizon for a particular incident. See event horizon, trends and potentials and capabilities and intentions.

NIPC National Infrastructure Protection Center

NMRT National medical response team

NSC National Security Council

Open-source Intelligence Open-source intelligence is information gathered from nonclassified sources such as the news media, the internet, and databases which when properly analyzed can provide decision-makers with timely and pertinent information on which to base decisions.

PDD Presidential Decision Directive

Physical Attack Attack against physical targets or infrastructure utilizing physical or conventional means.

Playbook Preplanned general guidance for field response to a complex situation, such as the integrated police, fire service and EMS response to a nerve agent attack at a convention center or stadium.

PPE Personal protective equipment

RFW Radio frequency weapons

Quasi-terrorism Activities incidental to the commission of crimes of violence that are similar in form and method to terrorism but lack an organized social, political, religious, or economic dimension.

Scanning Ongoing efforts to review reports of terrorist attack and threat information to access trends and potentials of local importance. See monitoring and forecasting.

Target Folder A specific, comprehensive reference and decision-making tool to guide integrated emergency response to a specific, high-profile target within a specific jurisdiction. A target folder would include site plans, terrain analysis, interior and exterior plume dispersal models, blast analysis, maps indicating vulnerable points and potential sites for incident support activities, etc.

Trends and Potentials The portion of the indications and warnings cycle for infrastructure protection that considers patterns of attack, and the selection of targets and tactics by terrorist or quasi-terrorist groups (trends) and their likely impact on the provision of emergency services (potentials). Evaluation of trends and potentials is based on open source or unclassified intelligence. Trends and potentials supports training and preparedness efforts. See capabilities and intentions, open source intelligence, and net assessment.

Virtual Attack An attack against a physical target achieved through the information infrastructure (such as crashing transportation vehicles by manipulating control systems).

VR Virtual Reality

Vulnerability The risk of exposure to attack, disruption or destruction faced by a segment or component of the physical or virtual infrastructure.

WMD Weapons of mass destruction

participants

John Sullivan
Deputy Sheriff
Los Angeles County Sheriff's Department,
Emergency Operations Bureau

Michael Byrne
Deputy Director
New York City Mayor's Office of Emergency Management

David C. Iglesias
Chief Counsel
New Mexico Division of Risk Management

Special thanks to the following for their comments and suggestions:

Thomas E. Baldwin, Ph.D.
Emergency Systems Group
Decision and Information Sciences Division
Argonne National Laboratory

Tony Sill, Ph.D.
Department Manager
Communication Systems Engineering Department
Sandia National Laboratories