I&C Sector
National Strategy Input

INFORMATION & COMMUNICATIONS SECTOR

National Strategy for Critical Infrastructure and Cyberspace Security

May 2002

Prepared by:

- **Cellular Telecommunications and Internet Association (CTIA);**
- **Information Technology Association of America (ITAA);**
- **Telecommunications Industry Association (TIA);**
- **United States Telecom Association (USTA); and**
- **Their members in support of the President's Critical Infrastructure Protection (CIP) program.**

CTIA
Building the Wireless Future
Cellular Telecommunications & Internet Association

ITAA

TIA
BUILDING GLOBAL COMMUNICATIONS

USTA
UNITED STATES TELECOM ASSOCIATION

Disclaimer

Many companies, organizations, and individuals have contributed to the development of this plan. It represents the collective viewpoints of the Information and Communications Sector (I&C Sector) and is submitted on a voluntary basis by the I&C Sector Coordinators under Presidential Decision Directive 63. However, this is not an agreement, contract or legal document. No statements made in this document should be construed to obligate particular companies to take or not to take specific actions.

This is also a living document. Change is a persistent theme throughout this plan and the industries represented in the I&C Sector and, therefore, future revisions must be foreseen to assure relevance going forward.

The I&C Sector is committed to doing its part to protect the nation's critical infrastructure and looks forward to working with government bodies, other industry groups and interested organizations to achieve this important end.

I&C Sector
National Strategy Input

Table of Contents

Executive Summary

The Information and Communications Sector (I&C) took a huge hit on September 11, 2001, both in human terms and physical destruction. Many I&C professionals died in the attacks, including management and technical professionals from Akamai, Accenture, BEA Systems, Cisco Systems, Compaq, GENUiTY, Metrocall, SAIC, Wipro, Oracle, Sun and Verizon. Much of the destruction consisted of property, including computers, software and data. One estimate places losses in Information Technology (IT) resources by the financial community alone at $3.2 billion. Morgan Stanley estimates losses of IT hardware, restoration of services, long-term IT costs to enterprises and annual World Trade Center IT spending at over $25 billion.[1]

In the midst of disaster, this sector -- a complex web of people, technology, products and services—responded brilliantly. The I&C Sector absorbed the blow and came back strong.

September 11th served as a grim reminder that the I&C Sector is a key component of the nation's critical infrastructure. As a result, it may in the future become the target of attacks from numerous quarters. In response, the sector must work to protect critical I&C assets, both those that serve the sector itself and the I&C products and services deployed in other industry sectors.

Presidential Decision Directive 63 ordered the development of sector-specific critical infrastructure protection plans and established the role of private industry sector coordinators. The I&C Sector has four organizations sharing this role and co-producing this document: the Cellular Telecommunications and Internet Association (CTIA), the Information Technology Association of America (ITAA); the Telecommunications Industry Association (TIA); and the United States Telecom Association (USTA).

Section One of this plan outlines the critical infrastructure assurance problem and identifies what steps must be taken to assure operational continuity. The purposes of this plan are to:

- provide an understanding of the technical and business environment in the Information and Communications Sector;
- define, in global terms, the threats and vulnerabilities associated with the environments;
- articulate the existing and ongoing activities of the I&C Sector in response to the concerns for protecting the critical infrastructures;
- and, indicate the future efforts that may be required to protect the I&C infrastructure.

[1] Internet Week, "IT Scrambles to Restore Order," Mitch Wagner, September 20, 2001

This plan also identifies a series of I&C Sector "First Principles." These principles must guide subsequent action in responding to the critical information infrastructure challenge.

Section Two puts critical infrastructure assurance into context. A realistic perspective is important in formulating a coherent sector approach to this issue. The I&C Sector must protect its own operations—and recognize its products and services are used to protect the infrastructure assets of other sectors. The challenge requires creating commercial solutions while simultaneously anticipating and responding to third-party attacks. Other variables include evolving customer requirements, product turnover, emerging technology and business models. The plan explores threats, vulnerabilities, interdependencies and the management of associated risks.

Section Three looks at how roles are established and partnerships built. The I&C Sector combines regulated and unregulated elements. Part of the challenge implicit in this plan is to understand what aspects of critical infrastructure assurance are properly industry led and government supported, and those that require more active government participation. Consideration is given to public-private partnerships, as well as the impact and, at times, unanticipated consequences of legislation on the provision of critical infrastructure assurance.

Section Four of this plan considers next steps. The I&C Sector is characterized by a marketplace in constant flux. Businesses will use I&C products and services that are different from those available today in applications that either cannot be foreseen or only briefly glimpsed through the power of imagination. Knowing that change is the only constant, the I&C Sector must be prepared to take a series of steps now and in the future that safeguard critical infrastructure components.

1. Background and Scope

During the past 50 years, the Information and Communications Sector (I&C) has grown to become an intrinsic part of the nation's critical infrastructure, as well as a key driver of global economic growth. As such, the sector recognizes that it has become the potential target of attack from numerous quarters. The sector also understands it has a responsibility to safeguard critical I&C assets, both those that serve the sector itself and the I&C products and services deployed in other industry sectors. The following plan has been assembled to outline the critical infrastructure protection problem and to explain what steps must be taken by industry and government to assure operational continuity. This section:

- introduces the four Department of Commerce-designated I&C Sector coordinators;
- describes the major market and economic trends in the information and communications technology industry;
- defines the purpose and objectives of this plan;
- and, identifies a series of I&C Sector "First Principles" in responding to critical information infrastructure challenges

A. Background

The Report of the President's Commission on Critical Infrastructure Protection, issued in October 1997, reaffirmed that the Information and Communications (I&C) Sector is vital to the national well being and that all critical infrastructures (*e.g.*, energy, banking and finance, transportation, water systems and emergency services, both government and private) are increasingly dependent on information technology and telecommunications systems. The Commission recommended a comprehensive program based on public-private partnerships to reduce vulnerabilities and on information sharing to protect information and communications as well as other critical infrastructures.

The Sector Coordinators

Presidential Decision Directive 63 (PDD 63) designated the U.S. Department of Commerce as the lead agency and the National Telecommunications and Information Administration (NTIA) as the Sector Liaison Official for the I&C Sector. As the lead agency in the U.S. Government for the physical and cyber protection for the I&C Sector, NTIA has worked closely with the I&C Sector via the Consortium for Infrastructure Protection. On February 25, 1999, then Deputy Secretary of Commerce Robert Mallet announced the creation of a private sector consortium of associations (*i.e.*, Information Technology Association of America (ITAA), the Telecommunications Industry Association (TIA), and the United States Telecom Association (USTA)), to act as the

Sector Coordinators for the I&C Sector. The Cellular Telecommunications & Internet Association (CTIA) recently joined these three associations as an additional Sector Coordinator for the I&C Sector.

While the consortium well represents the overall I&C Sector, each of the members of the consortium represents the varied interests of its respective memberships.

The Cellular Telecommunications & Internet Association

The Cellular Telecommunications & Internet Association (CTIA) is the international organization representing all elements of wireless communications, serving the interests of service providers, manufacturers, and others. As the voice of the wireless industry, CTIA represents its members through constant dialogue with policy makers in the Executive Branch, the Federal Communications Commission, and Congress. CTIA's industry committees provide leadership in the areas of taxation, roaming, homeland security, safety, regulations, fraud and technology.

CTIA distributes timely, factual and reliable information to members, policymakers, the investment community, customers and the media on the latest policy, regulatory and technology developments. While coordinating the industry's efforts to be responsive to concerns about wireless health and product usage issues, CTIA also operates an equipment testing and certification program to ensure high quality and reliability for consumers. CTIA runs an extensive anti-fraud program involving detection, prevention, investigation and research.

CTIA is also the parent of CIBERNET, the global leader in wireless transaction financial settlement for voice, data and m-commerce. CTIA also established The Wireless Foundation, a not-for-profit organization, which provides grants to worthwhile projects demonstrating the benefits of wireless communication to education, health care and job creation/productivity.

Information Technology Association of America (ITAA)

ITAA provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 500 direct corporate members throughout the U.S., and is part of a global network of 46 countries' IT associations. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields.

ITAA has been the leading IT trade association voicing industry concerns and positions on cyber threats and vulnerabilities. As one of the I&C Sector coordinators designated by Presidential Decision Directive 63, the Association worked with member companies to form the Information Sharing and Analysis Center (ISAC) for the IT industry, and also serves on the Board of Directors for the Partnership for Critical Infrastructure Security (PCIS), a public-private partnership addressing cross sector concerns and interdependencies.

Telecommunication Industry Association

The Telecommunications Industry Association (TIA) is the leading trade association serving the communications and information technology industry, with proven strengths in market development, trade shows, domestic and international advocacy, standards development and enabling e-business. It is accredited by the American National Standards Institute (ANSI) to develop American National Standards used in the telecommunications industry. Through its worldwide activities, the association facilitates business development opportunities and a competitive market environment. The association provides a market-focused forum for its more than 1,100 member companies that manufacture or supply the products and services used in global communications. TIA represents the communications sector of the Electronic Industries Alliance (EIA).

United States Telecom Association

USTA has been serving its member companies for more than a century. Over that time telecommunications technology and regulation have undergone tremendous change. With the introduction of competition into the local loop and emerging technologies that build and maintain the international information infrastructure, the telephone industry faces challenges and opportunities virtually unimaginable just a decade ago. USTA's full membership is comprised of facilities-based telecommunications carriers, including incumbent and competitive local exchange carriers as well as Information Service Providers (ISPs), wireless and cable companies. It includes three of four regional bell companies and more than 1,000 independent companies.

USTA associate members are businesses that have a professional interest in telecommunications. These include telephone companies operating outside the United States, information service providers, cellular providers, paging providers, television providers, publishers and businesses that provide products and services to the telecommunications industry, such as manufacturers and suppliers of telecommunications equipment, consultants, accounting firms and other telephone associations.

In response to the increasing globalization of telecommunications, USTA has added a special class of "international member" for companies and governmental agencies that

provide facilities-based local telephone service in other nations. This broadened approach to USTA's forums permits people from local exchange carriers around the world to meet with their peers to discuss and master the many complex issues they face in common. International members have the opportunity to participate in USTA committees and other USTA forums to address issues of interest to local public telecommunications network providers.

B. The Information and Communications Business

Information Technology Industry

The U.S. is the world leader in information and communications technology (ICT) products and services, representing almost 35 percent of global spending. U.S. spending on ICT has increased almost 70 percent since 1993, to over $810 billion in 2001.[2]

Information technology has been an incredibly powerful source of American employment and job growth. Approximately 10 million people earn their livings performing information technology jobs, 85 percent of which work for small companies. This count includes companies both in and outside of the IT industry. Almost 14,000 IT companies in the U.S. employ 50 or more employees.[3]

The IT industry has contributed to U.S. economic growth in other important ways. According to the Department of Commerce, the IT industry accounts for a full third of all real economic growth and half of all productivity growth between 1995 and 1999. IT has helped the economy contain inflation with an average annual computer price decline of 26 percent between 1995 and 1999.

In customer terms, the financial services industry is the single biggest consumer of IT products and services, spending over $70 billion in 1999. This industry is followed by communications services ($61.7 billion), manufacturing ($56.9 billion), wholesale ($50.1 billion), business services ($41.2 billion), retail ($18.7 billion), real estate ($17.1 billion) and transportation ($16.8 billion). At 24 percent, transportation and business services have experienced the highest average annual rate of IT spending growth between the years 1994 and 1995. This is followed by real estate, retail and manufacturing at 17 percent, financial services at 14 percent, and communications services and wholesale, both at 12 percent.[4]

While the IT industry has its legacy firmly planted in mainframe computers and software, its future appears to be in mobility platforms, peer-to-peer networks, content rich

---

2 Digital Planet 2002, World Information and Technology Services Alliance and IDC, February, 2002

3 When Can You Start?, The Information Technology Association of America, April, 2001

4 The Precursor Group, Independent Research, April 11, 2001

broadband applications, intelligent devices and more. Understanding the concept of convergence is critical to understanding the future of information technology itself. Convergence takes place in numerous ways. During the 1990s, advances in computer processing power and software functionality and ease of use coincided with dramatic price declines, making IT both widely available and readily useful for a wider range of people and businesses than ever before. The conversion of analog voice, music, graphics, and video files to digital formats collapsed barriers and elevated multimedia. Meanwhile, common standards for computer networking allowed for the integration of disparate computational devices, with the Internet protocol triggering a worldwide communications and knowledge-sharing phenomenon. The business community has responded to these developments with mergers and acquisitions that further blur the traditional distinctions between infrastructure, application and content providers.

Convergence will no doubt continue far into the future, with the integration of computer hardware, software and communications into real-time applications found at home and at work. Companies like FedEx and Hertz have been at the vanguard of this movement. While it is not clear to what extent wireless devices will blossom beyond cell phone usage and become true information utilities, the potential for this to happen seems clear and the possibilities limitless. Indeed, computer power will transition from the data center and desktop to thousands of points of interconnection—whenever and wherever people use information.

The Telecommunications Industry

The industry continues to outpace overall economic growth and, indeed, to drive it as businesses find it imperative to invest in technology that enhances customer care and streamlines operations. Service providers, having invested in bandwidth and the creation of capacity, are now investing in software and applications to make use of those solutions to provide the value-added services that are especially appealing to small and mid-size businesses. In a transport market that is becoming highly price-competitive, service providers are using applications as a means to differentiate themselves and are seeking to customize their offerings, thereby reinforcing customer loyalty and creating new revenue streams.[5]

The overall U.S. telecommunications market (equipment and services) grew by 12.5 percent in 2000, generating revenues of $609.2 billion. Spending on telecom equipment continued its double-digit growth, recording a 13 percent increase over 1999, reaching $159.8 billion. Spending on transport services reached $287.6 billion in 2000, an increase of 8.9 percent over 1999.

Specialized services, which consist of unified messaging, voice messaging and broadband Internet access increased to an estimated $5.8 billion, up 62.2 percent over 1999. Enterprise spending on professional and technical services in support of voice and data

[5] "2001 Multimedia Telecommunications Market Review and Forecast", TIA, January, 2001.

communications equipment reached $138.3 billion in 2000, while network service providers spending in support of network infrastructure equipment increased to $29.9 billion.

Enterprise spending on equipment and software reached $92.1 billion; network service providers spending reached $53.2 billion. Continued demand for bandwidth to facilitate high-speed Internet access, Voice-over-Internet Protocol (VoIP), convergence and high-level applications will drive the equipment market, offsetting anticipated declines in wireless infrastructure spending and a slowdown in spending on voice communications equipment.

There are several factors that will continue to affect the nature of the telecommunications industry and the telecommunications infrastructure: Convergence, next generation networks (NGN), increasing business reliance on IT and telecom, deregulation of the telecom industry, and consolidation of industry players in both IT and telecom. A brief overview of each factor and its implications is provided below:

Convergence

In recent years, growth in telecommunications activity has been largely focused on purely digital means, employing digital protocols such as the Internet Protocol (IP) and Asynchronous Transfer Mode (ATM). Circuit switched networks still carry significant amounts of traffic, but the trend towards digital will continue and the historical circuit switched network will be subsumed in a combined or "converged" structure. This converged network will preserve the essential elements of the historical switched network, incorporate those elements that are applicable in the new structures (such as wideband fiber optic facilities) and discard those that are not useful (such as circuit switching systems). Essential services such as operator assistance, alternate billing for calls, toll free calling and emergency services such as 911 will be preserved. The service structures of the new and emerging networks, in which implementations are made at the terminal ends or at the network edge, will also continue to flourish. In that regard, the converged network of the future will be a true hybrid, able to act in accordance with the wishes of the customer, transmitting intelligence in a transparent manner via digital means, and providing network intelligence resources or not, depending on customer demands.

The evolution, as described above, will continue long into the future, with vestiges of the older network being incorporated or discarded as technology and service trends continue to evolve. The situation is dynamic and will continue to be so.

Next Generation Networks

The evolving network, or more accurately, a series of interconnected networks and facilities, is configured to provide for competition in technical innovation and

entrepreneurial innovations in business. For many years, the competitive model has also been evolving, which permits an ever-increasing number of companies to interconnect with the established networks of traditional telecommunications service providers and with each other. This increased interconnection activity provides for much greater diversity, but it also requires diligence on the part of new entrants to assure that the necessary levels of network security are provided. In addition, the Federal Communications Commission and state regulatory commissions need to address national security policy when they review existing regulations and consider new requirements.

To expand on this point, the conditions of the Telecommunications Act of 1996 require widespread interconnection in which many different carriers connect at multiple points in the network. With a proliferation of interconnected networks, the large number of paths available can increase the resiliency and durability of the network structure in the event of attack, either from intentional attack or other causes. A major challenge is to evaluate and understand the implications of widespread interconnection among multitudes of carriers and the resulting effects on network reliability and service transparency.

Competition, Choice and Security

The highly competitive business environment for integrated digital communications is itself an important consideration. One of the benefits of competition is cost efficiency for consumers. Service providers must work to assure that the value-added nature of network security not be lost in the push to generate low-cost solutions.

All service providers have a clear economic stake in reliability of their service provision, and many of them have regulatory as well as business obligations with regard to protection of proprietary and customer information. Balancing cost, security and reliability factors is done on a company-by-company basis. As a result, competitive networks are by their nature variable and do not conform to a consistent set of expectations. Customers must understand that information security solutions correlate to risks involved. They must have a range of competing options. And they must be able to match their requirements to products and services that best meet their needs.

Consolidation of Industry Players

The highly competitive nature of the terms of service provision in the current environment as well and economic conditions in the marketplace can be expected to foster the launch of new companies, the failure of others, and the combination of still others into newly merged organizations or business partnerships. This pattern of consolidation and redefinition of business relationships will characterize the telecommunications sector well into the future.

In many cases, these arrangements may be for provision of assets required by a service provider in support of a particular project. Other arrangements of virtually unlimited

variety in their conditions prevail in the industry and many are created and others dissolved on a regular basis.

The effects of these interrelationships between companies that are otherwise unrelated in combination with the churn of new business creations and failures must be continuously factored into the understanding of the environment when considering network reliability and security.

C. Purposes, objectives, and target audience

The purposes of this plan are to: provide an understanding of the technical and business environment in the Information and Communications Sector; define, in global terms, the threats and vulnerabilities associated with the environments; articulate the existing and ongoing activities of the I&C Sector in response to the concerns for protecting the critical infrastructures; and, indicate the future efforts that may be required to protect the I&C infrastructure.

The objectives of this plan are: to provide a common understanding of the infrastructure and the protection concerns associated with the infrastructure, and to establish a set of processes to assure that adequate and appropriate protection measures are identified, implemented, maintained and updated as conditions change.

D. Call to Action

Information security is a lynchpin of homeland and economic security. Incentives to strengthen homeland cyber defense are driving industry efforts to continue building partnerships with government organizations. Combined with that reality and an ever-changing technical, competitive, and regulatory environment, the I&C Sector uses a variety of approaches to address critical infrastructure assurance risks. At a minimum, the I&C Sector is committed to the recognition of the following facts and principles:

- Industry owns and operates most of this infrastructure and, therefore, is its natural steward for safety and security issues;
- Government and industry share an interest in the health and growth of the Internet and E-commerce and must find common ground on which to coordinate on critical information infrastructure protection issues;
- Government entities at the federal, state, and local levels need to better coordinate their national security activities before they seek to impose new requirements on the industry, to avoid duplicative, unnecessary or inconsistent requirements;
- Stakeholders must be able to trust that the I&C infrastructures are a safe and secure environment; and

- "Cyber ethics" must become a regular and understandable part of the Internet lexicon. Ethical online behavior must be taught at home, in school and in the workplace.

Because the I&C infrastructure is a global medium where national boundaries are transparent, infrastructure protection is an issue that must be pursued on a global basis.

The nature of the cyber-crime threat is dynamic; critical infrastructure assurance requires on-going commitment, attention, and cooperation of industry and law enforcement worldwide.

Industry's call to action must be executed based not only on its own economic needs but must be in concert with our nation's critical infrastructure policy objectives, both domestically and internationally.

2. Threats, Vulnerability and Risk Management

The I&C Sector is unique among infrastructure industries in that critical infrastructure assurance tools and practices must be simultaneously embraced by I&C companies for their own operations and implemented within the products and services they offer to companies in other industries. The challenge here is formidable. I&C Sector companies must develop critical infrastructure assurance solutions while, almost at the same time, these solutions become the target of third-party contravention. Meanwhile, customer needs for information security vary, the pace of product change accelerates, and new modes of computing, such as wireless data, make dramatic alterations to prevailing business practices and the underlying information architectures. This section of the plan explores threats, vulnerabilities and the management of associated risks. Specifically, topics addressed are:

- The multi-dimensional nature of the threat
- Forces amplifying the threat
- Vulnerability assessment
- Sectoral initiatives
- Sectoral interdependencies
- I&C Sector risk mitigation activities

A. Threats and Vulnerabilities

The horrific events of September 11 demonstrated the tremendous resilience of the I&C Sector to even the casual observer. Less well understood, perhaps, is the fact that the level of the threat to information and communications systems has been rising steadily as an increasing number of people and organizations connect to networks. Government and industry alike are becoming more reliant on the Internet for critical services. This reliance has increased not only the vulnerability of these organizations to electronic attack, but also the potential damage such attacks can inflict. The rapid growth of the Internet has dramatically increased the number of potential targets.

Information technology took a huge hit on September 11, both in human terms and physical destruction. Many IT professionals died in the attack, including management and technical professionals from Akamai, Accenture, BEA Systems, Cisco Systems, Compaq, GENUiTY, Metrocall, SAIC, Wipro, Oracle, Sun and Verizon. Much of the destruction consisted of property, including computers, software and data. One estimate places losses in IT resources by the financial community alone at $3.2 billion. Morgan Stanley estimates losses of IT hardware, restoration of services, long-term IT costs to enterprises and annual World Trade Center IT spending at over $25 billion.[6]

---

[6] Internet Week, "IT Scrambles to Restore Order," Mitch Wagner, September 20, 2001

I&C Sector
National Strategy Input

In the midst of disaster, this sector -- a complex web of people, technology, products and services—responded brilliantly. The I&C Sector absorbed the blow and came back strong.

From the first passenger phone calls on the doomed American and United Airlines flights, information and communications technology has played a critical role in helping authorities understand the dimensions of and respond to this national emergency. In the immediate aftermath of the World Trade Center attack, voice, data and video communications became critically important for understanding the scope of the disaster, directing relief efforts and locating missing people. Unfortunately, some of the necessary communications infrastructure was located at ground zero:

- Verizon's switching office at 140 West St. in Manhattan, supporting 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites
- AT&T lost fiber-optic equipment in the World Trade Center and had switching equipment damaged in a nearby building. Remarkably, AT&T switching gear in the basement of the World Trade Center continued to function
- Internet Service Provider Earthlink lost two of 14 dial-up numbers in the downtown area
- Sprint PCS's wireless network in New York City lost four cells
- Cingular Wireless lost six Manhattan cell sites
- WorldCom lost service on 200 high-speed circuits in the World Trade Center basement

A spokesman for AT&T called the square mile around Wall Street "the most telecom-intensive square mile in the world."[7]

Exacerbating the situation, the spike in demand for communications on September 11 proved to be enormous. Websites like the New York Times, CNN and NBC News had zero percent availability between 9 and 10 a.m. that morning.[8] Traffic slowed on the Internet, with average response times from the most popular e-business sites slipping from 2.5 to seven seconds.[9] AOL Instant Messenger logged 1.2 billion messages—100 times usual message volumes.[10] AT&T reported that long-distance traffic doubled by midday. Verizon also said its call volume in Manhattan was roughly twice the normal

---

7 IDG News Service, "Carriers Report Steady Recovery in Manhattan," Scarlet Pruitt, September 21, 2001

8 Network World, "Internet, Telecom Networks put to Test in Wake of Terrorist Strikes on U.S., September 17, 2001

9 Internet Week, "Site Operators Regroup," L. Scott Tillett and Tim Wilson, September 20, 2001

10 Interactive Week, "Safety Net," Randy Barrett *et al*., September 17, 2001

115 million per day.[11] Cingular Wireless experienced a 400 percent increase in call attempts.[12]

But the bottom line is that even with all of this destruction and intense demand, telecommunications in Manhattan and Arlington, VA, scene of the Pentagon attack, bent but did not break. The Internet provided millions of users with an alternative route around clogged or destroyed New York circuits, providing a frantic public with critical services for finding loved ones—services like e-mail, instant messaging, and voice over the Internet phone calls.

Meanwhile, communications carriers scrambled to reroute their fiber optic cables, re-map circuits to new locations, and roll in Cell-site on Wheels Systems (COWS). Some firms provided wireless telephones to disaster site workers. One week after the attack, Verizon announced that it had restored 1.4 million of 3.5 million data circuits, and the New York Stock Exchange had phone and data service to 14,000 of its 15,000 lines.[13] The exchange handled 2.37 billion transactions without incidents on its first day back in operation. In fact, many customers in New York found that their communications problems stemmed not from destroyed telecommunications hardware but from power failures and stalled diesel generators.

The nature of the threat to the I&C Sector falls into several categories. Most incidents are intended to disrupt or annoy computer users in some fashion. "Script kiddies" using broadly available hacking tools, for instance, may cause more annoyance than actual damage. The combination of limited knowledge and powerful tools, however, heightens the risks involved. Distributed denial of service (DDoS) attacks crash servers and bring down websites through the concerted targeting of thousands of e-mail messages to specific electronic mailboxes. Viruses, trojans, and other types of malicious code introduce phantom computer software programs to computers, designed intentionally to corrupt files and data. Other online intrusions are conducted to deface websites, post political messages or taunt particular groups or institutions. Even though no one stands to profit, damages caused by such attacks can run from the trifling to the millions or billions of dollars.

What motivates these attackers? Hackers may view the attack as a technology challenge, may be seeking to strike a blow against the "establishment," may be looking for group acceptance from fellow hackers, or may be just indulging themselves in a perverse thrill. Still, others may be acting on behalf of formal organizations or even countries and are engaged in some level of cyber warfare.

---

11 Dow Jones, "Verizon Says It's Ready for Trading," September 18, 2001

12 Computerworld, "Nation's Networks See Sharp Volume Spikes After Attacks," Bob Brewin, September 17, 2000

13 Dow Jones, "Verizon Says It's Ready for Trading," September 18, 2001

Other attackers hope to profit from their intrusions by stealing valuable or sensitive information, including credit card numbers, social security numbers, even entire identities. Targets of opportunity also include trade secrets and proprietary information, medical records, and financial transactions.

For some cyber criminals, the Internet is a channel for the dissemination of child pornography and a tool used in the furtherance of other crimes against children and adults. These crimes include fraud, racketeering, gambling, drug trafficking, money laundering, child molesting, kidnapping and more.

Cyber terrorists may seek to use the Internet as a means of attacking elements of the physical infrastructure, like power stations or airports. As we have seen in the Middle East and other regions, cyber terrorists encouraging political strife and national conflict can quickly turn the Internet into a tool to set one group against another and to disrupt society generally.

Another class of cyber criminal and, unfortunately, the most common is the insider who breaks into systems to eavesdrop, to tamper, perhaps even to hijack corporate IT assets for personal use. These could be employees seeking revenge for perceived workplace slights, stalking fellow employees, looking for the esteem of peers by unauthorized "testing" of corporate security, or other misguided individuals.

Regardless of the category, the threat is real. A 2001 study produced by Asta Networks and the University of California San Diego monitored a tiny fraction of the addressable Internet space and found almost 13,000 DDoS attacks launched against over 5,000 targets in just one week. While most targets were attacked only a few times, some were victimized 60 or more times during the test period. For many small companies, being knocked off the Internet for a week means being knocked out of business for good.

The Computer Security Institute/FBI also documents the problem in a widely reported study on computer breaches, the "Computer and Security Survey." A 2002 survey of 503 security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities confirms "that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting."[14] "Ninety percent of respondents (primarily corporations and government agencies) detected computer security breaches within the last 12 months," with eighty percent of those respondents acknowledging "financial losses due to computer breaches."[15]

A public opinion poll by ITAA and Tumbleweed Communications that was released on December 11, 2001, "Keeping the Faith: Government, Information Security and

[14] Computer Security Institute Press Release, April 7, 2002.
[15] Computer Security Institute Press Release, April 7, 2002.

Homeland Cyber Defense," showed that over 70 percent of Americans are concerned about Internet and computer security. Another 74 percent expressed fears that their personal information on the Internet could be stolen or used for malicious purposes. An equal number said they are concerned that cyber-attacks could target critical infrastructure assets like telephone networks or power plants.

- Thirty-five percent of those polled said they are "very concerned" about Internet and computer security and 36 percent said they are "somewhat concerned."

- A full third of respondents said they are "very worried" about their personal information on the Internet being stolen or misused; 41 percent said they are "somewhat worried." Seventy-eight percent of respondents said they are either "very" or "somewhat" concerned that their government-held personal information could be misused.

- Seventy-four percent of respondents expressed worries about terrorists using the Internet to launch cyber-attacks against critical infrastructure. Thirty-seven percent said they are "very" concerned, while another 37 percent said they are "somewhat" concerned.

- Despite these fears, respondents failed to register major changes in online behavior as a result of the September 11 attacks or the war on terror. Only five percent said they find themselves using the Internet "a lot more" for updates and information, while 34 percent said their usage has stayed the same. Seven percent said they use the Internet "a lot less" since the September 11 tragedy.

- Likewise, even with the Anthrax events, e-mail has not become a replacement for paper mail. Fifty-five percent said their use of e-mail has not changed, while 35 percent said they do not use e-mail at all. Only three percent said they have made a significant shift to e-mail to avoid paper mail.

- The survey contained good news and bad news for federal officials. While only 17 percent of respondents expressed "complete faith" in the ability of the U.S. government to prevent cyber attacks against agencies, 54 percent said they have "some" faith and only 17 percent said they have "very little faith." Big brother fears also appear to be at a minimum. Few in the survey appear concerned that in the post-September 11 environment their e-mail will be subjected to government sleuthing. Only ten percent said they are "a lot more" concerned about federal authorities monitoring or reading their e-mail, while 14 percent said they are "somewhat more" concerned.

In addition to threats to the critical information infrastructure emanating from external sources, risks exist as a consequence of the physical and logical architecture of the networks themselves. These risks include the adequacy and vulnerability of the physical

architecture and practices to secure it, including premises security, as well as risks associated with logical architecture, such as widely deployed software and protocols. Collateral risk arises from lack of attention to cyber security as focus of investments in threat modeling and simulation at universities and national labs.

The concentrated presence of physical technology assets creates the possibility of single points of failure. This reality coincides with historical patterns of population concentration and industrial activity, and poses significant costs to remedy.

Moreover, failure to employ techniques such as vendor diversity for servers, storage, switches, telecommunications networks and power supplies is of increasing consequence as one goes up the Internet food chain.

In addition to physical security issues, known deficiencies in widely deployed critical protocols, including the Berkeley Internet Name Domain implementation of the Domain Name System (DNS/BIND) and the primary routing protocol, Border Gateway Protocol (BGP), have led to extensive, but unfinished research efforts to develop new, secure versions of this critical code. These efforts are well underway, both from the voluntary consensus technical standards bodies (the IETF is completing its effort on a secure BGP) and from individual companies.

In addition, a "theoretical" risk arises from the continuing failure to invest in security R&D. Substantial assets—in the form of computer simulation and modeling capabilities at national laboratories and at major universities—can help the nation understand and respond appropriately to embedded systemic risks.

The overall threat is amplified by a variety of other factors:

- The pace of change and constant introduction of new technology adding complexity and the possibility of unanticipated consequences;
- The borderless Internet and an array of jurisdictional approaches to cyber-crime prevention, detection and enforcement creating safe havens for attackers;
- Ambiguous motivations and anonymous actors leading to greater tolerance for online misdeeds;
- Executive indifference and lack of awareness, limiting the resources dedicated to information security; and
- Limited numbers of workers with the requisite skills in information security.

B. Vulnerability assessments

I&C Sector
National Strategy Input

Information and telecommunications systems are high-priority targets not only because of our extensive dependence on these infrastructures for national, international and economic security; but because of the types of information they transmit, store and process. The I&C Sector represents a highly dynamic and competitive marketplace, delivering a formidable array of technology solutions. Customers adopt solutions on factors such as performance, suitability, scalability, reliability and price. Similarly, solutions may feature greater or lesser information security capabilities, based on market requirements. For instance, the critical infrastructure assurance requirements of the finance or petrochemical industries are apt to be far different from the needs of the fashion or food services industries. Business decision makers must make tradeoffs and, because security will not always win, risk management within the I&C Sector becomes more complex.

At the sector level, the President's National Security Telecommunications Advisory Committee (NSTAC) has been very active over the last several years in assessing the vulnerabilities of the communications infrastructure, especially the public switched telephone network (PSTN) and more recently the Next Generation Network (NGN). The assessments included physical, operational and technology vulnerabilities. The USTA has been a member of NSTAC since its inception in 1982, and for the last several years, both ITAA and TIA have participated in NSTAC activities.

In addition, to stay abreast of the constantly changing risk environment for National Security and Emergency Preparedness (NS/EP) issues, the National Communications System operates the National Coordinating Center (NCC) for Telecommunications, which is staffed by both federal government and telecommunications industry representatives. Traditionally, the NCC has supported and coordinated responses across a broad spectrum of events. Since its inception in 1984, the NCC has shared information on telecommunications outages to expedite recovery in an "all hazards" environment. Initially, "all hazards" generally referred to international crises, acts of war, and natural disasters. As technology has migrated towards, and become increasingly dependent on automated information systems, the concept of "all hazards" has expanded to include the electronic intrusion threat to operations, administration, maintenance, and provisioning (OAM&P), systems supporting NS/EP telecommunications. In response to PDD-63, the NCC expanded its operations to include cyber hazards via the implementation of a Telecom information sharing and analysis center (NCC-ISAC) to share information on significant physical and cyber events affecting the telecommunications infrastructure. The scope of the Telecom ISAC information sharing and analysis includes organizations, personnel, procedures, facilities, and networks employed to transmit and receive information by electrical and electronic means. (*See more on the NCC-ISAC on page 33 of this report*.)

The IT industry has also adopted a formal approach to the information sharing challenge. In January 2001, many of nation's leading high-tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to

cooperate on cyber security issues. The objective of the IT-ISAC is to enhance the availability, confidentiality, and integrity of networked information systems. (*See more on the IT-ISAC on page 32 of this report*.)

C. Interdependencies

Profound changes in the nation's infrastructures involving interdependency, deregulation, and reliance on technology are creating new challenges to the assurance of infrastructure services. A few particular infrastructures are so vital that their incapacity or destruction would significantly compromise the defense and economic security of the United States. No technology has been more responsible for this dramatic change and had a more profound effect on the other infrastructures than the I&C infrastructure.

The national critical infrastructure systems incorporate a mix of public and private ownership entities that bring to the table varying perspectives with regard to security, protection, and economic competitiveness. Private owners, faced with loss of revenue and loss of confidence by their customers, regulators, investors, and insurers, seek to restore revenue and customer confidence, satisfy regulators, document losses, and avoid liability. Governments focus on protecting national security, preventing future attacks, and identifying and punishing attackers. As a result of the dichotomy of interests, any solution to or recommendation for the protection of critical infrastructures requires the participation of private industry in concert with Government. In addition, there needs to be better coordination among Government entities at all levels to avoid duplicative, unnecessary or inconsistent requirements.

In January 1995, the Director of the National Security Agency briefed the National Security Telecommunications Advisory Committee (NSTAC) on threats to U.S. information systems and the need to improve the security of critical national infrastructures. Reflecting on that information, the NSTAC principals discussed emerging threats to information systems and subsequently forwarded correspondence on the matter to President Clinton in March 1995. It stated that:

> "[the] integrity of the Nation's information systems, both government and public, are increasingly at risk to intrusion and attack . . . other national infrastructures . . . [such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk."

President Clinton replied to the NSTAC correspondence in July 1995, stating that he would "welcome NSTAC's continuing efforts to work with the Administration to counter threats to our Nation's information and telecommunications systems." President Clinton asked the NSTAC, with "input from the full range of national information infrastructure

users," to assess the national security and emergency preparedness requirements of the nation's rapidly evolving information infrastructure.

The NSTAC took an early leadership role in raising awareness of the critical infrastructure protection issue and bringing focus to the cross sector dependencies of an increasingly digital economy. Through dialogue with Government, the NSTAC identified three priority critical infrastructures for assessment: electric power, financial services, and transportation. Specifically, the NSTAC examined each infrastructure's dependency on information technology and the associated information assurance risks to its information systems. Because these vertical industry infrastructures are highly dependent on I&C solutions, systematic evaluation of each infrastructure indicates much about the readiness of the I&C Sector. The NSTAC completed the risk assessments of the electric power, financial services, and transportation infrastructures in March 1997, December 1997, and June 1999, respectively. In each assessment, follow-up recommendations were sent to the President, many of which, although somewhat dated, remain valid, and some of which appear applicable to other critical infrastructures:

Information Assurance Task Force (IATF), Electric Power Information Assurance Risk Assessment, March 1997.
In March 1997, the NSTAC issued a report to the President that assessed the security of the electric power control networks and electric power grid. The NSTAC determined that the electric power industry was undergoing significant change, fueled by marketplace forces and federal legislative and regulatory activities.

The NSTAC found that this change was stimulated by new players entering the power generation and delivery market and by existing utilities being required to offer open access to their transmission systems. The previously tightly integrated functions of power generation, transmission, and marketing were being separated within utilities; and some were even spinning off into new companies. Utilities were also rapidly expanding their use of information systems and interconnecting previously isolated networks because of competition, aging proprietary systems, and reductions in staff and operating margins.

The NSTAC recognized that, while physical destruction was still the greatest threat facing the electric power infrastructure, electronic intrusion of the utilities' information systems and networks represented an emerging threat. The NSTAC concluded that the probability of a nationwide disruption of electric power through electronic intrusion, short of a major coordinated attack, was extremely low, but the potential for short-term disruptions at the regional level was increasing. The NSTAC found that the industry considered the primary threat to information systems to be from insiders. Downsizing, increased competition, and the shift to standard protocols would add to the potential sources of attacks, whether from inside or outside a utility.

The NSTAC also examined recent legislation that had increased the jurisdiction of federal, state, and local law enforcement authorities over attacks on electric power control systems. It found that the lack of effective reporting mechanisms, inconsistent use of logins, passwords, and warning banners, and a low probability of being detected, caught, and prosecuted hindered effective deterrence of potential attackers.

The NSTAC determined that the substations presented the most significant information security vulnerability in the power grid. The NSTAC also found that many of the automated devices used to monitor and control equipment within transmission and distribution centers and corporate data networks, widespread use of dial-up modems, and use of public networks were other sources of vulnerabilities in the electric power grid.

The NSTAC recognized that utilities used a variety of mechanisms to protect the electric power grid from disruption, including contingency analysis, redundant control centers, dial-back modems, and firewalls. However, few utilities had an information security function for their operational systems, and the lack of convincing evidence of a threat tended to lead senior managers to minimize critical infrastructure assurance investments.

Although the NSTAC's study found no evidence of a disruption of electric power caused by an electronic intrusion, it concluded that three trends would increase the exposure of the electric power control network to attack:

- The shift from proprietary mainframe control systems to open systems and standard protocols.
- Increasing use of automation, outside contractors, and external connections to reduce staff and operating costs.
- The requirement to provide open access to transmission system information dictated under Federal Energy Regulatory Commission orders 888 and 889.

The NSTAC included in its recommendation to the President that he consider assigning to the appropriate department or agency the mission to develop and conduct an ongoing program with the electric power industry to identify the threat and increase the awareness of vulnerabilities and available or emerging solutions.

IATF, Financial Services Risk Assessment Report, December 1997.
The NSTAC delivered a financial services Information Assurance (IA) risk assessment report to the President in December 1997. The study reflected that the financial services infrastructure was sufficiently protected and prepared at the national level to address a broad range of current threats, from natural disasters to electronic intrusions. However, the NSTAC found that there were security implications and potential vulnerabilities associated with the financial service sector's dependence on a telecommunications infrastructure being subjected to deregulation, the integration of dissimilar information systems and networks resulting from mergers and acquisitions, and the introduction of web-based banking services.

The study focused on three objectives:

- Assess the security and robustness of the financial services infrastructure at the national level relative to the identified threats to its networks and information systems;
- Determine the risks to the industry that derive from its dependence on the telecommunications infrastructure; and
- Examine the implications of trends regarding the industry's use of information systems and networks.

The NSTAC found that the financial services industry approached the protection of its networks and information systems as an integral element of an overall program of risk-management accountable to the most senior levels of an institution. This approach is long established in the industry and affects every investment decision. The approach also incorporates security measures as fundamental risk controls.

The NSTAC concluded that trends in banking, securities, and new technologies indicated that information systems and networks would continue to be the primary vehicles for innovation and competition, enabling money, value, and related commerce to move with increasing velocity. It was further determined that, although the industry had suffered from its reluctance to discuss security issues in open forums through perceptions fostered by the media that the situation was far worse than it was, the financial institutions were very aware of the threats facing them. The financial institutions were also committed to any necessary investments in protection measures and had extensive experience addressing natural and man-made disasters and infrastructure outages. These measures taken by the industry put successful cyber attacks beyond the scope of all but a concerted nation-state effort. Physical attack remained the larger concern.

Information Infrastructure Group (IIG), Interim Transportation Information Risk Assessment Report, December 1997; IIG Transportation Information Assurance Risk Assessment Report, June 1999.
The NSTAC initiated its transportation IA risk assessment in December 1996. The findings were included in an interim report to the President in December 1997. The report concluded that the transportation industry lacked a uniform understanding of information system risks and vulnerabilities, and the industry lacked consistent methods for assessing vulnerabilities or gauging information system security. The report also concluded that the transportation industry was generally skeptical that meaningful industry/government information sharing about system threats and vulnerabilities could be achieved.

The NSTAC came to the following six conclusions about risks to the transportation infrastructure:

- The transportation industry is increasingly reliant on information technology (IT) and public networks.
- Although a nationwide disruption of the transportation infrastructure is unlikely, even a local or regional disruption could have a significant impact.
- Business pressures and widespread utilization of IT make large-scale, multi-modal disruptions more likely in the future.
- There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.
- There is a need for closer coordination between the transportation industry and other critical infrastructures.

The NSTAC recommended that the President continue support for the efforts of the Department of Transportation (DOT) to promote outreach and awareness within the transportation infrastructure as expressed in Presidential Decision Directive 63. These recommendations included the timely dissemination of Government information on physical and cyber threats, support for research and development programs to develop methods to counter emerging cyber threats, joint industry/government efforts to examine emerging industry wide vulnerabilities, and future DOT conferences to stimulate information exchange on threats, vulnerabilities, and best practices.

D. Risk Management Approach

The I&C Sector believes a multi-faceted approach is needed to manage risks and improve U.S. cooperation on issues of information infrastructure assurance. Cooperation must

extend across industries and borders and bring together industry with government. Protecting our infrastructure is a collective responsibility. Elements of the I&C Sector approach include: Awareness, Education, Training, Best Practices, Research and Development, Information Sharing, Reconstitution, and International Coordination.

Awareness and Education

In general terms, promoting awareness and education is a standard practice within I&C Sector companies. The sector intends to continue to utilize industry associations to develop and sponsor education and training programs. Awareness and education are also considered a part of the outreach and awareness goals.

I&C Sector coordinator organizations maintain a proactive program of outreach to policymakers, including Congressional member briefings, breakfast briefings and other consultations on both the House and Senate sides; testimony before Congress; and regular meetings with White House and other Administration officials.

Awareness-raising must take place within the I&C Sector and through partnerships with other vertical industries, including finance, energy, transportation, and health services. The efforts should include regional events, conferences, seminars and surveys to educate all of these industries on the importance of addressing critical infrastructure assurance and the efforts of the I&C Sector to provide a reliable network infrastructure. An awareness raising campaign targeting the I&C Sector as well as vertical industries dependent on information, such the financial sector, insurance, electricity, and transportation could be overlaid with a targeted community effort directed at CEOs, end users and independent auditors. The goal of the awareness campaign would be to educate the audiences on the importance of protecting a company's infrastructure, and instructing them on how they can accomplish this. The message is that critical infrastructure assurance must become a top priority for businesses and individuals.

Awareness is necessary but not sufficient to move people to appropriate action. Education programs must provide the tools necessary to channel motivation into productive activity. For instance, in an effort to take a longer-range approach to the development of appropriate conduct on the Internet, the Department of Justice and the Information Technology Association of America formed the *Cybercitizen Partnership*. The Partnership is a public/private sector venture formed to create awareness in children of appropriate online conduct. This ongoing effort extends beyond the traditional concerns for children's safety on the Internet, a protective strategy, and focuses on developing an understanding of the ethical behavior and responsibilities that accompany use of this new and exciting medium.

The I&C Sector has maintained an active campaign to communicate the nature of the information security challenge and to educate businesses and consumers on how to respond. The campaign has numerous facets, including websites, newsletters, press announcements, national surveys and more. The National Cyber Security Alliance and its

"Stay Safe Online" campaign and website is one such program in the sector http://www.staysafeonline.info/.

Specific ITAA surveys have focused on cyber-crime, denial of service attacks, international perceptions of information security and government handling of sensitive information. Overall, ITAA members are making substantial investments in information security and in educating and training their employees to practice sound cyber-hygiene and to create a larger pool of skilled information security workers.

While the IT industry's education and outreach efforts have increased awareness, and investments in education and training are increasing, there is still considerable work to be done. Until information security is dealt with at the Board of Directors level and by senior management -- in companies big and small -- the issue will not likely receive the needed attention and investment within the corporate structure.

In an ITAA-sponsored forum in Washington, DC on "Strengthening Homeland Cyber Defense" on October 18, 2001, Duane Andrews, Executive Vice President of SAIC, said that the lack of decisiveness on the part of the government and industry to protect against cyber terrorism and cyber-crime before September 11th was because: a) cyber security is technically complex and hard to understand; b) every dollar that would go into protection and reaction is a dollar out of another budget; c) there are no mechanisms to make government or industry accountable; and d) cyber crime has always been treated as a tactical problem, rather than a strategic one. According to Andrews, that can no longer be the case and terrorism, in any form, must be treated as an act of war, rather than as a criminal act that can be dealt with in a court of law.

Andrews also emphasized the need for continued education for government and industry on the importance of cyber security and the sharing of know-how. Businesses, particularly small and medium sized businesses, are more concerned with the insider threat to their security, and while that is an area that should be dealt with, resources must be invested into all facets of cyber security protection. Further, Andrews reiterated the need for the government to invest in even the most basic steps in solving the cyber security problem. Sound system designs, strong system administration, and improved security training for personnel are among the most basic steps that have to be taken. Most of all, Andrews claimed, there must be a mechanism for accountability that will place the responsibility of an attack on those that have the influence to make the changes necessary to protect against future attacks.

At the same ITAA forum on October 18, 2001, David Langstaff, CEO of the Veridian Corporation, emphasized the need for every corporation to be coordinated with each other in this effort and for the challenge to be on the agenda of every CEO. Langstaff said that over 95 percent of the Internet is owned by private industry so it is crucial that the government develop a new legal structure that will allow for increased information sharing both within the private sector and between the private sector and government.

Such a structure would have to remove the current barriers to information sharing, such as existing FOIA language. Finally, Langstaff restated the need for the government to invest more resources and funds into fighting this very viable threat.

Participation in Regional Events

Key national audit and business risk communities have initiated an unprecedented collaboration to elevate awareness and educate Boards of Directors, executive management, and Chief Auditors of public and private institutions on information security. These communities are represented by The Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA), The Information Systems Audit and Control Association (ISACA), and the National Association of Corporate Directors (NACD).

The consortium of auditors and CPAs held a series of five regional conferences across the country, and kicked off a high profile event in Washington, D.C. on April 18, 2000. The consortium has developed guidance for Boards of Directors that was introduced in the meetings and to auditors and board directors across the country from April to September, 2000.

Firms that represent Wall Street analysts who provide information to investors participated, as well as representatives from the "Big Five" public auditing firms and insurance companies. Local chambers of commerce also supported the regional events.

Global InfoSec Summit and Industry Coalitions

The Global Information Security (InfoSec) Summits gather industry and government leaders from around the globe to discuss the critical issues of information security and infrastructure assurance. The first Global InfoSec Summit in October, 2000 raised awareness of the issues, promoted cross-national and cross-sectoral collaboration, helped identify policy needs, and highlighted InfoSec best practices and case studies. In addition, this series of Summits launched a global partnership for addressing InfoSec issues on an on-going basis. Just as the successful International Y2K Summit in London in October, 1998 had a major global impact on solving the Y2K challenge, this InfoSec program is expected to forge cross-industry cooperation towards building and securing the global economy. This series will continue in 2002.

Other industry coalitions with key U.S.-based multinationals also have been actively engaged in awareness and education efforts globally. The Global Internet Project, a coalition of senior international Internet executives, has developed a series that highlight Next Generation Internet security and reliability concerns. The Next Generation Internet or NGI is a generic phrase used to describe the Internet of the future. The phrase describes not only the network that transports bits between users, it also covers the middleware, the applications software, and the services that make those bits useful.

The Next Generation Internet will evolve from today's Internet as new technologies and new standards are deployed. The group, which includes senior executives from GENUiTY, IBM, Microsoft, and WorldCom, has worked to bridge the gap between technology and policy and has developed an agenda to help foster combined solutions to emerging security and reliability concerns as the Internet becomes more pervasive. The Global Business Dialogue on Electronic Commerce, a CEO-driven effort to promote global electronic commerce for the benefit of businesses and consumers everywhere, is also involved in cyber security efforts internationally.

The I&C Sector has been a long supporter of a major outreach and awareness effort known as the National Colloquium on Information Systems Security Education. The goal of the Colloquium is to create an environment for exchange and dialogue among leaders in government, industry and academia concerning the need for and utility of information security and information assurance education. Given the scope and fluid state of knowledge of information security, the Colloquium strives to foster the development of academic curricula to respond to the need expressed by government and industry, and is based on the recognized "best practices" available in the field. The Colloquium will assist educational institutions by fostering the continued development and sharing of information security education resources. The Colloquium will also encourage educational institutions to teach appropriate information systems security courses in various curricula to meet the needs of 21st Century consumers and to offer courses to meet the growing demand for information system security professionals. Since its inception in 1998, the Colloquium has sponsored four conferences.

Training

The I&C Sector believes it is important to assess the need for and train information security specialists, and strives to train every worker on how to protect systems. We know from denial of service attacks that systems are only as strong as the weakest link—whether it is people or technology. Elements of a sector approach include a security skills set study to determine critical infosec skills; a mapping of identified skills with courses taught (or not taught) at the university level; promotion of “university excellence centers” in this arena; and funding advocacy for scholarships to study critical infrastructure assurance.

The challenge to find information security workers is enormous because they frequently require additional training and education beyond what is normally achieved by IT workers. Many of the positions involving information security require U.S. citizenship, particularly those within the federal government, so using immigrants or outsourcing the projects to other countries is often not an option.

Best Practices

The I&C Sector is committed to promoting best practices for critical infrastructure assurance, and looks to partners in many vertical sectors in order to leverage existing work in this area. In addition, the I&C Sector is committed to working with the government—whether at the federal, state or local levels. For example, ITAA has worked with the federal government's CIO Council on efforts to share industry's best information security practices with CIOs across departments and agencies. At the same time, industry is listening to best practices developed by the government. The Internet Security Alliance (ISAlliance^{SM}) announced in April 2002 a roadmap for its best practices and Internet security policy initiatives. The ISAlliance was formed in April 2001 to serve as an industry voice and information exchange vehicle for its multi-sectored, international membership. The alliance is a collaborative effort among Carnegie Mellon University's Software Engineering Institute (SEI) and its CERT Coordination Center (CERT/CC) and the Electronics Industries Alliance (EIA), a federation of trade associations. The ISA Best Practices Working Group is focusing on two categories of best practices: strategic and operational practices. Within the strategic practice category, white papers have been submitted on security awareness and training, security strategy, security management, security policy and regulations, business continuity planning and recovery, security assurance, and risk metrics. Categories under the operational practices include monitoring and auditing, vulnerability management, encryption, incident management and general staff practices. Additional best practice development is planned in other key areas such as physical security, system and network management and system administration tools.

These exchanges of information will help industry and government alike in creating solutions without reinventing the wheel.

Research and Development

The I&C Sector spends hundreds of millions, if not billions of dollars on research and development efforts allowing the United States to maintain our nation's role as the leader in I&C products and services. However, there are gaps in R&D. Industry focuses on R&D projects that are likely to lead to real products. The government, mainly the Department of Defense, focuses its information security R&D spending on defense and national security issues. We believe that in between industry's market-driven R&D and government's defense-oriented R&D projects, gaps may be emerging that no market forces or government mandates will address.

To assist in identifying these gaps, throughout the I&C Sector, we have addressed the research and development issues via a series of workshops, primarily the NSTAC's Research and Development Exchange and the Telecommunications and Information Security Workshop (TISW).

NSTAC Research and Development Workshop

NSTAC Research and Development Exchange. Rapid advances in networking technology, coupled with the proliferating number of network providers, vendors, and

users, raise new security issues and increase the importance of researching and developing new technologies to protect the Next Generation Network (NGN). On September 28-29, 2000, the President's NSTAC sponsored its fourth R&D Exchange in conjunction with TISW2000. The purpose was to stimulate an exchange of ideas among representatives from industry, government, and academia on the security challenges posed by network convergence. Issues discussed at the R&D Exchange included:

- The shortage of qualified information technology professionals;
- The need to expand the Information Assurance Centers of Excellence and other educational programs;
- The need to develop a business case for security to encourage investments in security technology R&D;
- Requirements for best practices, standards, and protection profiles to improve the security of the NGN; and,
- The need to enhance R&D efforts to develop better testing and evaluation programs.

Information Sharing

Given the changing nature of the threat, companies in the I&C Sector recognize the need to have formal and informal information sharing mechanisms. Internet service providers demonstrate an example of the latter circumstance. Because these firms provide networking capabilities commercially, they often have extensive network security expertise. Such firms act as virtual Information Sharing and Analysis Centers, gathering information about detected threats and incursions, sanitizing it by removing customer specific data, and sharing it with customers.

Information Technology ISAC

On the information side of the I&C Sector, the ITAA has adopted a formal approach to the information sharing problem. In January 2001, nineteen of the nation's leading high-tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues. The objective of the IT-ISAC is to enhance the availability, confidentiality, and integrity of networked information systems.

The IT-ISAC is a not-for-profit corporation that will allow the information technology industry to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. The organization is a voluntary, industry-led initiative with the goal

of responding to broad-based security threats and reducing the impact of major incidents. Membership in the IT-ISAC is open to all U.S.-based information technology companies. It will offer a 24-by-7 network, notifying members of threats and vulnerabilities. The group also is clear on what it will not undertake. Excluded activities include: standards setting, product rating, audits, certifications or dispute settlement.

The nineteen Founding Member companies of the IT-ISAC, all represented at the announcement, are AT&T, Cisco Systems, Computer Associates, CSC, EDS, Entrust, Hewlett-Packard Company, IBM, Intel Corporation, KPMG Consulting, Microsoft Corporation, Nortel Networks, Oracle Corp., RSA Security, Securify Inc., Symantec Corporation, Titan Systems Corp., Veridian and VeriSign, Inc.

The group plans for its information sharing activities over time to evolve, starting with IT companies, moving across sectors and, perhaps, establishing similar ties with government agencies.

Telecommunications ISAC

An ISAC (Telecom ISAC) has been formed in the National Coordinating Center for Telecommunications (NCC). Building on the NCC's traditional role as the operational focal point for the coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities, the Telecom ISAC facilitates voluntary collaboration and information sharing among government and industry participants.

The Telecom ISAC gathers information about network vulnerabilities, threats, intrusions, and anomalies from various sources, including the telecommunications industry and the U.S. government. That information is then analyzed with the goal of averting or mitigating the effects of computer intrusions on the telecommunications infrastructure. Resulting reports and analyses are sanitized to remove proprietary and classified information and disseminated in accordance with sharing agreements established by the Telecom ISAC participants. To further analyze the threats posed by computer intrusions and other incidents, the Telecom ISAC will develop baseline statistics and patterns of actual or attempted intrusions and compile a library of historical data. The Telecom ISAC has a signed memoranda of agreement with the Department of Defense's Joint Task Force for Computer Network Defense, the Federal Computer Incident Response Coordinating Committee (FedCIRC), the National Infrastructure Protection Center (NIPC), and the IT ISAC and is pursuing similar agreements with other U.S. Government incident response centers. As of May 1, 2002, there were 22 members of the Telecom ISAC, including several companies from the aerospace and defense industry who, because of their existing membership in NSTAC, have chosen to join the Telecom ISAC rather than form a separate Aerospace and Defense ISAC.

A major project underway within the Telecom ISAC is researching the development of a Global Early Warning Information System (GEWIS). The GEWIS will analyze data on

network utilization from commercial carriers and other sources to monitor the health of the Internet and provide real-time alerts of attacks.

Network Security Information Exchanges (NSIE)

Another example of a formalized process in the telecommunications industry is the Network Security Information Exchanges (NSIE) process, which was established in 1991. The Government NSIE and the NSTAC NSIE are separate but closely coordinated groups of security practitioners from the U.S. Government and the private sector, respectively. The government NSIE is composed of members from federal departments and agencies that are major telecommunications service users, represent law enforcement and the intelligence community, or have information related to network security. The NSTAC NSIE is composed of industry members from telecommunications service providers, equipment vendors, and major users.

NSIE representatives are individuals who are engaged full-time in the prevention, detection, and investigation of telecommunications network software penetrations, or who have security and investigative responsibilities as a secondary or collateral function. The NSIE process provides a forum for identifying network security issues and exchanging information on threats to, incidents involving, and vulnerabilities affecting the public network. To support efforts to share information and heighten awareness of network security issues, periodically the NSIEs assess the risks to the public network from computer intruders. The most recent assessment was completed in 2002.

Standards Bodies

TIA maintains close working relations with Committee T1 and its Advisory Group on issues relating to telecommunications security standards. In addition, the Association has developed CIP standards presentations for ANSI, a standards group in Canada, and worked with the FCC's Network Reliability Council (NRC), and the Network Reliability and Interoperability Councils (NRIC) on network security issues. TIA meets periodically with other Standards Development Organizations (SDOs) from around the world to collaborate on high interest subject areas for cooperation. The meetings were referred to as Global Standards Collaboration (GSC7) and RAdio STandardization (RAST10) meetings. In a Resolution adopted in November 2001 in Sydney, Australia, the Participating Standards Organizations from Europe, USA, Canada, Korea, Australia, and Japan agreed high interest subjects should include:

- development of a compound security architecture and security guidelines for NGNs; and
- development of NGN-specific security protocols and APIs.

Due to the fact that NGN security is inherent but nevertheless crucial and is touching many areas and SDOs, this is an important standardization area within NGN, since security issues interrelate with architecture, QoS, network management, mobility, billing and payment.

One of the most significant challenges facing the design of NGN security standards is the fact that the networks are no longer conceived as monolithic systems with clear interfaces. Much of the standardization work in NGN security has to be based on guides and principles along with APIs so that a secure network can be built from a given selection of specific NGN components.

The SDOs in the Sydney meetings also agreed that lawful/legal interception standardization work programs, a new high interest subject, might include:

- definition of new packet-based transport "handover" interface between target network and law enforcement agency;
- enhancement of existing Intercept Related Information to include new data elements covering both signaling and multimedia streams; and
- consideration of technical solutions for all related issues that respect the privacy of un-related communications

Government Outreach

As the lead agency for the I&C Sector, in order to promote and encourage information sharing, NTIA holds bi-monthly meetings of the Communications and Information Sector Working Group (CISWG). The CISWG is a cross-sectoral group of industry and government representatives that meet to discuss sectoral CIP activities and provide information about domestic best practices and international CIP bilateral and multilateral activities. The CISWG's International Outreach Subcommittee has played a key role in promoting industry participation in U.S. delegations to bilateral negotiations and multilateral organizations in order to ensure that private sector views will lead the discussions on economic security. Also, NTIA has coordinated closely with the Sector Coordinators as we have worked to collaborate with the U.S. Government in providing industry input into the National Strategy.

In addition, NTIA has worked with Qwest at the Cheyenne Mountain military base in the Rocky Mountain Corridor to facilitate a vulnerability assessment performed by DOD as part of an assessment of I&C Sector vulnerabilities. This NTIA-DOD joint venture is the first for any USG lead agency. Building on the Rocky Mountain Corridor project, Hawaii will be the next geographic region to test this model, with NTIA facilitating the effort with Verizon. In Hawaii, in addition to the telecommunications infrastructure, the IT infrastructure is to be included for the first time in the assessment.

The I&C Sector will also continue to be supportive of NATO through the Office of the Manager, National Communications System and the State Department.

E. Reconstitution

The need for risk mitigation through system redundancy, business continuity and emergency back up is nothing new to the I&C Sector. This is the type of work performed by disaster recovery firms such as Sungard and Comdisco. These and other companies provide a critical safety net to their corporate and government customers. While the type and degree of services vary, the basic idea of disaster recovery service is to have a redundant set of applications and data available at a remote facility in case of emergency. Maintaining geographically dispersed facilities assures companies that a single attack or natural disaster cannot destroy their information assets.

Companies can, of course, elect to maintain their own dedicated networks and data storage facilities at off-site locations. Large companies with multiple data centers go this route, but even these firms may elect to have a disaster recovery contract in place to test systems and mitigate risks. Others with smaller budgets can take advantage of the cost efficiencies of the Internet and web-based data storage firms to acquire an important measure of disaster recovery support.

Unfortunately, many companies operate without this type of service in place. One vendor estimates that 150 of the 350 businesses in the World Trade Center bombing of 1993 experienced disruptions sufficient to put them out of business a year later.[16]

This suggests that Business Continuity Planning (BCP) may distinguish between companies that emerge from disasters with a future—and those that do not. A business continuity plan identifies the mission critical processes and applications of the company as well as the interdependencies both inside and outside the enterprise necessary to support such functions. The plan determines the potential impact of outages in each area and prioritizes them in terms of their impact to the business. In this methodical way, risks can be identified and contingency strategies developed. Strategies could include a decision not to take any action whatsoever, modifying or adapting the mission critical process in some way to avoid the perceived risk, maintaining the process as is but attempt to eliminate the risk itself, and identifying the steps that must be taken to recover if and when the interruption occurs.

One issue that needs further but quick examination is the need to create greater redundancy in our telecommunications infrastructure, particularly diversity of egress and ingress in buildings with major telecommunications facilities. Having backup telecommunications systems that are located in the same part of a building and that go in

[16] Ziff Davis Media, "Safeguarding Data," Max Smetannikov, September 17, 2001

and out of the building through the same pipes may create a false sense of security. This issue is especially important when essential government telecommunications systems are involved.

The I&C Sector also believes that a component of risk management involves the thorough analysis of security processes and methods, identification of vulnerabilities, appropriate corrective action and, as necessary, the utilization of cyber risk insurance policies to prevent additional losses. The very process of underwriting such policies often assures that a comprehensive security analysis will be conducted. Increasingly, such a review will become part of corporate due diligence and board of director awareness and oversight of these issues may eventually become a factor in the underwriting of Director and Officers' insurance policies.

A second related issue concerns recent attempts by the federal government to seek indemnification from private sector contractors performing security-related services. Placing such requirements on contractors will have one of two possible consequences: companies will find themselves unable to pursue homeland defense related government projects or, to the extent that companies do seek such business, competition may be limited to the most aggressive, least financially stable businesses. Rather than asking companies to assume such risks, the federal government should act to give agency secretaries discretion under Public Law 85-804 to grant liability immunity to contractors performing homeland defense related services.

The telecommunications side of the I&C Sector has significant experience in the area of reconstitution. The primary vehicles, at a sector level, to assure reconstitution capabilities are vested in joint government/industry activities: Government Emergency Telecommunications Service (GETS), the Telecommunications Service Priority (TSP), and, the Telecommunications Electric Service Priority (TEPS) programs. These are in addition to service provider company-wide programs and resources and best practices issued as a result of the FCC's NRC/NRIC activities. The FCC has launched an NRIC VI which has the needs of public safety and interoperability as key focus areas for study.

Government Emergency Telecommunications Service (GETS)

The NCS established GETS to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized government users engaged in NS/EP missions. GETS satisfies these requirements by providing emergency access and specialized processing in local and major long distance telephone networks as well as government leased networks including the defense information system network. GETS ensures federal, state and local government and other authorized users of a high rate of successful call completion during network congestion or outages arising from natural or man-made disasters. Recent technological advances in networking have made telephone services increasingly more vulnerable to disruption by natural or man-made disasters. As a result, GETS increasingly plays a critical role in maximizing use of all available

telephone resources when outages occur. GETS had a completion rate of 95 percent following the September 11 terrorist attacks.

Telecommunications Service Priority (TSP)

The TSP program is the regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service. Qualified services include those used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that could cause injury or harm to the population, damage property, or degrade or threaten the NS/EP posture of the United States. TSP is mandated by the Federal Communications Commission on telecommunications service providers. The NCS administers the TSP program. TSP plays an important role in prioritizing telecommunications vendors' responses to outages. Following natural or technical disasters, these vendors might become overwhelmed with requests for new services and requirements to restore existing services. The TSP Program authorizes and requires service vendors to provision and restore TSP-assigned services before non-TSP services and provides those vendors with legal protection for giving preferential treatment to NS/EP users. Any organization (*e.g.*, federal government, state and local governments, private industry, or foreign government) that has telecommunications services supporting an NS/EP mission is eligible to participate.

Telecommunications Electric Service Priority (TESP)

In the event of electric power disruption, utilities use emergency systems to prioritize restoration of power. These electric service priority (ESP) systems reflect primarily essential state and local needs during peacetime conditions and typically include life support, medical facilities, and police and fire stations. The Telecommunications Electric Service Priority (TESP) initiative requests that electric utilities modify their existing ESP systems by adding a limited number of specific telecommunications critical facilities that service National Security and Emergency Preparedness (NS/EP) requirements. Typical NS/EP functions include national security leadership, maintenance of law and order, maintenance of the national economy, and public health, safety, and welfare. For the TESP, "critical facilities" are defined as those that perform functions critical to the monitoring, control, support, signaling, and switching of the voice telecommunications infrastructure. Participation in the TESP is voluntary. Participants include states, electric utility companies, telecommunications carriers, the U.S. Department of Energy (DOE), and the NCS.

F. International Issues

Regardless of industry, companies seem to recognize that critical infrastructure assurance must be addressed as an international issue. American companies increasingly are global corporations, with partners, suppliers and customers located around the world; conversely, international companies increasingly target the U.S. market for business

expansion and establish domestic subsidiaries. Interdependencies among players abound. This global business environment has only been accentuated by the emergence of online commerce: business-to-business and business-to-consumer alike. Companies also realize the need to take the lead in driving a business-focused critical infrastructure assurance agenda. As a result, several groups have either formed in direct response to this requirement or expanded their mission to embrace critical infrastructure assurance issues. These groups include:

- The Business and Industry Advisory Committee (BIAC) to the Organization for Economic Cooperation and Development (OECD) which has placed cyber-crime prevention on its agenda. BIAC has sought to assure that industry maintains a "seat at the table" in government attempts to craft cyber-crime fighting measures.

- The Global Business Dialogue on Electronic Commerce (GBDe) is an international, CEO-level group seeking to promote the benefits of electronic commerce. GBDe launched the Cyber Security Working Group last year in the belief that the future of the digital economy hinges on a secure Internet, and that there exists a rapidly increasing need to improve cyber security and fight cyber crime.

- The Global Internet Project (GIP) is an international group of senior executives committed to fostering continued growth of the Internet. Members come from leading Internet-centric companies representing the telecommunications, software, financial services, and content sectors. GIP participants are well-known leaders in the Internet revolution and represent companies based in Australia, East and South Asia, Europe, and North America. The group pursues an active agenda of critical infrastructure assurance related issues, including network reliability, encryption, and cyber-crime.

- The Partnership for Critical Infrastructure Security (PCIS) pursues cross-sector initiatives and complements public-/-private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security. Specific PCIS working groups focus on issues such as interdependency, information sharing and public policy. The group is expanding its scope to address cross-border critical infrastructure assurance issues. Each of the I&C Sector coordinators has a board seat at PCIS.

- The World Information Technology and Services Alliance (WITSA) is a consortium of 46 information technology (IT) industry associations from economies around the world. WITSA members represent over 97 percent of the world IT market. In October 2000, WITSA hosted the first international summit on critical infrastructure assurance issues. Event tracks focused on information security, education, law enforcement, emerging standards, and specific sector performance.

- NTIA's International Outreach Subcommittee has also been at the forefront of international CIP activities. Through the work of the Subcommittee, NTIA promoted industry's goal to participate in bilateral negotiations on CIP issues. In August 2001, during the U.S. - Australia CIP Bilateral in Canberra, nine private sector or industry representatives participated for the first time. Government and industry met together on the first day of the bilateral, followed by a second day of industry-to-industry and government-to-government meetings. A standards discussion with public and private sector representatives took place on the third day. As a result of the bilateral with Australia, the State Department concluded that it would be advantageous for industry representatives to participate in all future CIP negotiations. In May, 2002, five private sector representatives participated in an industry-to-industry CIP discussion organized by the U.S. Embassy in Rome. On the second day, the industry representatives also attended a CIP industry-government conference coordinated by the U.S. Embassy and the Italian Prime Minister's office. During the government-to-government bilateral that took place while the industry discussions were underway, both U.S. government and Italian government representatives stated repeatedly that they look forward to industry participation in future CIP bilateral discussions.

3. Industry and Government Roles

In building appropriate roles for critical infrastructure protection within the I&C Sector, one must recognize that this industry combines regulated and unregulated elements. By definition, industry and government are in the quest for protecting the nation's critical infrastructures together. Part of the challenge, therefore, is to understand what aspects of critical infrastructure assurance are properly industry-led, and those that require more active government participation. This section considers:

- Defining the relationship
- Industry roles and responsibilities
- Government roles and responsibilities
- Legal and legislative issues, including the Communications Assistance for Law Enforcement Act (CALEA) and the Freedom of Information Act (FOIA)

A. Defining the Relationship

The Information and Communications Sector consists of numerous and varied corporate entities, publicly and privately held. These multi-variate entities develop and observe a variety of corporate, financial and technology standards, practices, public (federal and state) policies, regulations and guidelines. How should these pieces fit together?

Defining roles and responsibilities in a National Strategy intended to protect the critical infrastructure of the United States is a daunting task. The danger in doing so is to oversimplify and, by so doing, render the attempt ineffective. Beginning this process by outlining fundamental principles for agreement is entirely appropriate.

The National Plan for Information Systems Protection[17], a framework for Critical Infrastructure Assurance partnership, version one, observed:

> "[*T]he Federal Government alone cannot protect U.S. critical infrastructures. Private industry and state and local governments directly own, effectively control, or greatly influence the large majority of the infrastructures that are vital to our national security and economic well being*."

The report further stated that the role of the federal government includes:

- Development of a relevant case for action to urge the private sector into motion;
- Sharing information with the private sector about threats and potential remedies;
- Supporting the private sector to design its own defensive programs;

---

[17] *Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to Dialogue.* The White House, Washington, D. C., 2000.

- Providing incentives for the private sector to implement those programs;
- Removing obstacles to private sector action (*i.e.*, information sharing);
- Spurring research and development; and
- At times, providing overall national leadership.

The earlier plan noted that the role of private industry is to:

- maintain robust and reliable service delivery systems;
- maintain customer confidence; and
- ensure integrity in the face of new threats and vulnerabilities.

The earlier plan also observed that the conduct of this activity will be strengthened by a "partnership" between industry and government. A partnership can be defined as " a relationship resembling a legal partnership usually involving close cooperation between parties having specified and joint rights and responsibilities."

How can the practical elements of close cooperation and "specified and joint rights and responsibilities" be established? The nation's growing dependence on the I&C infrastructure suggests that the relationship between the federal government and private sector infrastructure providers may need to be redefined with respect to "specified and joint rights and responsibilities."

Version 1.0 of the National Plan Report provided a set of partnering principles :

- Voluntary
- Mutual concerns, with achieving clear, focused, well-defined goals(s)
- Key complementary capabilities and roles exist between the participants
- Mutual understanding of each participant's values, expectations, needs, concerns, and individual objectives
- Persistent/frequent interaction
- Starts with planning

The I&C Sector offers the following additional observations for going forward:

- Government must be able to characterize its expectations of the private sector, *e.g.*, industry response to threats;
- Identical conditions are not pervasive across the I&C Sector; different levels of performance and degrees of resistance to disruption carry different price tags;
- Industry must be prepared to state its capabilities and relate performance to cost;
- Partners must define a process by which accommodations/understandings are reached;
- Stakeholders must realistically take into account the differences in environment among the carriers and other companies involved;

- Partners must define a management process for implementing joint understandings;
- Parties must share a definition of extraordinary conditions under which rules are suspended;
- Both sides must be agreeable to continuous re-negotiation of the relationship and the projects under changing business and technical state of the art conditions;
- Government should continue to rely on industry's voluntary working relationship and avoid unfunded mandates; and
- Government should not use legislation as a mechanism to compel industry action against its will.

These principles are broadly stated, but can be highly effective in moving government and industry to more detailed understandings. Interactions on this basis will be new to a significant degree, but not totally without precedent. There are many organizational interactions that come very close to this type of operating environment. For instance, the NCC acted as the telecom focal point during the Y2K transition, and more recently, has transitioned into the Telecom-ISAC.

B. Essential Ingredients for a Solution

The Critical Infrastructure Assurance Office (CIAO) draft outline for the National Plan presented the following sample policy statement:

> "It shall be the policy of the United States that physical or cyber disruption of the operations of any of the critical infrastructures should be rare, brief, limited geographically, manageable, and minimally detrimental to the national security, economy, essential government service, and public health and safety".

The I&C Sector agrees but notes that expectations must be realistic. It is unlikely that the nation's critical infrastructure will reach a state wherein no attacks are successful and no disruption occurs. An environment can be created, however, where reasonable levels of security are achieved.

Development of this consensus agreement, along with definition of the details of the actions and objectives of the parties to this effort, must be developed among those parties. Acceptable levels of risk are likely to vary by industry. For example, it may be that the I&C Sector can accept greater levels of intrusion than the Banking and Finance Sector. Greater levels of security will require greater effort, greater expense, and greater interruption of normal business operations. For those reasons, the details as to the development necessary to reach the end state conditions for each sector must be unique, but subject to a common rationale.

C. Industry Roles

One of the primary roles of industry is to assure that private enterprise provides reasonable, cost effective levels of security and reliability. At the sector level, continuing awareness and education, best practices, outreach, applied research and development, and information sharing programs assist this work. (*See Section 2*).

Another primary role is to periodically assess the sector level vulnerabilities and risks with the same or similar approaches as used by the NSTAC over the last few years. It should be noted that these assessments consider both the information technology and communications aspects of the I&C Sector and other infrastructure sectors.

Through the Sector Coordinator Consortium of CTIA, ITAA, TIA and USTA, industry should act to bring together the disparate entities within the sector and assist in the efforts to develop best practices and lessons learned. On a going forward basis, some of this work will be done under the FCC's NRIC VI initiative.

D. Government Roles

Beyond partnership, the federal government has a set of roles and responsibilities that it alone can undertake. The Administration, for instance, must bring substantial leadership to the critical infrastructure assurance arena and help raise the nation's level of awareness about cyber attacks and preventive measures. The responsibility is both national and international. The U.S. has critical defense and trade relationships around the globe. A breakdown in any link of this chain can have cascading consequences. It is, therefore, incumbent on the U.S. Government to accept its global critical infrastructure assurance role and educate foreign governments as to the nature of the threat and how to respond to it. Industry stands ready to work with multinational organizations and NGOs to help in this process.

Other roles for the federal government are:

- Coordinating national critical infrastructure assurance policy across agencies of government. On an individual basis, John Koskinen performed this role admirably as the government's Y2K "czar." The Homeland Security Office and the Critical Infrastructure Protection Board must work in concert with industry to elevate the importance of critical infrastructure assurance.

- Agencies should adopt strong critical infrastructure assurance practices. This means eliminating the ability of hackers to penetrate government websites and other information assets. The federal government can contribute significantly to a closer working partnership with the private sector on critical infrastructure assurance matters by making the exchange of information about intrusions, viruses and other disruptions truly a two-way street. Willingness to achieve this

worthy goal will no doubt facilitate the work of industry ISACs, the FBI's National Infrastructure Protection Center (NIPC) and other groups.

- Taking the lead role in the arrest and prosecution of cyber criminals. Existing law may be sufficient to punish malicious hacking, denial of service attacks and other illegal online activities. Working with industry to keep abreast of change and to avoid unintended consequences, government must identify where loopholes in existing law exist and close them. Government must also work with international counterparts to harmonize legal frameworks.

- Advancing pre-competitive research on Internet security. The Internet itself and many related innovations are the result of federally funded research. The federal government likewise can play a critical role by funding research on Internet security.

- Funding agency efforts to achieve an adequate level of critical infrastructure assurance. Asking agencies to improve their information security processes and train their people without the requisite budget increase is little more than a rhetorical exercise.

E. Legal and Legislative Issues

- The CALEA Experience and Lessons Learned

Public policy and effective critical information assurance are inextricably linked. As government and industry strive to create a balanced partnership, legislation and regulation must not hamper the ability of the parties to perform their security functions, create undue burdens or financial hardships, or favor one partner at the expense of another. Partnership building with Executive Branch agencies accomplishes little, however, if trust and good will are dissipated. This could occur through enactment of overly broad new laws or the inability of lawmakers to adapt laws on the books to meet the nation's new digital realities.

The Communications Assistance for Law Enforcement Act (CALEA) is a case in point. In the early 1990s, representatives of law enforcement and the telecommunications industry deadlocked on the issue of introducing very costly new network capabilities for law enforcement surveillance. Passage of CALEA broke the deadlock and mandated industry development of a capability standard and gave the Federal Communications Commission (FCC) regulatory oversight. The industry proposed standard has been challenged by law enforcement. The FCC has upheld the bulk of law enforcement objections. The U.S. Court of Appeals has vacated most of the FCC's decision. The FCC recently responded to the court's ruling by reaffirming the obligations it imposed in its earlier decision. The FBI also challenged TIA's ANSI accreditation but subsequently

withdrew that assault when new management took over the CALEA Implementation Section.

Meanwhile, the law contained many complex provisions for cost recovery by carriers, with implementation costs Congress arguably under-funded. The situation improved when the FBI agreed to fund development of the basic wiretap capability with the major switch vendors. A plan for flexible deployment capability has also been of value.

Other effects of CALEA have since surfaced. The Telecommunications Act of 1996 (the "Act") required local telephone carriers to make fundamental changes in their operations to encourage competition at the local exchange level. The Act also required that all subsidy arrangements become explicit, and that the price of service be moved toward cost. Local telephone carriers could no longer simply add the costs of meeting new requirements, such as CALEA, with a set profit percentage. In this situation, CALEA applied only to the regulated local exchange, cellular, and PCS carriers.

The Act introduced a multitude of requirements that foster competition in the local exchange market. CALEA engendered complex and costly requirements on the incumbent carriers.[18] In such a situation, the incumbents had no choice but to take all steps available to reduce to the greatest extent possible the costs that would result.

The CALEA experience underscores the need for cooperative rather than confrontational approaches to technology specification development and critical infrastructure assurance. Ironically, by the time the capabilities required by CALEA have been deployed, much of the specified technology may no longer be in use. To avoid delays and assure balanced partnership approaches, the federal government should likewise avoid legislation that creates un-funded mandates or unilaterally imposes formal obligations on industry. The government also must be sensitive to the industry's ability to develop and obtain compliant equipment within specific timeframes. Any partnership between government and industry that satisfies the security needs of government and the business requirements of industry will be an ongoing one and will require complex and extended activities that must be carefully managed.

- Legal Obstacles to Information Sharing Between Industry and Government

In addition, other public policy factors could act as barriers to critical infrastructure assurance, particularly in the information sharing area. Information sharing between the public and private sector and within the private sector is vital to the security of the nation's infrastructure. Comprehensive information sharing will not occur until the legal and economic obstacles to information sharing are removed.

[18] These requirements, in many regards have special additional requirements for cellular and wireless carriers, particularly with regard to determination of physical location.

One obstacle to information sharing between industry and government is related to the *Freedom of Information Act (FOIA)*.

Government agencies seek detailed data about computer attacks for the purposes of better law enforcement, earlier detection, and the promotion of best practices in government and industry. Today, however, corporate counsels advise their clients not to share voluntarily the details of computer attacks with government agencies because it could come back to haunt them. In their judgment, the risk that such data could ultimately be divulged through the Freedom of Information Act (FOIA) – even over the agency's objections – is unacceptably high.

Pending legislation in the U.S. House of Representatives (H.R. 2435, Davis-Moran) and U.S. Senate (S. 1456) corrects this situation by protecting the information from disclosure. The bills also provides limited use protection (not immunity) so that critical infrastructure information disclosed to the government cannot subsequently be used against the person submitting the information.

The legislation to alter the legal risk assessments necessarily carried out by corporate counsel also addresses concerns about sharing information within industry. The legislation includes a limited immunity for antitrust purposes for information shared solely for the purposes of facilitating the protection of critical infrastructures. We accept the assurances from the Department of Justice that business review letters would be forthcoming for information sharing and analysis centers (ISACs) constituted under the Administration's policies. Yet the issuance of even a set of such letters would prove inadequate, for at least three reasons. First, such ISACs would have to be constituted with a view toward satisfying the Department, as opposed to maximally fulfilling their primary mission. Second, there is the unavoidable negative implication for numerous other affected parties not in possession of a business review letter. Third, the ISACs are not the only organizations that have been constituted to share cyber threat information among industry sector members or with Federal agencies.

Beyond federal FOIA and antitrust, the proposed legislation goes on to clarify that computer attack data shared voluntarily with the government would not be disclosed either under the Federal Advisory Committee Act (FACA) or under state FOIA laws. We do recognize the federalism question that the second provision raises. At the same time, homeland defense is creating a need for federal, state, and local bodies to work jointly to a previously unprecedented degree. In some instances, first responders will not be from federal agencies. Information sharing ought not to dead-end at the federal level but should flow all the way down to the first responders. Without the same protection at the state level as at the federal, state agencies will face the same lack of revealing detail that federal agencies are experiencing today.

There has been, in our view, misunderstanding of the legislation by some critics. First, we are not calling into question the existing FOIA case law, which taken together

suggests that a federal agency would win a test case. Rather, we are saying only that the risk of a loss of such a test case – as viewed by the parties bearing the risk – remains unacceptably high. More importantly, corporations should not be required to accept such risks, or the cost of litigation, when reporting significant cyber events in an attempt to protect the public interest. Second, this legislative package has only to do with disclosure of computer attack data and critical infrastructure protection. Normal regulatory information gathering will proceed unimpeded, as it should.

The bottom line is that there is uncertainty about whether existing law may expose companies and industries that voluntarily share sensitive information with the federal government to unintended and potentially harmful consequences. This uncertainty has a chilling effect on the growth of all information sharing organizations and the quality and quantity of information that they are able to gather and share with the federal government. The I&C Sector is strongly in favor of removing disincentives to information sharing and that is why we support legislation in U.S. House of Representatives and the U.S. Senate to address these issues and that also will help sustain and strengthen voluntary information sharing models.

- HIPAA

Other issues of legislative and regulatory interest to the I&C Sector are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Financial Services Modernization (Gramm Leach Bliley) Act of 1999. HIPAA covers health care plans, clearinghouses and providers performing administrative and financial transactions electronically, and is intended to protect all medical records and individually identifiable health information used by covered entities. I&C Sector firms that may be affected by the HIPAA regulations include software companies, claims or bill processing firms, electronic data interchange providers, biometrics firms, record storage companies and more. While requiring that health care companies provide a high degree of patient privacy and medical record confidentiality, the government has rightly left the job of deciding how these protections are to be afforded to the private sector.

- Gramm-Leach-Bliley

Gramm-Leach-Bliley requires banks to post privacy notices and give customers the ability to block the sharing of records with outside parties. The Act also requires financial institutions to maintain formal critical infrastructure assurance programs, covering data security and confidentiality, risks and unauthorized data access. Elements to be addressed in such plans include access control, encryption, and change management, monitoring systems, incident response and disaster recovery. Again, because of the high degree of reliance banks and other financial institutions have on the I&C Sector, Gramm Leach Bliley creates implicit requirements for I&C firms in the financial services industry.

- Council of Europe Cyber-crime Convention

The Council of Europe Cyber-crime Convention was improved in many respects through the efforts of the U.S. delegation. However, the I&C Sector was disappointed to learn that several changes of critical importance to U.S. industry, privacy groups and noncommercial interests were not adopted in the final version of the Convention. For example, the Convention does not address the lack of reimbursement for compliance with surveillance mandates, lack of standard privacy protections for law enforcement requests, and potential liability for complying with requests. Therefore, we are concerned that implementation of the Convention will produce a patchwork of costly and inconsistent requirements worldwide that create significant market access barriers for communications companies, and undermine user privacy.

One important area of particular concern in implementation of the treaty is proposals by foreign governments to mandate that Internet and telecommunications companies maintain, for between one and seven years, massive logs reflecting every innocent user's communications over their networks, or to mandate that companies install new surveillance technologies. The Council of Europe Cyber-crime Convention that the U.S. Government helped to negotiate neither requires nor prevents such mandates.

The data retention mandates would require communications companies to retain enormous amounts of data that they do not retain in the ordinary course of business. Data would have to be retained about every user, without any showing that these users were suspected of engaging in illegal activity. The mandates would compromise user privacy, create costly barriers to entry for U.S. companies seeking to enter foreign markets, and threaten the security of user data by creating a ripe target for hackers. In some countries, such as Holland, service providers are subject to unique surveillance technology standards requirements, which create barriers to deploying international networks in those countries.

4. Next Steps

The I&C Sector confronts a technology landscape that is apt to change dramatically in the next five years. Businesses will use I&C products and services that are different from those available today in applications that either cannot be foreseen or can be only briefly glimpsed through the power of imagination. Knowing that change is the truest watchword, the I&C Sector must be prepared to take a series of steps that safeguard critical infrastructure components. This section describes:

- Immediate steps to be taken in response to current realities
- Some of the technology trends wielding the most powerful influence over the industry
- The impact of these trends on information security and critical infrastructure protection

A. Current Realities

The September 11 attack has caused I&C Sector companies to rethink the nature of their information security vulnerabilities. The shift has meant a refocusing from cyber-crime to defending against the far more sweeping impacts of cyber terrorism.

On July 19, 2001 the Code Red worm infected more than 250,000 systems in just 9 hours. The worm scanned the Internet, identified vulnerable systems, and infected these systems by installing itself. The infestation decreased the speed of the Internet, caused sporadic but widespread outages among all types of systems, and forced the White House to change its website address. The Code Red worm spread again on July 31, 2001 at 8:00 PM EDT and infected a similar number of systems. The second attack could have been much worse. Rapid mobilization of the Internet community by agencies of government, industry trade associations, and private sector companies brought extensive international media coverage of the Code Red worm; in less than a week, organizations downloaded over one million copies of the preventive patch.

Organizations working in unison to stop the worm spread were: The National Security Council (NSC), National Infrastructure Protection Center (NIPC) of the FBI, Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, Joint Task Force for Computer Network Operations (JTF-CNO) of the Department of Defense, and Federal Computer Incident Response Center (FedCIRC) of the General Services Administration, Computer Emergency Response Team Coordination Center (CERT/CC) of Carnegie Mellon University, Systems Administration and Network Security (SANS) Institute, Microsoft, Internet Security Systems, Inc. (ISS), Cisco Systems, Inc., Partnership for Critical Infrastructure Security (PCIS), Information Technology Association of America (ITAA), Digital Island, Inc., Information Technology Information

Sharing and Analysis Center (IT-ISAC), NCS, NCC, the Telecom ISAC, Internet Security Alliance (ISA), UUNet, and America Online.

The fast action of so extensive a group demonstrates the ability of the U.S. Government and industry to work together effectively in the face of a common threat. The experience validates the existence and capability of a virtual emergency response network within the I&C Sector. Attacks will no doubt continue into the future, although the type and severity of the event is apt to change. It is not yet clear whether the ad hoc nature of the emergency response team is beneficial, allowing participants to vary as attacks vary, or whether a more formal mobilization process is warranted. Answering this question is an important next step. If industry and government do not collaborate to minimize the impact of threats such as the "Code Red" or "Nimda" worms, the impact of such threats will grow and spread into other IT-enabled portions of our nation's critical infrastructures.

Uneven international response to the Code Red worm situation points up the need for more global solutions to the critical infrastructure assurance challenge. A possible next step is the creation of an International Critical Infrastructure Assurance Coordinating Center. Such a center would promote the sharing of best practices in information security, reporting of and coordination on cyber-crime incidents, and sharing information both inter and intra-industry among countries. The center would increase collaboration among governments, multilateral institutions, businesses, and NGOs. The common goal would be to increase public education, harmonize national cyber-crime laws, promote best practices, and energize global community efforts to protect critical infrastructure.

The Code Red worm, the “I Love You” Virus, Nimda, Goner, and similar threats have raised the public profile of critical information assurance. A second “next step” issue is to continue to enhance the new structure that was set up by Executive Order in mid-October 2001, including formalizing the NIAC and its relationship with the private sector and CIP coordinating committee in charge of relations with industry.

Within the U.S., other important next steps include:

- Explore how industry-specific Information Sharing and Analysis Centers (ISACs) can be mobilized for inter-industry information sharing.

- Develop relationships between law enforcement and the private sector that are built on trust and meaningful cooperation. Such relationships will not be created overnight. Improved information sharing between government and industry will be a step forward. Companies that participate in programs such as InfraGuard will become more comfortable in working with law enforcement. Once legal obstacles to information sharing between industry and government are overcome, companies could become more willing to share sensitive information with law enforcement and other federal agencies. Law enforcement may be able to assist in private sector screening of security personnel for past offenses;

- Determine the extent to which legislative initiatives in areas such as tax credits, liability protections, student loans, and other areas can influence organizations and individuals to adopt key critical infrastructure assurance goals and objectives;

- Appropriate and authorize additional funds to cover the cost of critical infrastructure assurance enhancements within federal agencies and to permit them to invest in pre-competitive research and development;

- Ascertain what vulnerabilities may be created as the public increasingly uses wireless devices and wireless LANs to conduct Internet-based transactions.

B. Trends for the Future

Many I&C Sector executives believe that in the not too distant future, society will function in a truly digital world, transformed by Internet technology. The Internet will be ubiquitous, seamless and integrated into every walk of life. Just as the power grid is always available, the Internet Protocol will be found in and on everything – cars, home appliances, clothing and more. The number of handheld devices connected to the Internet is expected to exceed the number of PCs so connected by 2003. The Internet will allow billions of intelligent devices to communicate – forming a virtual information bubble around individuals, anticipating and addressing many needs.

Voice over the Internet raises an entirely new category of security concerns. In the circuit switched environment, voice traffic can be intercepted; but the process has its limitations. Wiretapping requires telephone conversations to be monitored or recorded as they take place. With voice over the Internet, voice records are stored and, in addition to being vulnerable to real-time interception, may become the target for subsequent network intrusion.

The proliferation of broadband technology raises the bar for critical infrastructure assurance. The "always on" nature of cable modems or Digital Subscriber Line (DSL) connections raises questions about the security characteristics of tens of thousands of residential computers. Attack tools make the identification of vulnerable machines fast and easy. Such home-based machines may be the target for privacy invasions or theft of valuable assets. They may also become the staging area for subsequent denial of service attacks on critical infrastructure components. In the future, broadband technology will deliver content of increasing value to homes and businesses alike. With increased value comes the increased likelihood of attack.

The growing e-commerce space, mobile commerce and the very real prospect of digital ubiquity magnify the challenges of critical infrastructure assurance. In the old economy

and in the new, more businesses are using technology to manage operations, sales, employee relations, partnerships, and supply chains. More revenue is derived and more cost savings realized from online activity. Yet the same companies and organizations that devote considerable financial and human resources to physical security pay much less attention—or, sometimes, virtually no attention—to cyber security. In the same way, a business cannot properly function without sound financial processes and systems; similar prerequisites are necessary for managing network activity and the valuable, critical information that flows through the network.

Internet security measures must be addressed at the CEO and Boardroom level of every company and by political leadership at all levels. Until information security is dealt with at the Board level and by senior management -- in companies big and small -- the issue will not receive the needed attention and investment within the corporate structure. This process also applies to government at every level. Until government leaders recognize this as a key issue that must be dealt with through both education and financial investments in technology and management processes, we remain a nation at risk.

C. Conclusions

Any next steps for the I&C Sector must remain consistent with certain fundamental principles. A principled approach will help stakeholders communicate their positions and understand their differences, respond more effectively to change, and most importantly, meet the nation's requirement for critical information assurance and a vibrant information and communications industry. These principles include:

- The need to maintain industry leadership in the development and deployment of information security standards, practices and solutions; and

- Industry self-regulation is absolutely critical. This step will assure that actions taken will meet the test of the marketplace and the needs of customers; correlate in an affirmative and dynamic way to risks involved; and allow those closest to and with the best understanding of the problems involved in critical information assurance to define the solutions.

Next steps must recognize the diversity of interests in the expanded I&C Sector community and be prepared to adapt accordingly. This diversity includes the types of companies that will be interconnecting their products and services; the ways that customers will be using those resources; the high probability that technology and business models prevalent today are apt to be very different tomorrow; and the shifting points of leverage innovation creates throughout the nation's information infrastructure.

Along with a commitment to diversity is an understanding of the technical and economic interdependence of stakeholders. Critical infrastructure assurance can only be as good as its weakest link. In a world of e-commerce convenience and e-government service

delivery, organizations failing to embrace strong information security practices and procedures place others at risk. Interdependence must be accepted as both a right and a responsibility for all involved.

Because the situation now and in the future is highly dynamic, the response structures needed to address critical infrastructure assurance must be voluntary and ad hoc. While industry and government must be fully prepared to work together in response to infrastructure attacks, the nature of each episode is likely to be quite different. Static bureaucratic approaches and inflexible organizations are not sufficient to meet a constantly changing threat.

Critical infrastructure protection is vital to national economic security. The nature of the U.S. economy has changed and information and communication technology are basic to its performance abilities. Maintaining a strong posture on critical infrastructure protection will vouchsafe the nation's economic future; a highly disciplined attitude and broad acceptance of this fact is a key principle for moving forward.

With an understanding and acceptance of these principles, stakeholders can build a better, richer, more information driven society for future generations. The I&C Sector stands ready to do its part.

Other specific recommendations:

- ***Expand opportunities for information sharing.*** Information sharing and analysis centers (ISACs) must be established immediately in the critical infrastructure sectors where they are not yet present. Public-private information sharing must also be expanded (possibly through facilities modeled after the FBI's successful InfraGuard program). Finally, existing legal barriers to industry cooperation (*e.g.,* antitrust laws), and to industry-government cooperation (*e.g.,* the Freedom of Information Act) must be addressed.

- ***Increase awareness of critical infrastructure threats and defenses.*** The physical threat to critical infrastructure networks has not been sufficiently explored, and must be if we are to comprehend fully CIP. Neither can we assume that we have pinpointed all of the cyber threats to critical infrastructure. CIP must be considered a task of the highest priority, and treated as such. We should stop assuming that strikes against critical networks will be strategic, and consider the possibilities if they are tactically combined with physical attacks.

  Increase spending on cyber-defense. A truly comprehensive and effective plan will require the outlay of more money than ever before on cyber-defense. Government and private sector organizations must realize that this is not a "fail and fix" problem. Recovering from cyber attacks will always be more expensive than preparing for them; budgetary sacrifices in the name of prevention are

necessary. The federal government spent an estimated $3 billion to address the Y2K crisis. It should spend at least that amount, and probably much more, on cyber-defense.

- ***Increase training and education for individuals on the front lines of cyber-defense.*** Government (and industry, but to a much lesser extent) faces the possibility of a near-term dearth of qualified technical staff to fill its cyber-defense needs. Proposals to provide education subsidies to or forgive student loan debts of future government technical workers should be reexamined and revived. Continuous training should be used as an incentive not only for bringing in new staff, but also for keeping government cyber-defense employees in their jobs.

- ***Establish response and recovery assets and procedures to ensure critical infrastructure attack survivability.*** The successful response to and recovery from a critical infrastructure attack depends on the ability to ensure the continued functioning of the networks that are hit. Thus, a certain redundancy of systems is required, up to and including the creation of wholly separate networks for crucial government functions (*e.g.,* the proposed GovNet). It may also be worthwhile to consider the establishment of a separate Federal Emergency Management Agency (or perhaps a new bureau in the current one) to address specifically cyber attack response and recovery.

- ***Coordinate internationally to facilitate the investigation and punishment of cyber-crimes.*** Critical infrastructure protection is not now nor will it ever be a security concern solely of the United States. Any nation that depends on the efficient functioning of domestic or global cyber networks has a stake in CIP. International coordination of cyber-crime laws and cross-border sharing of information on threats and attacks is crucial to stemming the global expansion of cyber-crime.

The I&C Sector coordinators are pleased to have had an opportunity to develop this plan and make a contribution to raising new awareness of the issues contained herein. CTIA, ITAA, TIA and USTA stand ready to discuss any of the issues covered in this document and look forward to working with stakeholders on future development of a national strategy for critical infrastructure protection and cyberspace security.

Appendix 1

Advisory Committee Planning Statements

- The President's National Security Telecommunications Advisory Committee (NSTAC)
- NIAC
- NRIC

NSTAC-specific Next Steps

The President's National Security Telecommunications Advisory Committee (NSTAC) will be undertaking an assessment of the policy/technical issues related to the evolving public network supporting National Security/Emergency (NS/EP) communications. The scope of the assessment is bounded as follows:

Internet Architecture/Security Task Force (IASTF)

- Recommend a process for identifying pervasive software/protocols utilized on the Internet's critical infrastructure
- Extend current efforts to define the significant national "boundary" or "edge" elements of the Internet
- Integrate NSTAC efforts to define and monitor the significant critical infrastructure (i.e., Government, Department of Defense, and other sectors) supporting elements of the Internet with existing and developing activities

Vulnerabilities Task Force (VTF)

- How should industry address current and future physical (including human) and logical security issues?
- Should industry participate in Government-sponsored network assurance and vulnerability modeling and simulation activities?
- What sort of policy issues can NSTAC extract from the Network Security Information Exchanges Security Requirements Working Group activities related to the need for minimum baseline security requirements?
- What policy actions are required to eliminate any possible vulnerabilities stemming from the Internet Corporation for Assigned Names and Numbers issue?
- What policy actions are needed to eliminate vulnerabilities resulting from the lack of formal information sharing and notification processes for incidents and vulnerabilities (e.g., the ad hoc process in which Simple Network Management Protocol was communicated)?

Wireless Task Force (WTF)

- Investigate issues related to ubiquitous rollout of Wireless Priority Service (WPS)
- Determine national security and emergency preparedness users' unique security requirements
- Consider how advisory committees, standards bodies, and individual companies are addressing wireless security issues

Legislative and Regulatory Task Force (LRTF)

- Determine whether the Federal Communications Commission's 2nd Report and Order for Priority Access Service requires revision
- Consider law enforcement issues related to the implementation of WPS
- Explore strengthening legislation related to intentional and malicious attacks on the Internet as well as on the public and private infrastructure/assets through the Internet
- Propose a system for aggregating and disseminating condition reports to the appropriate industry, government, and consumer users by centralizing health and welfare monitoring of the Internet
- Define the dependencies and propose mechanisms for improving the effectiveness of the information sharing and analysis of Internet issues

Demonstrating the CEO-level commitment to CIP in the I&C Sector, the NSTAC is composed of only senior management from the companies involved:

NSTAC Members

NSTAC CHAIR
Mr. Joseph P. Nacchio
Chairman and CEO
Qwest

NSTAC VICE CHAIR (Designate)
Dr. Vance D. Coffman
Chairman and CEO
Lockheed Martin

Mr. F. Duane Ackerman
Chairman and CEO
BellSouth

Mr. Herbert W. Anderson
President, Northrop Grumman
Information Technology
Northrop Grumman

Mr. C. Michael Armstrong
Chairman and CEO
AT&T

Dr. J. Robert Beyster
Chairman and CEO
Science Applications International Corporation (SAIC)

Mr. Richard H. Brown
Chairman and CEO
Electronic Data Systems (EDS)

Mr. Daniel P. Burnham
Chairman and CEO
Raytheon

Mr. John T. Chambers
President and CEO
Cisco Systems

* Mr. Michael S. Dell
Chairman and CEO
Dell Computer Corporation

* Mr. Lawrence J. Ellison
Chairman and CEO
Oracle Corporation

Mr. William T. Esrey
Chairman and CEO
Sprint

Mr. James W. Evatt
President, Information and Communications Systems
Boeing

Mr. Christopher Galvin
Chairman and CEO
Motorola

Mr. Van B. Honeycutt
Chairman and CEO
Computer Sciences Corporation
(CSC)

Mr. Clayton M. Jones

President and CEO
Rockwell Collins

Mr. Charles R. Lee
Chairman and Co-CEO
Verizon Communications

Mr. Craig O. McCaw
* Chairman
Teledesic

Mr. Craig J. Mundie
Senior Vice President
Microsoft

Mr. Donald J. Obert
Group Executive
Network Computing Group
Bank of America

Mr. G. William Ruhl
CEO of D&E Telephone Company
United States Telecom Association
(USTA)

* Ms. Patricia F. Russo
President and CEO
Lucent Technologies

* Mr. Stratton Sclavos
President and CEO
VeriSign

Mr. Lawrence A. Weinbach
Chairman and CEO
Unisys

Mr. Edward E. Whitacre, Jr.
Chairman and CEO
SBC Communications

To be determined
WorldCom

To be determined
Global Crossing

To be determined
Nortel Networks

To be determined
TRW

* Membership pending White House approval.

NIAC-specific Next Steps

Initially established in January 2001 as a result of PDD 63, the National Infrastructure Assurance Council or NIAC, is due to continue as a high level national advisory council to provide the President advice "on the security of infrastructure support other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services."

According to the President's Executive Order signed on October 16, 2001, the NIAC's functions will include: 1) enhanc[ing] the partnership of the public and private sectors in protecting our critical infrastructures and provide reports on this issue to the President as appropriate; 2) propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, include information and telecommunications systems; and 3) monitor the development of private sector Information Sharing and Analysis Centers (ISACs) and provide recommendations to the Critical Infrastructure Protection Board how these organizations can best foster improved cooperation among the ISACs, the NIPC, and other federal government entities.

NRIC VI-specific Next Steps

The FCC has chartered NRIC VI to run for two years and end in January 2004. During that time many organizations involved in the I&C Sector will be actively involved in NRIC VI activities and Working Groups. The NRIC process has the advantage of getting CEO-level and Senior Management from I&C Sector companies and organizations to understand the issues faced in Homeland Security, CIP, and the needs of public safety organizations.

The Charter for NRIC VI provides:

<u>The Committee's Objective and Scope of its Activity</u>

The purposes of the Committee are to give telecommunications industry leaders the

opportunity to provide recommendations to the FCC and to the industry that, if implemented, would under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, and cable public telecommunications networks. This includes facilitating the reliability, robustness, security, and interoperability of public telecommunications networks. The scope encompasses recommendations that would ensure the security and sustainability of public telecommunications networks throughout the United States; ensure the availability of adequate public telecommunications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitating the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of telecommunications services. The Committee will address topics in the following areas:

1. Homeland Security

(A) Prevention. The Committee will assess vulnerabilities in the public telecommunications networks and the Internet and determine how best to address those vulnerabilities to prevent disruptions that would otherwise result from terrorist activities, natural disasters, or similar types of occurrences.

(1) In this regard, the Committee will conduct a survey of current practices by wireless, wireline, satellite, and cable telecommunications services providers and Internet service providers that address the Homeland Defense concerns articulated above.

(2) By December 31, 2002 the Committee will issue a report identifying areas for attention and describing best practices, with checklists, that should be followed to prevent disruptions of public telecommunications services and the Internet from terrorist activities, natural disasters, or similar types of occurrences.

(B) Restoration. The Committee will report on current disaster recovery mechanisms, techniques, and best practices and develop any additional best practices, mechanisms, and techniques that are necessary, or desirable, to more effectively restore telecommunications services and Internet services disruptions arising from terrorist activities, natural disasters, or similar types of occurrences.

(1) The Committee will report on the viability of any past or present mutual aid agreements and develop, and report on, any additional perspectives that may be appropriate to facilitate effective telecommunications services restorations. The Committee will issue this report within six (6) months after its first meeting.

(2) The Committee will issue a report containing best practices recommendations, and recommended mechanisms and techniques (including checklists), for disaster recovery and service restoration. The Committee will issue this report within twelve (12) months of its first meeting.

(3) The Committee will prepare and institute mechanisms for maintaining and distributing contact information for telecommunications industry personnel who are, or may be, essential to effective telecommunications service and Internet restoration efforts within six (6) months of the first meeting of the Committee.

(C) Public Safety. The Committee will explore and report on such actions as may be necessary or desirable to ensure that commercial telecommunications services networks (including wireless, wireline, satellite, and cable public telecommunications networks) can meet the special needs of public safety emergency communications, including means to prioritize, as appropriate, public safety usage of commercial services during emergencies.

2. Network Reliability

(A) The Committee will prepare and provide recommended requirements for network reliability and network reliability measurements for wireline, wireless, satellite, and cable public telecommunications networks, and for reliability measurements for the Internet, for reporting within twelve (12) months of the Committee's first meeting.

(B) The Committee will evaluate, and report on, the reliability of public telecommunications network services in the United States, including the reliability of router, packet, and circuit-switched networks.

(C) During the charter of a previous Committee, interested participants recommended that the FCC adopt a voluntary reporting program in conjunction with the National Communications System, to gather outage data for those telecommunications and information service providers not currently required to report outages to the Commission, and voluntary reporting was initiated. The Committee shall: (i) analyze the data obtained from the voluntary trial; and (ii) report on the efficacy of that process and the information obtained therefrom.

(D) Should the Commission initiate an inquiry or rulemaking with respect to any of the above-mentioned issues, the Committee will make formal

recommendations as a part of such proceeding(s).

3. Network Interoperability

The Committee will prepare analyses and, where appropriate, make recommendations for improving interoperability among networks to achieve the objectives that are contained in Section 256 of the Telecommunications Act of 1996, with particular emphasis on ensuring "the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks."

4. Broadband Deployment.

The Committee will make recommendations concerning the need for technical standards to ensure the compatibility and deployment of broadband technologies and services, and will evaluate the need for improvements in the reliability of broadband technologies and services.

5. Other Topics

(A) The Committee will make recommendations with respect to such additional topics as the Commission may specify. These topics may include requests for recommendations and technical advice on interoperability issues that may arise from convergence and digital packet networks, and how the Commission may best fulfill its responsibilities, particularly with respect to national defense and safety of life and property (including law enforcement) under the Communications Act.

(B) The Committee will assemble data and other information, perform analyses, and provide recommendations and advice to the Federal Communications Commission and the telecommunications industry concerning the foregoing.

Review of the NRIC VI membership demonstrates the senior level participation in NRIC VI.

NRIC VI Members

NRIC Chairman, Joseph P. Nacchio, Chairman and Chief Executive Officer (CEO), **Qwest Communications**. Other members: **Alcatel**, Mike Quigley, CEO Alcatel USA and President Alcatel Americas; **Allegiance Telcom, Inc**., Royce J. Holland, Chairman and CEO, Allegiance Telecom, Inc.; **ALLTEL**, Scott Ford, Chief Executive Officer, ALLTEL; **Alliance for Telecommunications Industry Solutions** (ATIS), Ross Ireland,

Chairman - ATIS, Senior Executive VP for Services at SBC; **AOL-Time Warner**, Robert Pittman, Co-Chief Operating Officer, AOL-Time Warner; **Association of Public Safety Communications Officials** (APCO), Glen S. Nash, President, APCO; **AT&T**, Frank Ianna, President, AT&T Network Services; **AT&T Wireless**, John Zeglis, Chairman and CEO**; BellSouth Communications**, F. Duane Ackerman, Chairman and CEO BellSouth Corp.; **BITS**, Catherine Allen, Chief Executive Officer, BITS; **Boeing Company**, Christopher J. Kent, VP of Computing Network Operations, Shared Services Group, The Boeing Company; **Cable & Wireless**, Donald B. Reed, CEO Global Cable & Wireless; **Century Telephone**, Glen F. Post III, President & CEO, Century Telephone; **Cingular Wireless**, Stephen M. Carter, President and Chief Executive Officer Cingular Wireless; **Cisco Systems**, Carlos Dominguez, Group VP-U S Service Provider Sales, Cisco Systems Inc.; **Citizens Utilities**, Jake Casey, President ILEC Operations, Citizens Utilities; **Comcast Corporation**, Bradley Dusto, Senior Vice President & Chief Technology Officer, Comcast Corporation; **Communications Workers of America**, George Kohl Assistant to the President/Director of Research & Development, Communications Workers of America; **Covad Communications**, Anjali Joshi, EVP-Engineering, Covad Communications Co.; **Cox Communications**, Chris Bowick, Sr. Vice President Engineering and CTO, Cox Communications; **Critical Infrastructure Assurance Office** (CIAO), John Tritak, Director, CIAO; **EarthLink**, Charles (Garry) Betty, Chief Executive Officer, EarthLink; **e-Commerce & Telecommunications Users Group** (eTUG), Brian Moir, Chief Operating Officer, eTUG; **Ericsson**, Angel Ruiz, President and Chief Executive Officer, Ericsson, **Focal Communications**, Robert C. Taylor, Jr., Chairman & Chief Executive Officer; **Genuity**, Paul R. Gudonis, Chairman and CEO, Genuity; **Hughes Network System**s, Dave Zatloukal, VP of Operations, Hughes Network Systems; **Intelsat, Ltd**., Ramu Potarazu, President and CEO, Intelsat Global Service Corporation; **Juniper Networks**, Scott Kriens, Chairman, President, and Chief Executive Officer, Juniper Networks; **Level 3 Communications, Inc**., James Q. Crowe, Chief Executive Officer, Level 3 Communications, Inc.; **Lockheed Martin**, Vance Coffman, Chairman of the Board and Chief Executive Officer, Lockheed Martin Corporation; **Lucent Technologies**, Patricia Russo, President and Chief Executive Officer, Lucent Technologies; **Marconi Corporation**, Michael J. Donovan, Chief Operating Officer, Marconi Corporation; **Motorola**, Robert Barnett, President - Commercial, Government and Industrial Solutions Sector, Motorola; **MSN.net**, David Cole, SVP, MSN.net; **National Association of Regulatory and Utility Commissioners** (NARUC), Jack Goldburg, Commissioner, NARUC; **National Communications System** (NCS), Brent Greene, Deputy Manager, National Communications Systems; **National Emergency Number Association** (NENA), Jim Goerke, Interim Executive Director, NENA; **National Science Foundation** (NSF), Dr. Rita Colwell, Director, National Science Foundation; **National Telecommunications and Information Administration** (NTIA), Nancy J. Victory, Assistant Secretary for Communications and Information, NTIA; **Nextel Communications, Inc.,** Tim Donahue, President and CEO, Nextel Communications; **Nokia Inc**., Kari-Pekka Wilska, President, Nokia Inc.; **Nortel Networks**, Frank Dunn, President and CEO, Nortel Networks; **Office of Science and**

I&C Sector
National Strategy Input

Telecommunications Policy (OSTP), Dr. John H. "Jack" Marburger, Director, OSTP; **Public Safety Wireless Networks** (PSWN), Robert E. Lee, Jr., Program Manager, PSWN; **SBC**, Edward E. Whitacre Jr., Chairman and Chief Executive Officer, SBC Telecommunications Inc.; **Sprint Corporation and Sprint PCS**, William (Bill) T. Esrey, Chairman and Chief Executive Officer, Sprint Corporation, **Telcordia Technologies**, Harold (Hal) C. Smith, President and COO, Telcordia Technologies; **VeriSign**, F. Terry Kremian, Executive Vice President, VeriSign; **Verizon Communications**, Ivan Seidenberg, Co-Chief Executive Officer, Verizon Communications; **VoiceStream**, Neville R. Ray, Vice President Engineering & Operations, VoiceStream; **WorldCom,** Tom Bosley, Senior Vice President-Network Implementation, WorldCom.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu