

Industry Compendium to the National Strategy to Secure Cyberspace

**To Chapter IV (Strategy for Action),
Section C (Critical Infrastructure Sectors),
Subsection 2 (Private/Public Critical Sector Organizations (non-Federal))**

Contents:

- **Purpose and Overview** page 1
- **Compendium C-1, Banking and Finance** page A
- **Compendium C-2, Electricity** page B
- **Compendium C-3, Information and Communications** page C
- **Compendium C-4, Oil and Natural Gas** page D
- **Compendium C-5, Railroads** page E
- **Compendium C-6, Water** page F

PURPOSE

The Industry Strategy Compendium comprises the critical infrastructure sectors' contribution to the National Strategy to Secure Cyberspace. Securing our critical infrastructures is not something the government can do alone. Private industry owns and operates the bulk of our critical infrastructures and only through a unique public-private partnership can we achieve the common goal of safeguarding our national and economic interests. Initially, the critical infrastructure sectors included Banking and Finance (Financial Services), Information and Communication (I&C), Electricity, Transportation, Oil and Gas, Water, Emergency Services and critical government functions. Emergency Services, though identified as an original critical sector, has been included in the state and local government section of this National Strategy.

Each of the of the critical sectors above has developed a sector strategy describing the actions that private industry, at the sector level, is taking to assure the delivery of its critical services. Their analysis takes into account both physical and cyber infrastructures that are crucial to the continued operations of each sector and their unique contributions to the nation. The following introduction, which covers issues common to all of the critical infrastructure sectors, has been written by the Partnership for Critical Infrastructure Security (PCIS). The PCIS is a non-profit organization that was established in December 1999 to address security issues facing the critical sectors – both of industry and government – in efforts to secure, protect and assure their vital infrastructures.

We would like to thank the many organizations and individuals who contributed to the cross-sector summary represented by the compendium and its affiliated sector plans – a sign of continued dedication and cooperation to secure both our information systems and critical infrastructures.

INTRODUCTION

Highlighted in this section are six areas of issues and concerns common to each of the critical infrastructure industries. Owners and operators of the infrastructure industries understand that critical infrastructure assurance is not only a national security issue, but a local and global issue, as well. Trends like increased use of technology, including the Internet, and just-in-time product and delivery systems create complex interdependencies and merge local, national and global interests. We are increasingly becoming interconnected and dependent on information systems. This interconnectedness fosters the need for strong economic security and a trusted E-Business environment. Central to this process is the need for public-private partnerships; new cooperative structures that seek to harmonize business and government actions at home and abroad. As new global and cyber linkages continue to increase our productivity and growth, they also create new vulnerabilities and potential avenues of disruption— even attack.

While several common themes are apparent across the sector strategies, their differences are notable as well. Some sectors had coordinating and information-sharing mechanisms already in place that encompass all or most of their organizations and members to facilitate sector-wide responses. Sectors lacking these broad coordinating structures are in the process of building them. Today, the critical sectors are at various stages in their development of industry-wide security strategies. Several of the strategies contain objectives, action lists and schedules, while others outline approaches to encourage sector members to address issues relevant to their specific situations and tolerances for risk. Consequently, the sector strategies vary in detail and depth.

INTERDEPENDENCY: Sectors depend on each other to operate and are growing increasingly interconnected.

RESEARCH AND DEVELOPMENT: Industry and Government need to develop a road map to identify new areas of research and streamline R&D efforts, as well as additional investments to fund them.

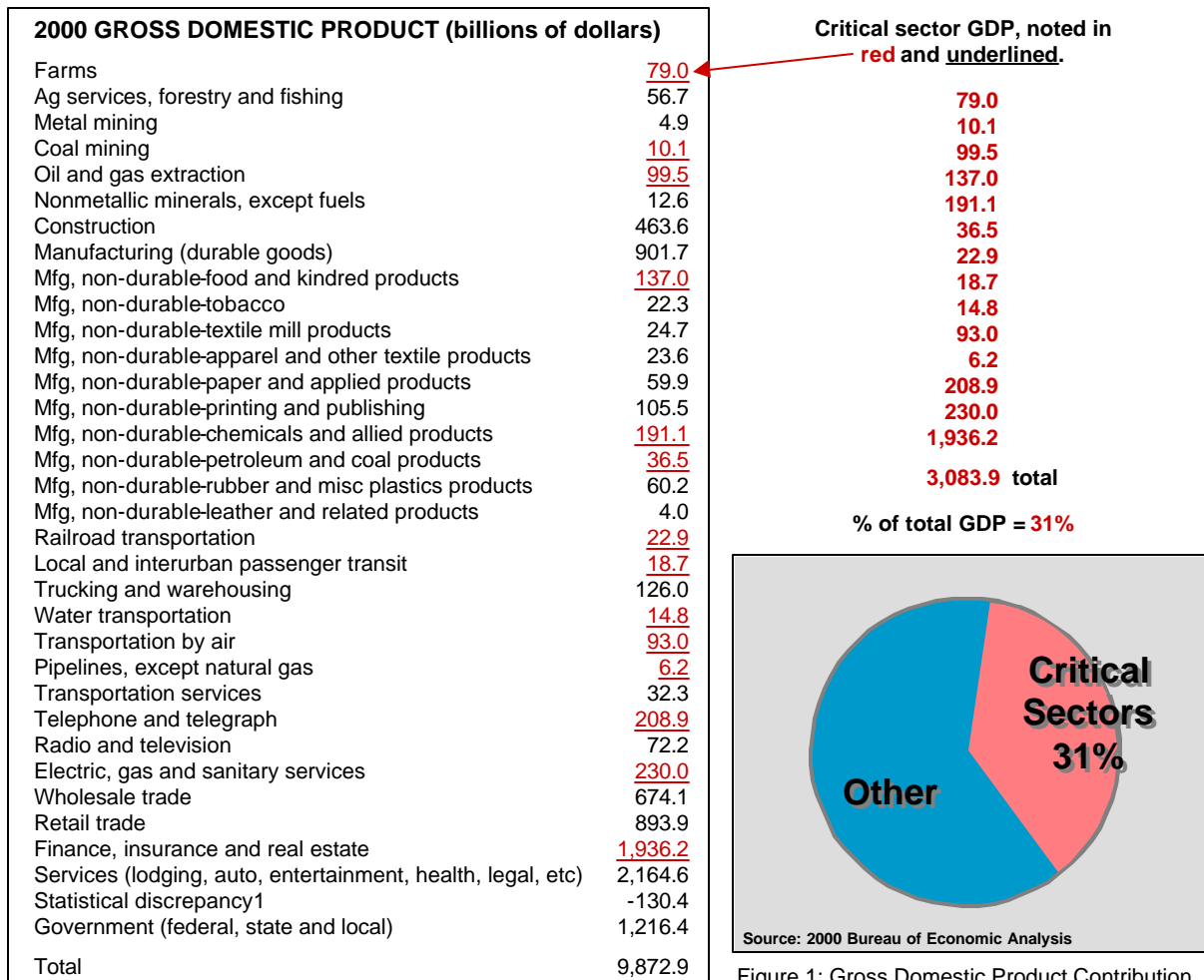
EDUCATION AND WORKFORCE DEVELOPMENT: Awareness and education continue to represent a major issue, even in the post-9/11 world.

INFORMATION SHARING: All sectors identify the need for a cross-sector, public-private information exchange capability.

PUBLIC POLICY AND LEGAL/LEGISLATIVE ISSUES: The Freedom of Information Act (FOIA), antitrust and liability laws represent barriers to public-private cooperation.

INTERNATIONAL ISSUES: Sectors operate beyond the physical confines of the United States and face different international concerns.

As a group, the critical infrastructure sectors proved backbone services for our nation’s economic engine and produce approximately 31% of the Gross Domestic Product (GDP).



CROSS-SECTOR COMMONALITIES

Interdependency

Infrastructure interdependency refers to the physical, electronic and new economy (e-commerce) linkages within and among the critical infrastructures. Besides each other, the critical infrastructure sectors also rely upon local, state and federal support to ensure adequate warnings, protection and

reconstitution in the event of a crisis. Easiest to identify among these critical relationships are the straightforward operational interdependencies shared among the sectors. What may not be so readily apparent, however, is the fact that an organization that directly depends on any particular sector also relies indirectly on the intricacies of that sector's infrastructure to varying degrees. So, with increased interconnectedness, comes increased dependency; and with that dependency comes the risk that disruption to one infrastructure could result from the failure of another infrastructure upon which it relies.

As Industry evolves toward a cyber-based marketplace, strategies for operating organizations, from both physical and business perspectives, must change as well. Many approaches today are the direct result of the burgeoning use of and subsequent dependence on electronics, ranging from simple communications systems to advanced electronic control systems. Furthermore, they reflect the need to compete and survive in a vastly expanded marketplace, which has meant procuring strategic alliances and enabling e-business transactions. Traditional business and control systems were designed for closed, trusted operating environments. As companies make accommodations for new cyber-based partnerships and exchange, however, their infrastructures become increasingly at risk for disruption through networking and connections to a wide range of other systems.

Consequently, in addition to greater dependence on technology for operating processes and procedures, increased use of information technology (IT) has created technical interdependencies between the operators of critical infrastructures and greatly magnified overall cyber risks. There is no turning back, however. The swift emergence of E-Business has already effected the re-engineering of many corporate structures, as well as physical changes to infrastructure systems that are essentially irreversible. Industry must work quickly to adapt its information assurance strategies to protect the IT investments it has made.

Sectors depend on one another to operate

The fact that organizations across the various critical sectors depend on one another to operate is apparent. Nevertheless, because of the rate at which technologies have advanced and the speed with which they have been adopted, it would be foolish to underestimate our ignorance with respect to the true extent of this interdependency. The water sector, for example, depends greatly on electricity for pumping and sanitation¹. Likewise, the electricity sector relies on water systems (dams) to generate hydroelectric energy, but its primary power sources are coal, oil and natural gas, which are in turn delivered by railroads and pipelines.

Oil and natural gas infrastructures depend on several critical sectors, as well. Electric power, information technology, telecommunications, transportation, water, and banking and finance all contribute to normal operations within the petroleum sector; conversely, they each rely greatly on the coal, oil and natural gas industries, which provide most of the energy generated in the U.S. today.

Likewise, America's railroads count on several critical infrastructures to maintain business as usual. Oil and Gas produces fuel for locomotives; Electricity supplies the power to run rail facilities; and I&C supports telecommunications and control system networks, which are basic necessities for rail operations and customer service². Conversely, rail systems move everything from mail and people to significant percentages of U.S. vehicles, coal, grain and chemicals. Additionally, because the Department of Defense (DoD) relies heavily on freight railroads to move ordnance and impedimenta in times of peace and war, it has designated 30,000 miles of rail corridors as essential to national defense³.

¹ Among others, the water sector also relies on I&C for control systems support, chemicals for sanitization and transportation to move those treatment supplies. In turn, nuclear power depends on water to cool its plants, and emergency services need it to suppress fires.

² *Terrorism Risk Analysis and Security Management Plan*, Association of American Railroads, January 2002

³ Specifically, the Strategic Rail Corridor Network (STRACNET), appropriated by the Military Traffic Management Command (MTMC), provides the backbone for transporting DoD shipments, especially during military mobilizations. *National Plan for Critical Infrastructure Protection – Rail Sector*, June 2002.

In the nation's other infrastructures, similar profound changes involving interdependency, deregulation and reliance on technology create new challenges to the assurance of infrastructure services. Perhaps the most significant change is the increasing degree to which these new challenges are pervasive across most or all sectors. For example, most sectors have dramatically increased their use of IT, for both internal operations and new E-Business practices between organizations. For their own operations, critical infrastructure providers depend upon IT products and on the services of the I&C sector. Further, I&C services are required for the E-Business practices that are themselves increasing the degree of electronic interdependencies. IT assets and I&C infrastructure therefore constitute both new dependencies and new cyber-risks. Because the new cyber risks are common to most or all sectors, IT/I&C dependency constitutes a single type of dependency and vulnerability that could be used to create damage in multiple sectors with a breadth that could significantly compromise the defense and economic security of the United States.

Sectors continue to grow increasingly interconnected.

Today's corporate infrastructures have become inextricably linked, thereby creating a complex network of interdependent systems. Thus far, we've only begun to illustrate the extent to which they rely on one another and, in light of recent world events, have merely touched on their importance within the context of U.S. security. As the scope of E-Business grows, the extent to which Industry depends on technology grows, as well. Businesses that open up their architectures to interact in this e-marketplace become increasingly interconnected and reliant on each other.

As transport and application networks continue to evolve, information delivery systems increasingly traverse the various private, yet interconnected, network facilities. Compromising the physical security of one sector's infrastructure, therefore, could result in localized effects on other sectors. Consequently, organizations of industry and government continue to grow inescapably vested in the security of each other's systems and should pay close attention to where their interdependencies and resulting vulnerabilities lie.

Many sector strategies also describe both existing and increasing interdependence among the organizations that make up their respective industries. For example, the I&C sector relies significantly on the physical assets and spaces of other sectors. Furthermore, the interconnectivity of networks in the public domain combined with the vast number of private networks that also connect to the Internet means that individual I&C constituents depend on the infrastructures of one another, as well.

Railroads have a long history of cooperation as a network industry. As a whole, however, the various segments of the transportation industry have traditionally remained separate with respect to their infrastructures. Nevertheless, the *Transportation Information Infrastructure Risk Assessment* of the President's National Security Telecommunications Advisory Committee (NSTAC) has two conclusions related to the increasing interconnectivity within the transportation industry. First, to meet customer demands, transportation companies across the board have opened their information systems thereby increasing their dependence on public and IT systems. Second, although the redundancy of the U.S. transportation system prevents it from any single critical point of failure on a national scale, increasing interconnectedness means that disruption of the sector's information infrastructure, even at a local or regional level, has the potential to impact economic or national security.

Because the oil and natural gas industries provide almost 62% of the energy used in the United States, their energy sources are vital to the U.S. and directly underpin much of its economy. Nevertheless, along with the rest of the market, oil and natural gas companies have experienced exponential changes to their infrastructures. While the sector's physical footprint has remained much the same, the approach to operating the petroleum industries has had to change from both physical and business perspectives.

As in other sectors, E-Business automation is a driving force for interconnection in the energy sector, both between companies, and between operational systems and business IT systems. Traditionally, Supervisory Control and Data Acquisitions (SCADA) systems that regulate operating processes⁴ within refineries, along pipelines, and in producing fields were designed for deployment in closed environments with trusted operators. To enable new e-business arrangements and transactions, however, current control systems are increasingly networked and interconnected with a variety of other systems that are in turn connected with partner companies—sometimes via public networks. Resulting organizational changes, such as mergers, alliances and joint ventures have produced corporate entities that no longer resemble the energy companies of the past; and the lines between traditional oil, natural gas, power and pipeline companies have become blurry.

To address the vulnerabilities associated with the risks of introducing cyber technologies, as well as the complexities of merging companies, security tactics within the oil and natural gas industries must also evolve. Historically, they have focused on the physical protection of personnel and property from human error or natural disasters, and emergency plans to deal with such events remain in place. However, current processes remain inadequate to deal with the changes affiliated with the increased dependence on cyber and other electronic networking⁵.

Local, State & Federal agencies must coordinate with the critical sectors.

In addition to assuring business-as-usual operations, the critical infrastructure sectors must also consider the significance of business continuity and disaster planning. When developing viable emergency response plans, the extent to which the sectors would rely on local, state and federal support in the wake of an emergency, natural disaster or the ever-increasing likelihood of a malicious attack becomes clear. Conversely, as the private-sector industries would rely on key government agencies, those public agencies would, in turn, depend on the private sectors to respond in times of crisis.

To that end, the assurance of adequate emergency response plans is paramount to the nation's recovery during periods of critical action; the successful development of those plans hinges on regular coordination and input from all levels of government with the private sector in order to identify the specific interdependencies of each agency. Therefore, to better assist private industry in structuring statewide, regional and federal emergency response planning, and sustained communication and cooperation between the private and public sectors are necessary.

Not only do governments at the local, state and federal levels have an important role in working with the private sector, their coordination with one another is critical to ensuring that resources, both public and private, are utilized in the most efficient manner. Such coordination would be especially important during large-scale events that could impact more than one critical sector. Most importantly, as shown during the events of 9/11, it is important to have adequate, redundant communications facilities that properly interoperate to allow for the efficient exchange of various types of communication.

From a security perspective, the prevalent concern of the transportation industry has been – and remains to be – the impact of physical threats to its infrastructures; therefore, protecting critical hubs and transportation vehicles from natural disaster, theft, or terrorist action continues to be the sector's primary focus.⁶ In its recent *Terrorism Risk Analysis and Security Management Plan*, however, the AAR has also recognized the more contemporary need for the rail industry to share security information and, thereby, coordinate joint efforts to address both physical and cyber vulnerabilities⁷.

⁴ The petroleum industries, as well as other utility sectors such as water, utilize Supervisory Control and Data Acquisition (SCADA) systems to operate and monitor critical components of pipeline systems and refineries (wells, gathering systems, processing facilities, transmission systems, and distribution systems).

⁵ *Securing Oil and Natural Gas Infrastructures in the New Economy*, National Petroleum Council, June 2001

⁶ *Transportation Information Infrastructure Risk Assessment*, the President's NSTAC, June 1999

⁷ *Terrorism Risk Analysis and Security Management Plan*, December 2001

The AAR sponsored Surface Transportation ISAC (ST-ISAC) launched in March 2002⁸ implements the rail association's findings.

In addition to private industry resources, ISACs depend a great deal on all levels of government to provide reliable, salient threat information. Adequate preparation for disruptions that extend beyond the scope of individual organizations demands that responding organizations, whether public or private, have the ability to act as one. Consequently, development of the fundamental framework necessary to enable that capacity requires on-going cooperation between government and industry.

Additional Considerations

- Sectors increasingly share common rights-of-way, geographic commonalities, etc. For example, at the World Trade Center, nine co-located I&C organizations lost infrastructure as well as personnel.
- Sectors increasingly out-source staff. For example, the financial services sector out-sources many services, including electronic funds transfer, IT services and software development.

RESEARCH & DEVELOPMENT

Current R&D needs pose challenges that cannot be addressed through traditional forms of R&D sponsored by government agencies (DoD and civilian), private industry and universities. Issues include both physical and electronic information security, as well as new threats and vulnerabilities from the growing and complex interdependence among the critical infrastructures. Current U.S. research and development efforts is mostly fragmented and uncoordinated, because multiple government agencies fund studies in accordance with their agendas, while private industries simultaneously conduct their own R&D efforts with little awareness of the work underway in the public sector.

Further, market forces alone cannot adequately support the necessary investment to conduct fundamental research. Rising to meet these challenges demands a new paradigm. A public-private R&D roadmap is needed to reduce the redundant efforts and streamline research activities across the board. Such a framework would provide a fresh examination of R&D requirements, new and enhanced resources, and identify gaps in the security model. To succeed, an unprecedented partnership that combines the best resources of Government, academia, and private Industry needs to be undertaken to tackle the new challenges.

The range of research activities is comprised of three areas of effort: technical R&D to create new information security technologies for CIP; development of industry criteria for vulnerability assessments; development of industry best practices including contingency planning. All three areas are gated by a critical constraint on any R&D program planning: lack of current, accurate information about the real cyber vulnerabilities present both in and across sectors today. Therefore, in addition to gap analysis of existing research, R&D roadmap efforts must include assessments and operations analyses of the individual critical infrastructures. Government and Industry can then share the results to define priorities for new R&D studies focused on critical infrastructure assurance. Once developed, the R&D roadmap would provide a comprehensive foundation for building policies, strategies, assessments and actions. The PCIS has initiated work to develop a roadmap for information technologies. Broader efforts are still needed to encompass the full spectrum of infrastructure needs, including physical protections, new policies and coordinating structures.

Technical R&D (Both sector-directed and government-directed R&D is needed.)

Technical R&D activities range from assessment of existing products, *as used for CIP*, to development of new technologies needed to fill gaps in current CIP technology. For example, many organizations in the U.S. would benefit from a standardized process through which information security products could

⁸ <<http://www.surfacetransportationisac.org/index.htm>>

be independently assessed and rated. Creating such a mechanism would allow individual companies, which are often too small and/or do not have the in-house expertise to conduct such assessments, to learn from the collaborative efforts of a pool of R&D resources. SCADA and digital control systems are critical targets for this kind of assessment. Because relatively few such products exist; the same products are widely used across sectors by critical infrastructure operators, who may lack specific knowledge about the vulnerabilities of these systems. Pooled research to better understand the limits of these current products would help to create new, practical approaches to solving security challenges.

A major issue in securing critical infrastructures is the lack of security in Process Control Systems (PCS) used in critical infrastructures (e.g., Supervisory Control and Data Acquisition or SCADA and Digital Control Systems (DCS)). Existing technologies lack internal security mechanisms because these systems were typically physically isolated, or used proprietary hardware and communication protocols that made cyber attack more difficult. To complicate matters, current security technologies and products are used for general purpose systems and generally do not meet the [specific] needs of DCS and SCADA products. Further, PCS are real-time systems that require fast response rates, and adding currently available security controls is difficult and decreases the speed of the systems. Because of current market conditions, PCS vendors are focusing more on speed than security. As a result, many critical infrastructure operators deploy DCS and SCADA systems without security mechanisms in changing electronic environments that are becoming more vulnerable to attack. In order to determine a course of action and work on solutions to enhance the security of these systems, critical infrastructure sectors, the Government and the PCS vendors must work together.

For example, there is a body of government-funded research on real-time systems that may apply to part of real-time DCS systems. Similar research in the electric power sector has explored the limitations of existing security technology as applied to current process control systems, the I&C Sector has addressed R&D issues through a series of NSTAC-sponsored R&D Exchange Workshops. Among the issues discussed is the divergence of agendas with respect to industry-funded and government-funded studies. Between Industry's market-driven efforts and the Government's defense-oriented efforts, I&C believes that R&D gaps exist, which no market force or government mandate alone can currently address. Therefore, protection of the Next Generation Networks (NGN) clearly calls for specific efforts geared toward to securing them.

There are significant R&D concerns related to infrastructure assurance in the transportation sector, as well. Some transport modes point out that their infrastructures would benefit from ongoing, proactive R&D efforts to develop new technologies designed to counter information security vulnerabilities and, in complement, a standardized mechanism by which to assess and rate such products. Additionally, the rail sector has stated that government-sponsored vulnerability and countermeasure assessments of rail shipments of certain hazardous materials are warranted.

Research and development is a unique area for Banking and Finance. In contrast to other industries, such as the energy and transportation sectors, the financial services sector has received no significant government funding for R&D. Currently, industry leaders have plans to review ongoing and proposed government research and development initiatives. In turn, they will provide feedback to the financial-sector constituency about what R&D priorities could be supported by the various sector entities. Meanwhile, the financial services industry must develop a focused, comprehensive approach to R&D. To do so, it is important for the sector to identify all current studies within the sector, whether privately or government funded, and then determine the status of those efforts so that the industry can avoid duplicating existing research.

Necessary government-funded R&D would specifically address national security and other key Critical Infrastructure Protection (CIP) issues, such as mitigation, and response and recovery, which transcend the individual sectors and the companies within them. Unfortunately, competitive pressures

within Industry often lead to the use of immature technologies, which can, in turn, introduce significant vulnerabilities and increased exposure. To minimize the potentially negative impact such untested products can have on the critical infrastructures, the results of government-funded CIP studies should be rapidly transferred to the private sector, especially in the IT and telecommunications areas, so that Industry remains vigilant and thoroughly investigates new IT investments before introducing them into their infrastructures.

Vulnerability Assessment and Guidelines

There is a clear need for R&D to develop comprehensive set of industry criteria for vulnerability assessments. The critical infrastructure industries need the tools on which to baseline security postures and make improvements. Efforts to identify sound practices have begun but still require development before they can become useful standards that are applicable across the critical infrastructure sectors and all levels of government.

The importance and scope for such guidelines and criteria is illustrated by the juxtaposition of the importance placed on assessment by the various sector plans, and the fact that the majority of CI operators lack the skills or motivation to conduct periodic vulnerability assessments.

Immediately following September 11, 2001, the AAR utilized national intelligence community best practices to conduct a thorough vulnerability assessment of the freight railroad industry and to create a security management plan. Rail leadership continuously refines its security plan, which entails periodic updates of its critical assets database, and evaluating potential actions and countermeasures.

Best Practices and Contingency Planning

As with vulnerability assessment, there is a clear need for R&D to develop comprehensive set of industry best practices, spanning information security and physical security, to be used as guidelines not only for defining and auditing ordinary operations but also for defining contingency plans. The I&C and other sectors are working to identify and share security best practices and promote “university excellence centers” for information security training. This sector has completed vulnerability assessments by comparing operations to the best practices that are extant today.

Contingency planning is a critical aspect of best practices. Both information security and physical security are vital parts of any security plan being fundamental to all security efforts. When evaluating the integrity of any infrastructure, the ability to recover from crisis or disaster situations is crucial. Therefore, every potential threat to the systems that constitute those infrastructures must be identified and planned for, which includes not only threats of cyber crime, but also human error, natural disasters and physical assaults. Adequate contingency, or disaster, planning assures that an organization has the know-how, resources, and comprehensive approach necessary to resume normal operations following a crisis. Failure to plan properly can result in the loss of time, functionality, money, and – perhaps most importantly – irreplaceable information.

Because of the ever-changing natures of industry and technology, contingency planning should be dynamic, as well. Therefore, once a business continuity and/or a disaster recovery plan has been established, it should be tested periodically to ensure that it remains entirely robust. Moreover, as critical sectors grow increasingly interconnected, and their contingency plans grow more complex; it may become necessary for interdependent organizations to perform integrated tests together.

In contrast to the testing of electronic system security, the testing of physical system security is a mature and well-understood discipline, and most facilities have well laid plans for physical recovery in place. Over the years, the oil and natural gas industries have undergone several physical failures, such as fires and detonations, from which they have developed the strategies currently used both to prevent the causes of physical incidents, and to respond to and recover from disasters when they do

occur. Tabletop exercises are effective in testing response and recovery procedures for natural disasters and can apply to physical security issues as well. Planning for electronic disruptions is not so straightforward, and the oil and gas sector believes that, with increasing dependence on cyber systems, response and recovery plans within the petroleum industries should be enhanced to include information technology disruptions.

The recovery and restoration components of the electricity sector's *Approach to Action*⁹ document refer to activities that develop plans for managing an emergency from the moment it occurs; managing efforts to restore systems to normal; conducting simulation drills; tracking lessons learned; and sharing best practices. Recovery and restoration efforts differ for physical and electronic assets, however. Most electricity organizations now rely on computerized systems for billing, system operation and internal management functions. Moreover, in scenarios where the competitive electricity market depends on the electronic exchange of bids and offers, the reliance on technology is even greater and more time-critical. A plan to restore business operations following an electronic disruption incident could mean the difference between commercial success and failure; yet it is difficult to predict all potential disturbances. Nevertheless, to be **truly** effective, electronic contingency plans must account for as many types of attack as possible and, furthermore, their associated implications for remediation. Electronic crimes, for example, may require special planning to deal with the requirements of external parties, such as law enforcement's need to preserve computer evidence, a factor that could further affect timely restoration of services or facilities.

Banking and Finance recognizes the complexity of the effort required to protect the critical infrastructure components underlying the U.S. financial system. Individual institutions must identify and assess threats to their infrastructures so that sector leaders can develop a comprehensive management plan to coordinate and direct sector-wide responses to those threats. Many of the individual financial institutions have security programs and contingency plans in place that are capable of handling only "normal" threat levels that arise in the course of regular business operations. Accordingly, sector leaders plan to develop a sector-wide contingency, including a series of definitive actions to be followed when faced with the loss of "significant" business operations that the business-continuity plans of individual institutions may not cover. Also to be considered are the financial dependencies of the organizations themselves, and the various risk management models that determine the need for liquidity should one or more organizations become unable to function or meet their financial obligations. Finally, the financial services industry, in conjunction with appropriate government agencies, should lead sector-wide discussions regarding potential catastrophic failures to determine whether appropriate high-level restoration and reconstitution plans have been established and are in place.

Railroad Chief Executive Officers (CEOs), Chief Operating Officers (COOs) and Chief Information Officers (CIOs) played integral roles in the industry's risk analysis, and the formation and implementation of the security plan. Railroad senior management, including risk management officers, is fully engaged in both physical and cyber security. The sector's *Terrorism Risk Analysis and Security Management Plan* encompasses contingency plans, which include re-routing options and shared dispatching capabilities. As of yet, however, the rail sector does not participate in the Telecommunications Service Priority (TSP) Program, which has been designed by the Federal Communications Commission (FCC) to ensure priority treatment for the Nation's most critical telecommunication services¹⁰. Although the sector's priority would logically fall below that of national defense and emergency responders, enrolling in the TSP Program would ensure Rail's proper place among organizations in need of support following a regional or national disaster.

⁹ *An Approach to Action for the Electricity Sector*, Version 1.0, June 2001

¹⁰ "The FCC's TSP Program identifies and prioritizes telecommunication services that support national security or emergency preparedness (NS/EP) missions. The TSP Program also provides a legal means for the telecommunications industry to provide preferential treatment to services enrolled in the program." *Telecommunications Service Priority* < <http://tsp.fcc.gov> > [Accessed June 13, 2002].

EDUCATION AND WORKFORCE DEVELOPMENT

An organization's best defense against attack is its people: employees and management who understand and support security policies and procedures. The ability to address and resolve security issues requires several levels of understanding: all system users must be aware of potential security problems; they must recognize and accept their individual responsibilities with respect to preventing them; and they must know what to do when one actually exists. Security awareness programs deal with the proper use of security tools and the execution of proper controls¹¹ and are imperative to creating a secure infrastructure environment. They educate employees on actions they must take to reduce overall infrastructure risk and to mitigate the severity of effects from security incidents. Furthermore, **consistent** outreach keeps security practices fresh in the minds of employees and engages the recipients of security information as problem solvers—capturing existing knowledge, expertise and creativity—thus broadening the available resource.

Employees need awareness, policy and procedure training.

Some sectors already have industry-wide outreach and awareness programs in place. For example, the railroad sector thoroughly briefs its employees in matters of security awareness and, in turn, they serve as 20,000 pairs of eyes and ears for the rail systems. Security briefings, like safety updates, are a daily part of an employee's job.

In response to September 11th, The American Water Works Association (AWWA) produced an EPA funded teleconference and webcast to educate water utility professionals on subjects from the basics of infrastructure vulnerability to dealing with terrorist attacks. Presented by the AWWA Research Foundation (AWWARF), experts from Sandia National Laboratory led viewers through practical steps of the assessment process based on the AWWARF vulnerability methodology for water utilities.¹²

NERC's "Approach to Action" reference document is a significant step in education and awareness for the electric sector. NERC and EEI web sites provide access to various security reference documents that have been created for electricity sector members (i.e. security guides, threat-alert levels and response guidelines). Also, the Electric Power Research Institute (EPRI) has created various primer and reference documents for its electricity sector members (i.e., procurement guidelines, power line and power plant security primers).

The financial services sector has undertaken a variety of strategic and tactical initiatives as part of its security awareness efforts. The sector plans to distribute "sound practices" to the industry. The Securities Industry Association (SIA) is working to improve business continuity planning and institute a command center; similarly, the American Bankers Association (ABA) has created a Financial Privacy Toolbox and Identity Theft Communication Kit. Such compilations of security recommendations represent a small piece of the Banking and Finance Sector's fundamental goal to reach out and educate its constituency through programs geared toward building a strong support base for the sector's collective critical infrastructure mission. Additionally many financial services firms provide security awareness as a part of new employee training.

Leadership needs awareness, policy and procedure training.

Awareness training and outreach programs geared toward senior levels of management (i.e., industry leaders, operators, managers and stakeholders) provide information for making informed business choices with respect to identifying and managing emerging risks. Thus far, most sectors have worked on senior management communication, such as development of targeted brochures, presentations, linkages to other educational programs and topic-specific toolkits; however, the changing face of

¹¹ Such education and awareness topics include the selection and protection of "good" passwords, managing modem use, and awareness of social engineering techniques used by criminals

¹² American Water Works Association. E-MainStream, Volume 46, Number 3. May/June 2002.

http://www.awwa.org/Communications/mainstream/Archives/2002/Jan_Feb/Lead01_Security_story.cfm [Accessed July 9, 2002.]

threats and vulnerabilities is dynamic, making security awareness at all levels an on-going assignment and responsibility. While sector efforts to date have been successful, the need for more comprehensive and systematic industry-wide outreach programs remains. Furthermore, such efforts should include local and state government leaders whose budget support is needed for infrastructure assurance efforts.

For that reason, the financial services sector's recent strategy for outreach and awareness comprises a new enhanced three-tiered model aimed at executive, business and operations management. Until now, education and outreach in the financial services sector has primarily been the responsibility of individual companies. To initiate broader industry-wide efforts, the sector has first focused on engaging the attention of the sector's information security specialists. Then, to drive home the importance of infrastructure assurance at the individual firm level, Banking and Finance leaders have formulated a "*business case*" for infrastructure assurance. The business case is defined in terms of risks to the confidentiality, integrity and availability of customer data, which are fundamental to both customer trust and the trust between financial institutions, and the financial and legal consequences attendant to those risks¹³.

Similarly, NERC and the Edison Electric Institute are working on a series of voluntary security guidelines for the industry that describe general approaches, considerations, practices, and planning philosophies that can be applied in protecting electric infrastructure systems. Additionally, NERC has rolled out awareness programs, specifically targeting CEOs, CIOs, operations managers and the NERC Board of Trustees. For example, the Analysis and Warning Program provides training for grid system operators through information on identifying cyber events, reporting incidents to the ES-ISAC and NIPC, and receiving alert notifications

In cooperation with the U.S. Environmental Protection Agency (EPA), Sandia National Laboratories developed a train-the-trainer course for water sector security professionals based on the AWWA Research Foundation (AWWARF)/Sandia vulnerability assessment tool. The vulnerability assessment workshops are designed for personnel responsible for developing, implementing, and assisting with security plans and procedures. The program's goal is to license certified trainers to begin offering the course throughout the United States to support the EPA's objective to have regular vulnerability assessments conducted at water utilities.¹⁴

Additional Considerations

- Mergers and downsizing have resulted in less stable work environments with fewer loyal workers.
- Disgruntled or inexperienced employees deliberately or accidentally disrupt critical infrastructures
- Using contract employees multiplies vulnerabilities.

INFORMATION SHARING

Dangerous and illegal groups, such as hackers, narcotics traffickers, organized criminal enterprises and terrorists, often benefit from coordinated efforts to share vulnerabilities they have identified and tools they use to exploit them. In contrast, many market-based businesses, historically, have resisted sharing security information for competitive reasons—sometimes to their detriment. Now, however, under the shadow of emerging threats and increasing vulnerability, it is clear that adequate security preparation will require Industry and Government to cooperate and improve the coordination of information flows.

¹³ *Banking and Financial Sector "The National Strategy for Critical Infrastructure Assurance,"* Version 1.0, Page 49. May 13, 2002

¹⁴ American Water Works Association. E-MainStream, Volume 46, Number 3. May/June 2002.

<http://www.awwa.org/Communications/mainstream/Archives/2002/May_Jun/WN02_vultraining.cfm> [Accessed July 9, 2002.]

To date, the independent critical sectors have established and continue to develop collaborative frameworks through which their constituencies can share security information, such as threat, vulnerability, countermeasure and best-practices information. Some have built their information-sharing systems upon existing coordinating structures, while others have had to invent new structures to accomplish this task. In addition to facilitating sector-wide information sharing, however, several sectors have also begun to develop mechanisms through which they can share information beyond their individual industries, across sectors and with Government.

Information Sharing and Analysis Centers

At the heart of most industry efforts are the sector-specific Information Sharing and Analysis Centers, or ISACs. A sector-ISAC is an industry-led mechanism for gathering, analyzing, sanitizing and disseminating about sector-specific cyber and physical security threats, vulnerabilities, incidents, and solutions. The purpose of the ISACs is to prevent and mitigate disruptions that would affect the operation of the critical sectors. Initially, the ISACs were designed with the specific purpose of reporting cyber incidents. However, over time, a common theme has emerged that ISACs should address both cyber and physical incidents. This information sharing mechanism continues to be a crucial part in a successful government-industry partnership.

The sector-ISACs and NIPC are relatively new organizations. Some of the critical infrastructure industries were recently in flux, and their sector-ISACs are not fully operational. Much cooperation and work goes into ISAC start-up, and anticipated changes within those organizations should take place before the undertaking of developing a sector-ISAC is made. Challenges faced by new and established ISACs include improving business participation; enhancing the timeliness and effectiveness of NIPC threat information; and overcoming legal barriers, such FOIA rules that can hamper the overall efficacy of information sharing efforts of some sectors.

During the events on September 11, many of the ISACs were used to help the various sectors respond, and to support our nation's infrastructure. Valuable relationships between sectors and the ISACs were able to foster further cross-sector communication and coordination among the sectors. September 11 created a new intensity and seriousness to advancing further the activities of the ISACs.

Examples of sectors developing ways to share incident information

Several of the critical infrastructure sectors have either created or are now planning the development of their industry-specific ISACs. For example, the water industry is committed to creating its sector-ISAC and has set its sites to begin in December 2002. To meet that goal, the AMWA has applied for an EPA grant to assist funding the ISAC development, and the sector has formed the Water CIP Advisory Group to provide advice during its construction.

Similarly, Oil and Gas is in process of building an ISAC. IT and telecommunications vulnerabilities are the immediate focus, but the sector plans to include physical vulnerabilities and threat information as the mechanism evolves. Among the reasons cited in support of the oil and natural gas ISAC is the fact that the National Petroleum Council found that some energy companies simply do not receive enough security information, while others may receive none at all. Moreover, some companies may not have physical or IT security staffs to act on such information even if they had it. A cost-effective ISAC would permit such companies access to vital security information, such as threats and vulnerabilities, as well as solutions to manage them.

Other sector-ISACs are even farther along. Launched in October 1999, the Financial Services ISAC (FS-ISAC) represents Industry's first response to Government's call for critical infrastructure assurance and Banking and Finance's efforts to keep its constituency well informed. The FS-ISAC has established a long history of keeping the sector aware of security issues, incidents and vulnerabilities, and has

been the first to report on such attacks as Code Red, NIMDA and SNMP IT. Recently, the FS-ISAC mechanism has expanded to share information with government groups such as the NIPC and the U.S. Secret Service. Resulting cooperative information exchange and analysis have yielded valuable, exciting results. Based on the information sharing efforts during 9/11 incidents, ISAC leaders are expanding their original information dissemination model. The improved mechanism, which is expected soon, facilitates the distribution of information to sector management and first responders.

Other sectors that have successfully established industry-ISACs are Rail and I&C. The Surface Transportation ISAC (ST-ISAC), launched by the AAR on March 15, 2002, invites regional and short-line railroads, public transit authorities, and other transportation modes and users of transportation infrastructure to join. I&C has two industry-ISACs to accommodate both sides of its sector, the ITAA-operated Information Technology ISAC (IT-ISAC) and NCC-ISAC operated by the National Coordinating Center for Telecommunications (NCC).

Additional Considerations

- The ISAC should obtain a business review letter from the Justice Department's Antitrust Division to allow information sharing regarding cyber security.
- Declassified federal intelligence provided to Industry is often so watered down as to be of little use. Certain industry people should be permitted to obtain national security clearance in order to access classified threat information.
- The IT systems used for information sharing also create new electronic dependencies and inter-connections that likely have new cyber security vulnerabilities that have not been assessed and which may require new information security technology to be developed.

PUBLIC POLICY AND LEGAL/LEGISLATIVE ISSUES

The sectors have begun to share security information privately, however, similar exchange with Government is more complicated. Three legal areas represent barriers to public-private cooperation in critical infrastructure assurance: the Freedom of Information Act (FOIA), antitrust laws and liability laws.

Barriers exist to public-private information sharing.

Under FOIA, there is a presumption that records in the possession of the agencies and departments of the executive branch of the U.S. government are accessible by the public. Recognizing the legitimate need to restrict disclosure of some information and to promote cooperation through statutes and regulations, however, Congress has provided exemptions under which information is not subject to disclosure. Nevertheless, whether *any* existing FOIA exemption provides the certainty of protection in disclosing threat and vulnerability information has not yet been proven to private industry's satisfaction. The concern is that information voluntarily shared for the express purpose of critical infrastructure awareness and security planning may be subject to FOIA requests, and the parties behind those requests could be competitors, litigators, and even potential attackers seeking to exploit system vulnerabilities.

In addition, various state and federal agencies have different rules with respect to how they administer FOIA. As a result, the different sectors approach the FOIA issue each in its own way. To err on the side of caution, many of them are reluctant to share security information with their local, state, or federal government counterparts until the ambiguities are clarified. The problem is exacerbated at the State level by Sunshine laws.

Sharing information within industry groups also could be hampered by antitrust concerns. Well-intentioned businesses and their critical information exchange efforts require shelter from federal and state antitrust laws. Certain agreements, cooperative arrangements and information sharing among industry participants can have anti-competitive consequences, such as raising prices or reducing

outputs – irrespective of intent. The intent of the sector-ISACs is clear. However, mere cooperation of large segments of various markets may raise questions by non-participating companies in relevant markets, agencies and other non-governmental organizations – thus, increasing the risk to ISAC members.

Finally, companies specializing in information security as well as the individual sector-ISACs are reluctant to set security standards because of potential liability litigation when such standards are allegedly breached.

Public Policy and Legal/Legislative Issues Summary

Members of the critical infrastructure sectors require comprehensive, consistent rules and controls in place to assure that participation in ISAC activities does not make them more susceptible to parties that might misuse information contained in their security plans. Sharing security information within the ISAC framework needs to be protected from FOIA release.

For robust and effective voluntary information sharing to work, the government's treatment of the various critical sectors needs to be consistent.

Within the framework of the sector-ISACs, critical infrastructure information shared voluntarily with the government and in good faith with other industry members:

1. Should be exempt from federal and state FOIA rules;
2. Should be exempt from federal and state antitrust laws; and
3. Should be sheltered from liability with safe harbor legislation.

Narrowly written legislative efforts in all three areas could reduce these concerns and enable more effective public-private cooperation in response to emerging threats and vulnerabilities.

Additional Considerations

- Industries would benefit from real-time relevant vulnerability and threat information that currently is only available to the government.
- When infrastructure disruptions occur, the roles and responsibilities of local, state and federal governments are often in conflict, and could hinder response efforts.

INTERNATIONAL ISSUES

Some critical business sectors in the United States have established strong cross-border infrastructure relationships throughout North America. However, because of the many seam-less connections that already exist in many sector activities, most organizations accept infrastructure assurance to be a global issue. The Internet, for example, knows no borders; beneficial and harmful traffic moves upon the same global pathways—often at its best speeds. Furthermore, special problems exist with foreign ownership of key organizations on which United States infrastructures depend. To address US national security without considering international economic impacts would be not only incomplete, but also counterproductive.

Most countries around the globe have reached some level of maturity with respect to a strategy for national infrastructure protection. Synchronizing U.S. efforts with those of other countries, and influencing them where possible, could help the global economy avoid being left with an electronic environment in which global systems must straddle islands of protected national infrastructure to communicate. Together, these national infrastructure protection programs should represent an integrated methodology in which the global systems can operate and work together.

When working across national borders, however, social, cultural and political norms cannot be ignored. Failing to accommodate different cultural biases towards security, privacy, and government or industry control will inevitably lead to inconsistencies between national efforts. For instance, many nations have yet to undertake comprehensive privatization of key business sectors; therefore, they may adopt views on security assurance and information sharing that are much different from those held by the public/private partnership of the U.S.

Finally, the benefits of using information technology come with risks that until now have not been well recognized. Mergers, acquisitions and partnerships (and their dissolution) require the organizations involved to create links to and/or integrate (or compartmentalize) their existing networks. In some industries, such information assets may include links to offshore or foreign-market, and disruptions to these systems or the information they contain can have increasingly serious consequences. Therefore, great pains must be taken to assure the integrity of these increasingly international infrastructures.

Countries throughout the world contain strong cyber infrastructure relationships.

The I&C infrastructure provides a cyber marketplace within a global medium where national boundaries are transparent. Therefore, infrastructure protection is an issue that must be pursued on a global basis. The dynamic nature of the cyber crime demands that critical infrastructure assurance entail long-term international commitment and attention from industry and law enforcement agencies.¹⁵

Financial institutions that are critical to the U.S. are dependent on many different levels of infrastructure at a national and international level. Financial institutions are subject to global threats. These institutions form part of, and rely on, the U.S. national infrastructure, the infrastructure of other nations, and a complex web of international infrastructure that collectively forms the global financial system.

Even many primarily domestic institutions are dependent on international markets and capital flows for their day-to-day liquidity. A domestic institution can be just as vulnerable, albeit indirectly, to the global threats facing U.S. based global financial institutions or non-U.S. institutions with substantial U.S. market presence. The risk to U.S. citizens is not confined to institutions operating within the U.S. Many citizens and their financial assets are increasingly mobile; operating in many markets simultaneously. Consequently, they depend on the national and commercial infrastructure of many countries. Therefore, the protection of the interests of U.S. citizens in a global financial market place needs to be considered.

Countries within North America contain strong physical infrastructure relationships.

In addition to cyber infrastructure, many U.S. sectors also share physical infrastructure. For those sectors, it is especially important to coordinate international efforts for remediation in the event of a disaster. For instance, Canada, Mexico and the U.S. essentially form one electric network, and, to a certain extent, the United States depends on the foreign networks to [maintain vital services both within the electric sector itself and, more broadly, to all of the other critical infrastructures]. Similarly, energy resources (i.e., natural gas) flow across the borders of Canada, Mexico and the U.S. through the same pipeline infrastructures. The oil and natural gas sector points out that, although it is well positioned to deal with physical infrastructure disruptions, closer coordination and integration of CIP efforts with Canadian and Mexican infrastructures should be considered.

Global laws require enhanced consistency.

Irrespective of industry, organizations now realize that critical infrastructure assurance is an issue that must be addressed internationally. American companies are increasingly becoming global corporations, and the U.S. federal government should encourage countries to enact globally consistent laws addressing the interconnected, electronic commercial marketplace. Universal technical standards, and uniform business and legal practices should be encouraged. For example,

¹⁵ *Information & Communications Sector, National Strategy Input. December 2001. Executive Summary, page 12.*

the author of the “I Love You” virus could not be prosecuted under Philippine law, yet he deliberately caused international disruption.

An example of international efforts in this direction is the Global Information Security (InfoSec) Summits, which gather government and industry leaders from around the globe to discuss the critical issues of information security and infrastructure assurance. Similarly, the Council of Europe Cybercrime Convention has improved several consistency issues for the I&C sector, but problems still remain, including a lack of international consensus on what actually constitutes a cybercrime. International businesses also need to be shielded from legal liability for a wide range of risk management planning activity. Issues that need to be addressed include limiting liability from inconsistent requirements on national or global companies.

CONCLUSION

This compendium to the National Strategy to Secure Cyberspace represents private industry’s view and the steps the sectors have taken both individually and together. The events of September 11th demonstrated the importance of the cross-sector cooperative efforts and reinforced the need to accelerate them. Industry’s determination to protect critical assets continues to evolve – and represents responses to both cyber and physical threats, vulnerabilities and incidents to deter, prevent, mitigate, respond, reconstitute, and learn as we move into a changed environment post 9/11. While September 11th raised America’s awareness and clarified the need for national anti-terror initiatives, industry’s collaborative critical infrastructure assurance efforts are not new. The discussions and recommendations contained in this document are not the culmination of nine months of work, but rather represent years of critical infrastructure protection and information assurance cooperation and dialogue among and across all industry sectors.

This compendium includes contributions from critical infrastructure sector organizations that recognize the need for a complex strategy, understand that without a continued private-public partnership organizations alone cannot effectively tackle these issues, and acknowledge that success still needs to be defined. Questions remain, however, by working together, the government and private sector can achieve our common goal on securing our critical infrastructures from cyber and physical attack.