Protecting Critical Infrastructure: The Role of the Private Sector

By Sue Eckert*

Introduction

More than any other event in recent memory, September 11, 2001 underscored America's vulnerability to new types of security threats. At stake is not just the security of innocent civilians going about their daily business, but also the physical and cyber infrastructures upon which U.S. economic prosperity and well-being is based. In particular, the events of 9-11 brought to the fore the need for new thinking regarding the private sector role in a new security environment. Unfortunately, as time passes since the attacks, the urgency behind this effort has diminished, putting our national success and economic well-being at risk.

With approximately eighty-five percent of U.S. key infrastructures privately owned or operated[1], the private sector is an increasingly important actor in the new security issues associated with homeland security. While an integral part of national security, homeland security, differs in that it is a shared responsibility that cannot be met by the federal government alone. It requires coordinated action on the part of government (federal, state, and local) *and the private sector*. New forms of public-private partnerships are essential to meet the challenges posed by new technologies and non-traditional threats.

Prior to September 11th, independent advisory groups and government agencies warned of possible attacks on U.S. soil and the need for the public and private sectors to work together to address such risks.[2] Progress in establishing a sustained effort in the late 1990's, however, was slowed by the lack of perceived threat, especially within the private sector. The tragic events of 9-11, however, changed this, at least temporarily. The attacks prompted renewed attention to the issue and motivated both government and industry to pursue cooperative mechanisms that had previously languished. One of the most significant of these initiatives is the Information Sharing and Analysis Centers (ISACs). ISACs are intended to promote collaboration and information-sharing both between government and industry and within key industries with respect to threats. They are the primary means of partnering for the protection of critical infrastructure, although little public attention or analysis has been focused on them.

This chapter explores a topic at the intersection of emerging political economy and security issues – governments' increasing reliance on the private sector to help secure the homeland.[3] It surveys the record to-date of U.S. public-private partnerships in addressing critical

infrastructure protection, examines impediments faced by industry collaboration through the ISACs, and offers analysis and recommendations for enhancing such partnerships so as to provide greater security in the future.

Changed Conceptions of Security

September 11th marked an important turning point in how Americans perceive security. Until then, security was generally viewed in traditional terms – military efforts to defend US interests against external threats, principally from states. With the nightmare of fuel-laden commercial planes being flown into key buildings and the resulting catastrophic loss of life and economic disruption, however, came the realization that a new more comprehensive security paradigm is required -- one broad enough to encompass protection of both Americans at home, and also key areas of the economy vulnerable to attack, -- that is, "critical infrastructure." In the aftermath of 9/11, protection of the homeland, or homeland security, has become an integral part of US security, this in a way that the indiscriminate threat of nuclear devastation never required.[4]

Prior to September 11th, few in the U.S. worried about threats against domestic facilities. The attacks changed this by vividly demonstrating U.S. vulnerability. Subsequent information found in Afghanistan -- diagrams of American nuclear plants and water supplies – underscored the nature of these new threats against commercial targets.[5] Furthermore, recent communications of Al Qaeda specifically focus on the US economy as a target, or in Osama bin Laden's words, on "this policy in bleeding America to the point of bankruptcy."[6] The FBI and Department of Homeland Security (DHS) have issued repeated warnings of possible targeting by terrorists of nuclear utilities, chemical facilities and modes of transportation, especially aviation and rail. In August 2004, financial institutions in the New York and Washington areas became the first sector publicly warned of specific terrorist threats, with DHS issuing an elevated threat advisory.[7] Thus, "the front lines of defense in this new type of battle have moved into our communities and the individual institutions that make up our critical infrastructure sectors."[8]

The US government owns and controls very few of these national assets – estimates range from eighty to eighty-five percent of critical infrastructure owned or operated by the private sector.[9] Because of technological developments, especially increased reliance on interconnected computer and telecommunications networks, a broad range of modern economic activity is now more vulnerable to exploitation. Financial systems operating 24/7 linking intermediaries globally, power plants and electrical grids, gas and oil distribution pipelines, water treatment systems, oil and chemical refineries, transportation systems, and even essential military communications -- all rely on an interdependent network of information systems that connect and increasingly control the operations of other critical infrastructures. These systems are attractive

and viable targets for terrorists, or other adversaries, either through physical bombing or cyber attacks.[10] The August 2003 power blackouts of much of the East Coast further underscored the susceptibility of interconnected networks not only to terrorist attacks, but to also to severe disruption. "Without a conscious societal or political decision, we have forged public and private dependencies on computer-based interlinked information systems."[11]

Thus, in this new security environment, the boundary between the private and public sector has blurred. Whereas security traditionally-defined has been the province of the federal government, homeland security is not solely the responsibility of the federal government, but also of state and local government *and the private sector*.[12] Homeland security is a shared responsibility that cannot be met by government alone. "Just as winning this war [on terrorism] requires international coalitions, intelligence sharing, and law enforcement cooperation, so too does it require finding a new division of labor between the public and private sectors.[13]

Defining Critical Infrastructure

Critical infrastructure has been defined in various ways over time, but generally consists of "those physical or cyber-based systems essential to the minimum operations of the economy and government."[14] Since the events of 9-11 and passage of the Patriot Act, the definition has been expanded by adding, "the incapacity or destruction of which … would have a debilitating impact on the security, national economic security, and national public health or safety….[15]

In 1996, the Clinton Administration defined eight sectors as critical: telecommunications, electric power systems, oil and gas storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government.[16] In 2003, other sectors were added or reorganized to form fourteen critical sectors, including food, public health, and the chemical industry and hazardous materials.[17] While all have a basis for being considered "critical," the expansive definition covers a broad cross-section of economic and governmental activity.[18]

To get a sense of magnitude, the Department of Homeland Security characterizes the nation's critical infrastructures and key assets as including 68,000 public water systems, 300,000 oil and natural gas production facilities, 4,000 off-shore platforms, 278,000 miles of natural gas pipelines, 361 seaports, 104 nuclear power plants, 80,000 dams and tens of thousands of other potentially critical targets across fourteen diverse critical infrastructure sectors."[19] While several policy documents and the Congress have mandated the development of a uniform methodology to identify and catalogue critical facilities and systems, a comprehensive list has proven problematic.[20]

The Clinton Administration's Critical Infrastructure Policies

A concerted effort by the U.S. Government to address systematically critical infrastructure issues is relatively recent. The Reagan Administration considered aspects of national security challenges posed by new telecommunications technology, especially as they related to encryption and the government's ability to wiretap. An advisory committee of U.S. companies was formed, but *ad hoc* interactions between the government (primarily the National Security Agency) and affected companies were the norm. Rather, it was during the Clinton Administration that the first comprehensive effort was made to address national infrastructure issues.

The concept and lexicon of critical infrastructure, and the focus on public-private partnerships to address such concerns, first emerged in the mid-1990s when the Clinton Administration initiated a dialogue with computer and telecommunications companies. Partially in response to growing concern for computer vulnerabilities and the need to protect information systems from attack, President Clinton issued Executive Order 13010 on 15 July 1996, establishing the President's Commission on Critical Infrastructure Protection (PCCIP), a governmental body to recommend a national policy and strategy to protect critical infrastructures from physical and cyber threats.[21] As part of its tasks, the PCCIP was charged with identifying and working with private sector entities that conduct, support or contribute to infrastructure assurance. In October 1997 the Commission issued its report, urging a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures. It recommended greater cooperation and communication between the private sector and government since critical infrastructure protection was a shared responsibility.[22]

Building on the recommendations of the Commission, Presidential Decision Directive (PDD) 63 was promulgated in 1998 as the first comprehensive attempt to protect physical and cyber-based systems essential to the economy and government.[23] PDD-63 established critical infrastructure protection as a national goal and articulated a strategy for cooperative government-private sector initiatives to accomplish it. The policy emphasized that government would, to the extent feasible, focus on market-based incentives for addressing critical infrastructure protection and avoid increased government regulation. The government was to consult with owners and operators of critical infrastructures to encourage the voluntary creation of private sector information sharing and analysis centers (ISACs).

PDD-63 also established the National Infrastructure Protection Center (NIPC) within the FBI to serve as the principal governmental body to facilitate the U.S. Government's infrastructure threat assessment, warning, vulnerability, law enforcement investigation and response. The NIPC

was designated to serve as the conduit for information sharing with the private sector through the ISACs. The Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce was also created under PDD-63 to coordinate the Federal Government's initiatives on critical infrastructure assurance efforts and to support the ISACs. To provide overall direction to the policy, President Clinton designated Richard Clarke, a seasoned career bureaucrat, as National Coordinator for Security, Infrastructure Protection, and Counter-terrorism.[24]

Because of increasing incidents of cyber attacks on both government facilities and private companies, infrastructure protection initially focused primarily on cyber-security.[25] The run-up to Y2K and denial of service attacks in 2000 highlighted this vulnerability and heightened awareness, especially among the information industries. The Clinton Administration actively encouraged the formation of sector-specific ISACs to begin sharing information among companies, and between the government and the private sector. While the effort got off to a slow start, four ISACs were established from 1999-2001 in the financial services, telecommunication, electronic and information technology sectors. With varying degrees of industry participation and differing operational methods, ISACs have evolved into the primary mechanisms for government-industry interaction on critical infrastructure issues.

Post-9/11 Critical Infrastructure Initiatives

In early 2001, the new Bush Administration allowed most infrastructure protection activities initiated under President Clinton to continue while it conducted an internal review of policies. There was little public attention to the issue in the first nine months of George W. Bush's presidency, and apparently little private sector initiative. As a result, the momentum behind the creation of the first ISACS diminished. The events of September 11th intervened, however, and critical infrastructure issues became a priority unlike any time in the past.

In response to the attacks, President Bush signed two relevant executive orders. The first, Executive Order 13228 on 9 October 2001, established the new Office of Homeland Security within the National Security Council, headed by an Assistant to the President for Homeland Security. Its mission was to develop and coordinate the implementation of a comprehensive national strategy to secure the U.S. from terrorist threats, and to protect U.S. critical infrastructure from terrorist attacks.[26] In July 2002, the National Strategy for Homeland Security was released, detailing the range of governmental initiatives to protect the US homeland, including efforts to work with the private sector. Specifically, the strategy identified protection of the America's critical infrastructure and key assets as one of six critical mission areas.[27]

Increasing Congressional pressure for a more permanent institution dedicated to homeland security, however, ultimately gave way to the Administration's decision to eliminate

the office within the NSC and to create a Department of Homeland Security. On November 22, 2002, Congress approved the largest government reorganization since the Truman Administration's creation of the Department of Defense and the National Security Council – the Department of Homeland Security.[28] With a mission that specifically included the protection of critical infrastructure, the DHS consolidated responsibility for cyber and physical protection efforts, including functions formerly of NIPC at the FBI and CIAO at the Department of Commerce.

The second executive order, issued concomitantly with the creation of the Office of Homeland Security, established the Administration infrastructure protection policy. Building on PDD-63, President Bush issued Executive Order 13231 on October 18, 2001, which laid out the Administration's policy and organizational structure, including establishment of the President's Critical Infrastructure Protection Board and the National Infrastructure Advisory Council.

> "It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations."[29]

In February 2003, the Administration elaborated its critical infrastructure objectives in two policy documents -- the "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," and the "National Strategy to Secure Cyberspace."[30] Both documents emphasize the importance of developing effective mechanisms between the public and private sector to exchange information regarding threats, vulnerabilities, and incidents. On December 17, 2003, President Bush codified the policy in a new Homeland Security Presidential Directive (HSPD)-7 on Critical Infrastructure Identification, Prioritization, and Protection. HSPD-7 supercedes PDD-63 and requires Federal departments and agencies to identify, prioritize, and protect US critical infrastructures from attack.[31]

In its most important aspects, the Bush Administration's stated policy concerning critical infrastructure protection has essentially been the same as that of the Clinton Administration.[32] While bureaucratic structures differ, both administrations emphasized the importance of working with the private sector, not regulating it. Indeed, the National Strategy for the Physical Protection of Critical Infrastructures called for "a new paradigm of cooperation and partnership…that

requires a culture of trust and ongoing collaboration among relevant public and private stakeholders, rather than more traditional systems of command and control [of the Cold War]."[33]

Private Sector Role in Security

A private sector role in the national security realm is certainly not new --either in practice or treatment of the issue by the academy. For as long as there have been wars, governments have hired mercenaries and purchased armaments produced by private industry. Traditionally, scholars have tended to concentrate on topics related to weapons production and arms trade, and more broadly, defense industrial base concerns when addressing issues at the intersection of national security and political economy.[34] More recently, academic interest has focused on issues surrounding the "privatization of security" in warn-torn regions and the increasing private sector support of logistical and support services as seen in Iraq.[35]

Aaron Friedberg's *In the Shadow of the Garrison State: America's Anti-Statism and Its Cold War Grand Strategy* detailed the reasons behind the privatization of arms production in the United States following World War II, the result of which placed primary reliance on the private sector to produce the nation's arms.[36] Reflecting an anti-statist tradition in American politics, the US established a mechanism to procure arms from privately-owned firms instead of adopting a more onerous industrial policy. According to Friedberg, this represents the success of the national security state in harnessing the private sector and private resources for national purposes; this largely through the government's near-monopoly over military acquisition. However, at the same time, the government created a system with heavy dependence on privately-owned institutions.[37]

In the post-9/11 world, the security threat is not one that can be successfully managed through the purchasing power of the government. Rather, the risks are now more specifically shared. At issue is no longer whether or not the private sector can be replied upon to manufacture high quality weaponry at a reasonable cost, but whether or not the private sector will invest the necessary resources to defend itself, short of direct government intervention. Unwilling, or unable, to compel such a response, the federal government under both the Clinton and Bush Administrations has opted to encourage action through cooperative measures. Questions remain, however, as to whether such a voluntary approach can produce the necessary outcome.[38] Subsequent sections will discuss this issue in greater detail, and address whether new tools are needed to ensure that the private sector takes the necessary steps to protect critical infrastructure.

Information Sharing and Analysis Centers (ISACs)

Over the past eight years, a variety of government-industry initiatives have evolved to address critical infrastructure protection issues. The Partnership for Critical Infrastructure

Security (PCIS), formed in 1999, provided an overall forum for dialogue on infrastructure security issues across sectors.[39] InfraGard, a pilot program started in 1996, is a partnership between companies and government --the FBI originally and DHS now-- to provide for the secure exchange of information on cyber intrusions, vulnerabilities, and infrastructure threats.[40] The US Computer Emergency Response Team (US CERT), administered by Carnegie Mellon in cooperation with DHS, provides a coordination center to direct the US response to possible cyber attacks, ensuring that all necessary information to repel an attack is distributed across all critical infrastructure sectors during an attack or heightened level of alert. In addition, DHS's Information Analysis and Infrastructure Protection division provides a range of bulletins and advisories of interest to professionals involved in protecting public and private infrastructures.[41]

Yet, the Information Sharing and Analysis Centers (ISACs) remains the primary vehicle to address infrastructure protection concerns. As envisioned in PDD-63, ISACs were to facilitate on a sectoral basis the voluntary gathering, analyzing, and dissemination of information to and from industry sectors and the federal government. Activities were to focus on infrastructure vulnerabilities, threats, and best practices for private sector organizations in designated sectors.

Both Clinton and Bush policies emphasized that ISACs were not to interfere with direct information exchanges between companies and the government. Although ultimately designed by members, ISACs were modeled on mechanisms such as the Centers for Disease Control and Prevention that have proven effective, particularly in extensive interchanges with the private and non-federal sectors. As such, ISACs were to possess a large degree of technical focus and expertise, primarily on non-regulatory and non-law enforcement missions. The expectation was that they would establish baseline statistics and patterns on various sectors, become a clearinghouse for information within and among members and sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, the government.[42] Of particular importance to the government, ISACs were to provide information on security incidents experienced by companies to the government.

From the private sector perspective, ISACs were envisioned as a means to deal with concerns that detailed security incident reports to the government might otherwise reveal. Public disclosures of vulnerabilities can have a negative impact on corporate reputations and impinge on business proprietary information, in particular due to Freedom of Information Act (FOIA) and open record requirements of federal agencies. Both PDD-63 and the Homeland Security Act contain provisions intended to enable ISACs to share security information outside of the burdens of open-record laws -- if the information relates to vulnerabilities, threats, and incidents. As

noted, below, however, ongoing industry concerns for the confidentiality of information shared have proven to be a significant factor affecting greater exchange.

Evolution of ISACs

Initially, ISACs got off to a slow start after PDD-63, both because they were breaking new ground and because of the natural reluctance of market competitors to share information. ISACs originally focused on cyber-security issues, with the basic structure in place in related sectors when cyber-attacks escalated to unprecedented levels in February 2000. Such events provided momentum, especially for the Telecom and Information ISACs, to intensify their efforts. The events of 9-11 further served to broaden the scope of ISACs responsibilities to deal with the physical protection against terrorist risks and incidents.

In October 1999, banking, finance and security organizations formed the Financial Services ISAC, and hired Global Integrity, a subsidiary of Scientific Applications International Corporation, to design and operate the ISAC. The Financial Services ISAC (FS/ISAC) maintains a database to which members voluntarily report information (on either an anonymous or attributed basis) regarding security threats, vulnerabilities, incidents and solutions. Security specialists analyze the input and, depending on the seriousness of the case, the FS-ISAC will distribute an alert to members. While the exact number of incidents submitted is confidential, there have been over 2000 entries related to general threats, vulnerabilities and solutions impacting the critical information infrastructure at large.[43] The data cannot be accessed by the government. Instead, it is used to share incident information among members in near-time, and will be used to develop trending and benchmarking information for the benefit of the members. Likewise, ISACs have been established in the telecommunications, information technology, electric power, energy (oil and natural gas), food, chemical, water, transportation, and emergency fire service sectors.[44] See Table 1 for an Overview of various ISACs.

Table I: Overview of Current ISACs*

Component/ Sector	Financial Services	Telecommunications	Electricity	Information Technology	Energy (Oil & Gas)
Formation Date	Oct-99	Jan-00	Oct-00	Dec-00	Nov-01
ISAC Operator	Science Applications International Corporation (SAIC)	National Communications System (NCS)	North American Electric Reliability Council (NERC)	Internet Security Systems Inc.	SAIC
Lead Agency (Federal)	Department of Treasury	Department of Homeland Security (DHS)	Department of Energy/DHS	Department of Homeland Security	Department of Energy
Private Sector Partner	American Bankers Association, Securities Industry Association	NCS	NERC	CERT	National Petroleum Council
Structure of ISAC	501©(6) nonprofit corp	National Coordinating Center (NCC)	Not-for-profit corporation	Non-profit, Limited Liability Corporation (LLC)	LLC
Membership	Banks, S&Ls, credit unions, securities firms, insurance companies, credit card companies, mortgage banking companies, industry associations	30 individual telecom companies providing telecom or network services, equipment or software, and 3 associations	Entities in electricity sector: American Public Power Assn, Canadian Electricity Assn, National Rural Electric Cooperative Assn, NERC regions etc.	Vendor, manufacturer, or provided of Information Technology (including Internet and e-commerce) products (hardware & software) solutions or services	Licensed energy industry companies - oil or natural gas, pipeline, energy trading, or industry service & support companies
Website	www.fsisac.com; Detailed information: operating rules, presentations, testimony, press releases, FAQs,	www.ncs.gov/ncc/main/html; members list, capabilities and initiatives	www.esisac.com; information on security standards, guidelines & workshops, board members, testimony, FAQs	www.it-isac.org; Detailed information: by-laws, articles of incorporation, alerts & advisories, corporate members, FAQs	www.energyisac.com; Detailed information, operating rules, FAQs
Funding	Tiered membership fees based on level of service: free, $750, to $10,000; Treasury grant	NCS; agencies bear costs of personnel	NERC	Tiered membership fees based on level of service: free up to $40,000	DoE grant; $150 login fees beyond 2 free
Scope of ISAC Coverage	Represents 90% of sector -- more than 800 members; 8500 firms receive alerts	95% of infrastructure -- 95% wireless providers & vendors, 90% internet service networks	90% of NERC members	70% IT globally; 85% cross-sector	85% of oil & gas sector
Sharing Mechanisms	Text based alerts, biweekly conference calls with DHS	CWIN	Secure telephone & website	CWIN, secure website, GETS (Government Emergency Telecommunications Service)	secure website

* The information in this table was derived from ISAC websites; ISAC Council White Paper "Reach of Major ISACs," 31 January 2004; and GAO Report 04-780, "Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors," 21 April 2004

Component/ Sector	Food	Chemical	Transportation (Surface)	Transportation (Public)	Water
Formation Date	Feb-02	Apr-02	May-02	Jan-03	Dec-02
ISAC Operator	Food Marketing Institute (FMI)	American Chemical Council's Chemical Transportation Emergency Center (CHEMTREC)	EWA Information & Infrastructure Technologies, Inc.	EWA Information & Infrastructure Technologies, Inc.	Association of Metropolitan Water Agencies
Lead Agency (Federal)	DHS, Department of Agriculture (meat/poultry) Department of Health & Human Services (all other foods)	Department of Homeland Security	Department of Homeland Security	Department of Transportation	Environmental Protection Agency
Private Sector Partner	FMI	American Chemistry Council	Association of American Railroads (AAR)	American Public Transport Association (APTA)	Association of Metropolitan Water Agencies
Structure of ISAC	Individual Subscriptions overseen by FMI	ACC members and individual subscribers	AAR members	APTA - nonprofit association	Nonprofit organization with board of managers of water utility leaders appointed by 8 US drinking water & wastewater organizations
Membership	Over 40 food industry trade associations & members	Companies or organizations involved in the manufacture, storage, transportation, or distribution of chemical products.	Major North American freight railroads and Amtrak	Public & private transit systems & commuter rail operators, transit assns & state departments of transportation	U.S. drinking water and wastewater systems, regardless of size or type of ownership.
Website	www.fmi.org/isac; business plan news releases, security alerts, food & disease Information, FAQs	www.chemicalisac.chemtrec.com; FAQs about CHEMTREC	www.surfacetransportationisac.org; FAQs, virus alerts, news	www.surfacetransportationisac.org; FAQs, virus alerts, news	www.waterisac.org; Information on board, services, FAQs
Funding	No current funding; volunteer labor contributed by FMI; no charge to participants	CHEMTREC	Membership fees and grant from Federal Transit Administration	Federally funded	EPA grant; subscription fees
Scope of ISAC Coverage	> 40 industry trade associations	CHEMTREC	95% of freight railroad industry and Amtrak	100 major transit organizations	275-300 water utilities, > 1000 individuals at drinking water and wastewater systems
Sharing Mechanisms	Watch Commander List	Biweekly conference call with DHS; secure communications network	secure telephone	secure email	secure portal & email

* The information in this table was derived from ISAC websites and ISAC Council White Paper "Reach of Major ISACs" 31, Jan. 2004. This paper is available at: http://isaccouncil.com/pub/Reach_of_the_Major_ISACs

Reflecting the unique characteristics of individual sectors, each ISAC operates independently. Each determines its own structure, operational procedures, business model, and funding mechanisms. Most ISACs are managed or operated by private entities as nonprofit, Limited Liability Corporations, owned by the members to manage the process and share information; others are managed as parts of existing industry trade associations. Articles of Corporation and By-Laws have been established, as well as Boards of Directors responsible for approving members through an application process open to U.S. firms in the designated sector. Differing funding mechanisms are used, with many ISACs financed largely through membership fees. Some ISACs offered tiered memberships with fees based on the level of service.[45] The Financial Services ISAC provides five levels of service ranging from free basic service, to $750 for limited access to website and reports, up to $10,000, $25,000, and $50,000 for commensurate access and benefits.[46] Other ISACs have partnered with federal agencies, with some having received federal grants or contracts.[47]

Benefits of membership include early notification of threats, anonymous information sharing, subject matter expertise, access to trending and other benchmark data. Membership is voluntary. Since membership lists are confidential, it is difficult to confirm the degree of industry participation, although indications are that most ISACs have good corporate participation. The ISAC Council, a group of 11 ISACs created to improve cross-sectoral coordination and effectiveness of ISACs, estimated that as of January 2004, ISAC membership and outreach extended to approximately 65% of U.S. private critical infrastructure.[48] Table 1 includes the estimated scope of industry coverage by each ISAC.

Assessment of ISACs

The relative novelty of most ISACs, and especially the lack of transparency common to them, makes anything more than a preliminary assessment difficult. Progress has been made in establishing ISACs and beginning the process of information sharing. DHS has organized numerous briefings with industry sectors, exercises and cross-sectoral ISAC meetings. In October 2004, for example, more than 200 security executives from a wide variety of industries and ISAC members met with government representatives for the ISAC Congress tabletop exercises to improve detection and response to threats and vulnerabilities facing infrastructure.[49] In addition, as noted previously, some government funding of ISAC operations has been provided.

However, much more needs to be done. To begin with, only a few critical infrastructure sectors have more than rudimentary ISACs. Moreover, the record of those that do varies considerably, especially in terms of sector participation and also in terms of the actual information being shared.[50]

Less broadly, there are several important issues that appear to be practical stumbling blocks hindering the effectiveness of ISACs as this is being written:

1) A uniform methodology for identifying facilities, systems and functions with national-level criticality has been difficult to establish, thereby impeding prioritization and resource allocation. Notwithstanding DHS's promise for such a risk assessment in 2003, it is not expected until at the earliest the end of 2004. Members of Congress who have been briefed on the work in progress have been critical of the list characterized as consisting of more than 30,000 potential targets.[51]

2) Follow-through has been poor on implementing the government's touted partnerships with industry to address security issues.[52] Beyond meetings and recommendations, there has been little in the way of concrete actions. As the GAO noted, the DHS has not developed a plan to address the challenges in building a public/private information sharing partnerships.[53]

3) The Department of Homeland Security - the lead agency responsible for ISACs and critical infrastructure protection - has been preoccupied with its own internal start-up and organization, thereby weakening government leadership in public-private partnering. Industry, Congress, the GAO, and DHS's Inspector General have been critical of various aspects of DHS's overall effort, citing a lack of coordination, poor communication, and a failure to set priorities.[54] A sense that "not enough is happening" pervades the issue.

Challenges to Public-Private Cooperation

Provided these impediments can be overcome, several serious challenges remain that are likely to hinder effective partnerships between government and the private sector through ISACs without concerted action to resolve them.

Information Sharing

Information sharing has been identified consistently as the key element of government and private sector efforts to protect critical infrastructure. While all embrace the concept, developing effective information sharing mechanisms has proven difficult. Overcoming long-standing cultural differences between the two communities and establishing trusted relationships and information sharing mechanisms necessary to support such coordination is not a simple or quick matter. Information sharing is evolving slowly, and according to a 2003 report by the National Academy of Sciences, "most information sharing still occurs through informal channels. Fundamental questions persist about who should share what information, when, how, why, and with whom."[55]

From the outset, industry raised concerns about the protection of proprietary information shared among members and with the government. Specifically, many industry representatives

believe that confidential information provided to the government may be disclosed to third parties under the Freedom of Information Act (FOIA). To address the issue, section 204 of the Homeland Security Act provides that information voluntarily provided by non-federal parties to the Department of Homeland Security that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism is not subject to public disclosure under the Freedom of Information Act.[56] While some cite the FOIA exemption as substantial progress in removing legal obstacles to sharing of information between the government and private sector, public interest groups have criticized the provision and proposed legislation to restore FOIA provisions, potentially reversing the information-sharing improvements.

In February 2004, DHS attempted to resolve the issue through the launch of the Protected Critical Infrastructure Information Program (PCII). The PCII is intended to encourage industry to voluntarily share confidential, propriety and business sensitive information about critical infrastructure with the government by establishing a specific process to exempt from disclosure to the public any critical infrastructure information voluntarily submitted to the Department.[57] Based on the reaction from public interest groups, however, it appears that the issue is still not entirely settled, reducing the certainty that government hoped to provide and fueling continued private sector reluctance to move forward with information sharing.[58]

An additional private sector concern relates to the risk of prosecution under antitrust regulations for sharing information with other companies.[59] Like the FOIA issue, the new antitrust exemptions called for by business raise a host of serious questions, and persistent perception problems related to what is permissible or illegal under existing law appears to serve an a disincentive for firms to share information.[60]

As information sharing is a two way street, it appears that problems also exist with the information provided by the government to the private sector. Historically, the government has been reluctant to share information that could compromise intelligence sources or investigations. According to the Business Roundtable, "improving the flow of information will depend in part on improving the ability of the government to communicate relevant and sensitive information – including pertinent, but often classified, threat intelligence – in a timely manner without violating security classification protocols."[61] Moreover the quality of information provided has been cited as a problem. Chemical companies indicate that they do not receive enough specific threat information and that it frequently comes from multiple sources. This represents a significant problem since industry officials have stated that they need more specific information about potential threats in order to design their security systems and protocols.[62]

Liability[63]

A related issue of concern revolves around broad questions of liability. What are companies' downstream or third party liabilities for the effects of attacks on infrastructure? What responsibility do owners and operators of infrastructure facilities have for managing risk? To what degree must utilities and service providers protect customers, including upgrading physical security and infrastructure? Since legal liability often depends on which actors are best positioned to prevent harmful activities, answering such concerns is extremely complicated.

One of the reasons for the lack of progress in information-sharing on infrastructure protection relates to the confusion regarding liabilities in sharing information within and between industry sectors and the government. This concern specifically affects industry's willingness to participate in ISACs. Companies fear liability if they provide flawed information to the ISAC, or if the ISAC prepares flawed analysis. What happens if ISAC members fail to share or disclose information that could have averted an attack? Is membership in the ISAC a mitigating factor, if losses occur and the company is sued? The host of unanswered questions and uncertainty represent important issues that need to be addressed. Many analysts believe, however, that industry's questions will be answered in court before long, perhaps leading the private sector to advocate liability protection for participation in ISACs.

Incentives for Infrastructure Protection

Beyond sharing information as to threats, the critical question remaining is how to ensure that industry takes the necessary actions to protect privately-owned critical infrastructure. Firms clearly have inherent incentives to protect their assets, not the least of which is profitability and reputational concerns. Even prior to 9/11, private sector costs for security were reported to exceed $40 billion annually, with the cyber-security market alone reaching $10 billion.[64] As a result of 9/11, costs are estimated to have increased as much as 100 percent, even without factoring in increased insurance costs. While it is difficult to measure precisely, security-related expenses for are considerable.

Business groups, however, note that shareholders have little financial incentive to invest in security beyond their stake in the corporation, and thus shareholders support security investments only to the extent that to do so would be profitable.[65] Thus, private markets themselves would not normally generate sufficient incentives to secure infrastructure vulnerabilities. "Relying on best practices and industry self-policing was acceptable for meeting our pre-9/11 regulatory needs, but they are simply inadequate in the post-9/11 world.[66] Hence, there is a need for new types of incentives to encourage infrastructure protection.

But the question of who appropriately bears the cost for enhanced security is a significant one. Some have proposed that the starting point for determining responsibility for business and government should focus on the costs of the security program and its beneficiaries, but even this is not a simple task.[67] Innovative solutions, such as the cost recovery program instituted by the Federal Energy Regulatory Commission after 9/11, or grants provided by EPA of $51 million to assist water utilities prepare vulnerability assessments and security plans -- provide models to encourage greater private sector investment in infrastructure protection.[68] Yet even with government funding of additional ISAC activities, questions arise as to government access to the information shared in the ISAC.[69]

Improving the security of the American homeland requires substantial new investments by both the public and private sector. The Bush Administration FY 05 Homeland Security budget proposed $865 million for the Information Analysis and Infrastructure Protection Directorate, an increase of $31 million from FY 04.[70] While this includes a broad spectrum of measures, some beyond critical infrastructure protection, the figure is clearly dwarfed in comparison to the financial costs of securing the vast privately owned and operated critical infrastructure. As noted by the 9/11 Commission, "private sector preparedness is not a luxury; it is a cost of doing business in the post 9/11 world."[71] Because little new money has been provided to state and local authorities for infrastructure protection, let alone to the private sector, questions concerning who pays for security will remain problematic.

Voluntary/Regulatory Approaches

Consistently, US policy has emphasized the voluntary nature of private sector efforts to protect critical infrastructure. The power outages in August 2003, however, and recent attention to vulnerabilities of chemical and nuclear plants beg the question -- are voluntary efforts on industry's part alone are sufficient, or is regulation necessary to compel adoption of safeguards? While a 2003 GAO report praised the chemical industry's voluntary security efforts to date, it also raised serious questions as to the adequacy of such efforts.[72] In such high-risk sectors, legislation has been introduced in Congress to establish uniform standards for securing chemical sites and to provide DHS authority to enforce such standards.[73] To date, these efforts have failed, however, largely due to industry opposition and the Administration's continued reliance on voluntary/self-regulatory approaches.

Enhanced regulation of critical infrastructure raise serious questions regarding the desirability, feasibility, and cost of such an approach. Legislation and regulations relevant to infrastructure protection are a patchwork, making efforts to develop a comprehensive regulatory framework complicated, let alone to enforce.

The Bush Administration has vigorously pursued self-regulatory approaches, leaving it to private industry to determine whether, how, and to what degree to protect itself. Government officials cite initiatives such as that of the Self Storage Association (SSA) as an example of how business can effectively take the lead in setting standards. Concerned that the federal government would impose new requirements following 9/11, SSA put into place new checks to verify customers' identities and ascertain any criminal records; the new procedures were funded through $7.50/renter charge for the security check. This "know your customer" system has not been widely utilized yet, but is expected to grow as companies try to preclude mandatory regulation.[74]

Yet, a purely voluntary approach by industry alone is not the answer. Public safety demands some minimal degree of standards, and serious questions remain as to the adequacy of existing requirements developed for purposes other than security or protection against terrorism. The 2004 Presidential campaign addressed the issue, with Senator Kerry criticizing the Bush Administration's laissez-faire approach to infrastructure protection, arguing for mandatory measures to improve security at high-risk targets such as chemical and nuclear facilities. And while most industry groups favor market-based incentives to increasing security, a recent study by the National Infrastructure Advisory Council indicated that some industry representatives acknowledge that regulation may be needed for certain sectors.[75]

Notwithstanding progress within certain industry sectors in adopting voluntary standards, the imperative of securing critical infrastructure requires a more concerted approach – one involving both established standards and increased incentives for investments in security. "Unfortunately, without standards, or even the threat of standards, the private sector will not secure itself."[76]

When the next attack comes, the likely result will be enhanced government regulation. The threat of regulation, therefore, should serve to motivate industry to pursue aggressively self-regulatory efforts. This is an appropriate initial step, while the effectiveness of such measures and the need for mandatory requirements in certain sectors is evaluated, as well as new incentives created. Indeed, increased participation in ISACs is viewed as one indicator that the private sector is moving toward greater self-regulation in critical infrastructure areas.[77]

Conclusions

One of the most dangerous shortcomings in the Administration's homeland security activities to date has been the general absence of measures to strengthen private-market incentives.[78] Prior to the events of September 11, 2001, incremental advancements were achieved in addressing threats to critical infrastructure protection. Since 9/11, some genuine progress has been made to foster public-private cooperation.

Frankly, however, much of what's been accomplished amounts to lip service to the idea, without adequate or effective efforts to realize the objective. As was a common theme in the 2004 campaign, the question is not whether we are safer, but are we safe enough? The gap between the rhetoric of creating public-private partnerships to address these security issues, and reality of action to support such efforts is significant. Much more needs to be done to meet the challenges we face.

There are a number of legitimate reasons for the slow progress – the general inability of government to utilize effectively the private sector, traditional government-industry concerns regarding information sharing, the distraction resulting from the bureaucratic reorganization to create the Department of Homeland Security, and most importantly, the lack of appropriate incentives to motivate the private sector to embrace critical infrastructure protection. Ironically, the apparent success of the US in thwarting additional attacks on the homeland, may have served to decrease the urgency perceived by the private sector to act. It would be nice if the threat had indeed receded, but terrorism will be a fixture well into the 21st century.

Thus, a more concerted strategy to encourage the private sector to put into place adequate security measures is needed. A system of public policy incentives -- for example, tax incentives, loan programs or grants for investment in protection, cost-recovery measures, government underwriting of insurance[79] -- should be developed to harness market forces to provide infrastructure protection. The US Government should use its purchasing power to encourage enhanced security, requiring vendors take steps to make products more secure. Given the enormity of task, new and creative ideas to promote public-private partnerships must be explored, which include new mechanisms and funding.[80]

The National Strategy for Homeland Security acknowledged the need to use "all available policy tools", including legislation, and in some cases, regulation, to create incentives for the private sector. But the sense of urgency has diminished, and creative leadership on new approaches is lacking. Now is the time to redouble efforts and devise new approaches. Minimal security standards, with appropriate incentives to reward companies investing in security and partnering with the government, are more likely to be successful than attempting to regulate compliance.

In addition, the government needs to make critical infrastructure protection a higher priority. Understandably, the effort to stand-up the Department of Homeland Security was an enormous task, but appropriate attention to and leadership on these issues within DHS has not been forthcoming. Frustration among industry and the Congress has mounted, threatening the credibility of current initiatives. Moreover, greater effort needs to be devoted to defining what is

critical. An overly broad understanding of critical infrastructure will actually serve to weaken protection by diffusing efforts and funding.

In short, the government and private sector both need to work together more effectively. Increased attention to and support of the ISACs, successfully demonstrating how legitimate concerns can be addressed, will promote cooperation and encourage new modes of partnership. New challenges require new thinking, not business as usual. Nothing less than our continued national success and economic well-being depend on it.

---

[*] The author's views on this issue were informed by her role as Assistant Secretary of Commerce from 1993-1997, when she was involved with early efforts by the Clinton Administration to engage the private sector on critical infrastructure issues.

[1] "The National Strategy for Homeland Security: Office of Homeland Security," 16 July 2002, available at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

[2] See in particular, "U.S. Commission on National Security in the 21st Century (Hart-Rudman Commission)" which warned two years prior to 9-11 of the likelihood of attacks against American citizens on American soil with heavy casualties, and recommended the creation of a National Homeland Security Agency. (available at http://www.nssg.gov/Reports/reports.htm.)

[3] This chapter focuses on US experiences with critical infrastructure protection, as the US is a forerunner in the field, but the trend of relying on the private sector to secure infrastructure is not limited to the US. See Dunn, M., and Wigert, I., *International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries* (Swiss Federal Institute of Technology, Center for Security Studies: Zurich, 2004), available at: http://www.isn.ethz.ch/pubs/ph/details.cfm?r_oID=454&sid=AE7EB4E71753E9948A2AE4421D766EBD. Ongoing work by the author includes comparative analysis of other countries' efforts to address critical infrastructure protection issues.

[4] It is important to distinguish between Homeland Security and Homeland Defense. Homeland security is the concerted national effort to prevent terrorist attacks within the US, with primary responsibility resting with the Department of Homeland Security. Homeland defense is defined as the military protection of US territory, the domestic population, and critical defense infrastructure against external threats and aggression. DoD, through a new Assistant Secretary of Homeland Defense, is primarily responsible for homeland defense, as following the 9/11 attacks defense of the homeland was restored as a primary mission of DoD. See Steve Bowman, "Homeland Security: The Department of Defense's Role," (Congressional Research Service, Library of Congress, 14 May 2003). Also of note is that most European efforts analogous to homeland security in the American context are referred to as "Internal Security."

[5] "Administrative Oversight: Are we Ready for A Cyber Terror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (13 February 2002).

[6] See "Transcript: Translation of Bin Laden's Videotaped Message," provided by the U.S. Government, of Osama bin Laden's videotaped message aired on the al-Jazeera satellite television network, 1 November 2004, located at: http://washingtonpost.com/ac2/wp-dyn/A16990-2004Nov1?language+printer.

[7] "US Warns of High Risk of Qaeda Attack," Eric Lichtblau, *The New York Times*, 2 August 2004, pg. 1.
[8] "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003, p. 8, available at http://www.whitehouse.gov/pcipb/physical_strategy.pdf,
[9] The Administration cited private-sector ownership of critical infrastructure at eighty-five percent in July 2002 "The National Strategy for Securing Homeland Security," and "approximately eighty-five percent" of critical infrastructures and key assets owned and operated by private industry in the February 2003 "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," available at http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf). While subsequent Executive branch documents have not always characterized the amount of critical infrastructure in private hands the same, the figure of eighty-five percent of critical infrastructure and key assets owned and operated by private industry has become widely quoted and broadly accepted, although no data appears to be available to assess the number. An industry group places private sector ownership and control at "over eighty percent of our critical infrastructure, including various networks, services, and physical facilities that provide us necessities like electronic power, agriculture, and water services." ("Terrorism: Real Threats. Real Costs. Joint Solutions" The Business Roundtable, June 2003, at http://www.businessroundtable.org.
[10] Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, 6 February 2002.
[11] CSIS report [GET CITE]
[12] The issue of an effective response to terrorist treats against the homeland raises numerous questions of federalism, and the appropriate role for the state and local levels of government, as well as the private sector. While an important topic that has been the subject of considerable study of late, the state and local issues will not be addressed in this paper, since the focus is on the private role in protecting infrastructure and the partnership necessary primarily with the US government to achieve this objective.
[13] David J. Rothkopf, "Business Versus Terror," *Foreign Policy*, May-June 2002 at: http://www.foreignpolicy.com/issue_mayjune_2002/rothkopf.html.
[14] *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63*, White Paper, 22 May 1998. For a discussion of the varying definitions of critical infrastructure, see John Moteff, Claudia Copeland and John Fischer, "Critical Infrastructure: What Makes an Infrastructure Critical" (Congressional Research Service, Library of Congress, 29 January 2003), and John Moteff and Paul Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," (Congressional Research Service, Library of Congress, 1 October 2004).
[15] The USA Patriot Act (Public Law No.107-56, Section 1016(e)) defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." See http://www.whitehouse.gov/homeland/book/sect3-3.pdf.
[16] Executive Order 13010, Critical Infrastructure Protection, 15 July 1996, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr17jy96-92.pdf
[17] In the most recent listing of critical infrastructure sectors, the oil and gas storage and transportation area was combined with the electric power systems to form an overall Energy sector. In addition, information was added to telecommunications to form the Information and Telecommunications sector. New sectors include agriculture, food, public health, defense industrial base, chemical industry and hazardous materials, and postal and shipping. See "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003, available at http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

[18] The broad characterization of critical infrastructure has lead some to question whether too expansive a definition may have the effect of actually diluting protection efforts. See James A. Lewis, "Critical Infrastructure Protection – With All Deliberate Speed" in The CIP Report, December 2003, Volume 2, Number 6, at http://gmu.edu/archives/cipp-report.html). Because of the preliminary stage that critical infrastructure efforts are currently at, it is not possible to determine if this is in fact the case. Based on other governmental experiences, however, especially in the area of export controls, the author believes it is important to try to identify as precisely as possible which infrastructures and which parts are "truly critical."

[19] U.S. Department of Homeland Security, "Homeland Security Budget in Brief, Fiscal Year 2005," at http://www.dhs.gov.

[20] DHS has developed a framework to identify vulnerabilities, but it is still in its infancy, and is not expected until the earliest at the end of 2004. Members of Congress whom have been briefed on the effort have been critical of the effort, with more than 30,000 potential targets identified. Such a study is an essential first step in helping to prioritize protection efforts, and help decide where available resources should be spent. See "Homeland Security Identifies Potential Infrastructure Targets," Danielle Belopotosky, *National Journal's Technology Daily,* located at: http://www.govexec.com/dailyfed1004/101404tdpml.htm.

[21] E.O. 13010

[22] "Critical Foundations: Protecting America's Infrastructures: A Report of the President's Commission on Critical Infrastructure Protection," October 1997, available at: http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf

[23] "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," 22 May 1998, available at http://www.nipc.gov/about/pdd63.htm

[24] Richard Clarke details the Administration's deliberations in developing PDD-63 and related critical infrastructure initiatives in his book, *Against All Enemies*. (Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004) 167-171.

[25] According to Carnegie Mellon University's CERT Coordination Center, the number of cyber security incidents has been increasing at an alarming rate – from 20,000 in 2000 to 52,000 in 2001 and 82,000 in 2002, and more than 76.000 in the first six months of 2003. See: http://www.cert.org/annual_rpts/cert_rpt_02.html#intro).

[26] Executive Order 13228 -- Establishing the Office of Homeland Security and the Homeland Security Council, available at http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html

[27] "The National Strategy for Homeland Security: Office of Homeland Security," 16 July 2002, available at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf

[28] The Homeland Security Act (P.L. 107-269).

[29] Executive Order 13231 – Critical Infrastructure Protection in the Information Age. *Federal Register* Vol. 86. No.202. 18 October 2001,at http://www.ciao.gov/News/EOonCriticalInfrastrutureProtection101601.html

[30] "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003, available at http://www.whitehouse.gov/pcipb/physical_strategy.pdf, and "The National Strategy to Secure Cyberspace," February 2003 available at http://www.whitehouse.gov/pcibc/cyberspace_strategy.pdf.

[31] Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," 17 December 2003, available at: http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html

[32] See John D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation," *Report to Congress by the Congressional Research Service*, 17 December 2002, p. 10 for a comparison of the two administrations' approaches to critical infrastructure protection.

[33] National Strategy, p. 8.

[34] For an overview of issues traditionally addressed by scholars in this context, see Ethan Barnaby Kapstein, *The Political Economy of National Security: A Global Perspective,* (New York: McGraw-Hill Inc., 1992).
[35] See P.W. Singer, "Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry," (*International Security*, Vol. 26, No. 3, Winter 2001/2002).
[36] Aaron L. Friedberg, *In the Shadow of the Garrison State: America's Anti-Statism and Its Cold War Grand Strategy*, (Princeton, New Jersey: Princeton University Press, 2000).
[37] Ibid. See also Aaron L. Friedberg, "Why Didn't the United States Become a Garrison State," *International Security* (Vol.16, No.4, Spring 1992) 136-141 for a discussion of the history of military-industrial interactions.
[38] Following sections address growing concerns with voluntary approaches in a post 9/11 world. See in particular, Stephen Flynn, *American the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*, (New York: Harper Collins Publishers, 2004), p 56.
[39] PCIS was a private sector initiative to share information and strategies across sectoral lines, and although the federal government is not officially part of the partnership, the government (first through CIAO and subsequently DHS) liaises with the group and provides administrative support. PCIS was incorporated as a non-profit corporation in 2001, and is operated by companies and associations in each of the critical infrastructure sectors. See http://www.pcis.org/index.cfm.
[40] "About InfraGard" at http://www.infragard.net/about.htm. InfraGard has expanded membership substantially, from 277 in October 2000 to almost 9,4000 in September 2003, with members including industry and other government agencies and the academic community. (Robert F. Darcey, "Homeland Security: Information Sharing Responsibilities, Challenges and Key Management Issues," Statement before the Subcommittee on Cyberspace, Science and Research and Development of the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives, 17 September 2003, p 24.)
[41] An example of the type of unclassified information disseminated by the government is the Department of Homeland Security/Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report, which is a daily summary and assessment of open-source published information concerning critical infrastructure issues, located at http://www.nipc.gov.
[42] Presidential Decision Directive 63.
[43] http://www.fsisac.com/faq.cfm
[44] As of April 2003, the Department of Homeland Security reported that there were sixteen ISACs, including some established for sectors not identified as critical infrastructure. See U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, DC: February 2003), p. 25. In July 2004, GAO reported on nine ISACs in critical infrastructure sectors, as well as others (real estate and research and education) and continuing efforts to establish ISACs in agriculture and healthcare. See U.S. General Accounting Office, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, DC: July 2004), p. 6-7.
[45] See https://www.it-isac.org/faq.php.
[46] See website of the Financial Services ISAC, at: http://www.fsisac.com/join.cfm.
[47] The FS-ISAC received a $2 million contract from the Treasury Department to enhance security awareness and protect critical infrastructure ("Financial Services Information Sharing and Analysis Center Funded to Protect America's Financial Infrastructure with Next-Generation Services," Press Release by FS/ISAC, 19 December 2003, at: http://www.fsisac.com. The Environmental Protection Agency issued a $2 million grant in March 2004 to the Water ISAC to fund operations and increase ISAC membership. (GAO-04-780, p 8.)
[48] The ISAC Council released a series of white papers in early 2004. See "Reach of the Major ISACs" and "A Functional Model for Critical Infrastructure Information Sharing and Analysis: Maturing and Expanding Efforts," ISAC Council White Paper, 31 January 2004, located at http://www.isaccouncil.com.

[49] "Private Sector Security Leaders Join Forces Against Terrorism," press release by the Financial Services ISAC, 14 October 2004 at: [GET CITE]
[50] See Robert F. Darcey, p 25.
[51] Tim Starks and Martin Edwin Anderson, "Congress, Industry Both in Dismay Over Homeland Security's Performance on Critical Infrastructure," Congressional Quarterly's Homeland Security, 2004, located at: http://www.ewa-iit.com/content.asp?sectionID=47&contentID=140. There appears to be some confusion as to how critical assets are identified, as the DHS's Information Analysis and Infrastructure Directorate reported in April on its list of 1,700 assets deemed "nationally" critical, that was derived from a database of 33,000 assets considered regionally or locally critical. See John Moteff and Paul Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," 1 October 2004, p. 13.
[52] Jonathan Krim, "Report Faults Cyber-Security," *The Washington Post*, 23 July 2004, E01.
[53] GAO-04-780, July 2004, p. 11.
[54] Jonathan Krim, Ibid.
[55] Stewart D. Personick and Cynthia A. Patterson, ed., *Critical Infrastructure Protection and the Law: An Overview of Key Issues*, (Washington: National Academies Press, 2003) available at http://books.nap.edu/books/030908878X/html/7.html#pagetop.
[56]The purpose of FOIA is to ensure US citizens access to government information. The issue of FOIA exemption for sharing of critical infrastructure information has been an extremely thorny and confused one, with public interest groups opposed to industry for what they view as an overly broad exception to FOIA that could allow a wider range of information to be protected, and possibly shield owners and operators from liability under environmental, health, tax or other laws. Critical infrastructure operators, however, content that current law does not provide certain protection and have advocated in favor of additional clarity. Legislation on both sides of the issue has been introduced in Congress that could have a substantial effect on companies' willingness to provide information to the government. For a thorough discussion of the issues, see John D. Moteff, "Critical Infrastructure Information Disclosure and Homeland Security," Report for Congress of the Congressional Research Service (RL31547), 29 January 2003.
[57] "DHS Launches Protected Critical Infrastructure Information Program to Enhance Homeland Security, Facilitate Information Sharing," 18 February 2004, available at http://www.dhs.gov/dhspublic/.
[58] Robert Block, "US Law Shields Company Data Tied to Security," *The Wall Street Journal*, 18 February 2004, p. B1; and John Mintz, "US to Keep Key Data on Infrastructure Secret," *The Washington Post*, 19 February 2004, p. A21.
[59] Officials of the Energy ISAC stated to the General Accounting Office that they have not reported incidents because of FOIA and antitrust concerns. (Darcey, p. 26).
[60] Personick and Patterson, pp. 30-34.
[61] The Business Roundtable, p. 27.
[62] Darcey, p. 29.
[63] See Personick and Patterson, Chapter 3, "Liability for Unsecured Systems and Networks," pp 35-60 for a discussion of liability issues and industry concerns.
[64] Limited information is available on private sector spending in the U.S. but even before September 11, 2001, was placed at between $40-$55 billion annually (See Patrick Lenain, Marcos Bonturi and Vincent Koen, "Economic Consequences of Terrorism," Organization for Economic Cooperation and Development, 17 July 2002, p 31, and " The National Strategy for Homeland Security," p. 65. See also "Picking the Locks on the Internet Security Market," Redherring.com 24 July 2001, which estimated the cyber security market prior to 9-11 at $10 billion in products and services which does include physical security measures.
[65] The Business Roundtable, "Terrorism: Real Threats. Real Costs. Joint Solutions., June 2003, p. 19.
[66] Flynn, p. 130.

[67] See "Terrorism: Real Threats. Real Costs. Joint Solutions," pp. 45-48.
[68] See GAO, February 2003 report, p. 57.
[69] Martin Edwin Anderson and Tim Starks, "Three Years After 9/11, U.S. Security 'Partnerships' With Industry Are a Work in Progress," Congressional Quarterly's Homeland Security, 2004, located at: http://www.ewa-iit.com/content.asp?sectionID=47&contentID=139.
[70] The Directorate is the focal point for infrastructure protection efforts within DHS. See US Department of Homeland Security, "Homeland Security: Budget in Brief, Fiscal Year 2005," p. 46-47.
[71] Final Report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission Report"), (New York: W.W. Norton & Company, 2004) p 398.
[72] "Homeland Security: Voluntary Standards are Underway at Chemical Facilities but the Extent of Security Preparedness in Unknown," General Accounting Office Report 03-439, 14 March 2003.
[73] See legislation introduced by Senator Jon Corzine (D-NJ) mandating security requirements at certain chemical plants, which died at the end of 2004 as a result of strong industry opposition. The issue was raised as part of the 2004 Presidential campaign, with Senator John Kerry criticizing the Bush Administration's voluntary approach to chemical and nuclear safety issues.
[74] Louis Uchitelle and John Markoff, "Terrorbusters Inc.: The Rise of the Homeland Security-Industrial Complex," *The New York Times*, 17 October 2004.
[74] Greta Wodele, "Panel Developing Infrastructure Protection Recommendations," *National Journal's Technology Daily*, 14 April 2004, at http://www.govexec.com/dailyfed/0404/041404tdpml.htm.
[76] Flynn, pg. 54 for a discussion of how the absence of clearly-defined standards actually place companies that invest in protective measures for infrastructure at a competitive disadvantage due to "tragedy of the commons" dilemma. See also pp 130-131.
[77] Personick and Patterson, pp. 56-60.
[78] Peter Orszag, "Homeland and the Private Sector: Testimony before the National Commission on Terrorist Attacks Upon the United States," 19 November 2003 at: http://www.brookings.edu/views/testimony/orszag/20031119.pdf, p. 1.
[79] Peter Orszag describes such measures as anti-terrorism subsidies, pg. 5.
[80] See in particular Stephen Flynn's book, p 145-155 for discussion of the merits of the creative idea of a Federal Reserve-like system for homeland security.

Critical infrastructure protection (CIP) consists of measures to safeguard interdependent systems, networks, and assets that form the backbone of services essential to society. Examples of vital physical infrastructure include roads, bridges, airports, communication facilities, and power plants.Â Thatâ€™s why McAfee believes the private sector should take the lead role in protecting it. Government should allow industry to continue to innovate voluntarily in critical infrastructure protection. Regulations and mandates will be counterproductive to the goal of ensuring the protection of our critical infrastructure. If regulations were to force manufacturers to guard against todayâ€™s threats, tomorrowâ€™s might very well slip through the cracks.