CRITICAL INFRASTRUCTURE INFORMATION SHARING

Sean Gallagher
Michael Neugebauer

"Protecting America's critical infrastructure and key assets requires an unprecedented level of cooperation throughout all levels of government-with private industry and institutions, and with the American people. The federal government has the crucial task of fostering a collaborative environment, and enabling all of these entities to work together to provide America the security it requires."[1] Critical infrastructure (CI), as stated in the USA PATRIOT Act, are "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 any combination of those matters."[2] Put more succinctly by Senator Joseph Lieberman in a Senate hearing on the Homeland Security Act of 2002, critical infrastructure assets are "our nation's most vital organs."[3] Because these systems are so vital to the functioning of the nation, they have become attractive targets for terrorist attack.

Protection of our nation's critical infrastructure has been a priority for a decade. President Clinton officially recognized the destructive consequences of an attack upon our critical infrastructure. The administration formulated the basics for a network of shared information among the different levels of government as well as actors within the private sector. Post-September 11th, our nation's critical infrastructure protection policy experienced a major overhaul. In response to these events, our nation saw the creation of new governmental entities, the Office of Homeland Security and the Department of Homeland Security (DHS), passage of important legislation, the USA PATRIOT Act and the Homeland Security Act of 2002 (HSA), as well as the formulation of numerous national strategies.

Critical infrastructure information (CII) sharing provides several benefits. First, sharing allows greater coordination among the various levels of government. Information sharing among federal, state and local government entities better prepares each level of government to assess CI vulnerabilities, repair those vulnerabilities, and respond to threats and attacks. Second, sharing CII engages and improves the technical expertise of the private sector. By increasing the flow of information to private sector entities, which control much of the critical infrastructure, our nation will be better equipped to protect our CI assets.[4] Third, CII sharing allows faster and more efficient response and recovery. Better preparation will inevitably lead to better responses to terrorist attacks.

However, the effort to promote a greater level of CII sharing is not without its risks. As more information is shared, the likelihood of terrorist organizations accessing and exploiting that information increases. Therefore, heightened security measures will be required when sharing vital information. Additionally, information sharing in the private sector may lead to the incidental release of confidential business information to competitors and expose private sector entities to increased liability.

Several barriers must be overcome to employ an effective information sharing structure. First, the government must be able to ensure the sanctity of information released by private sector actors. Private sector entities desire limits to the application of the Freedom of Information Act on the information they share. Second, the stringent principles of originator control can inhibit the timely release of CII. Lastly, the inconsistencies in the various federal information security procedures hinder effective CII sharing. A single uniform system employed throughout the federal government will enhance the distribution of CII.

INTRODUCTION AND BACKGROUND

The recent events of September 11, 2001 proved our country is not immune to acts of terrorism. Terrorist attack capabilities have become

more complex, sophisticated, and potent over the years. This sophistication and potency is not limited to physical attacks. The Internet gives a single person the ability to harm those systems vital to the operation of our nation. The increasing interconnectivity of the nation's computer systems across multiple networks leave CI systems open to attack and exploitation. Accordingly, the protection of the critical infrastructure should be an area of high priority.

The United States must continue to protect its critical infrastructure through increased information sharing and proper implementation of government plans such as the National Strategy for Homeland Security. Critical infrastructure protection allows our nation to function in a smooth and effective manner. An electrical distribution facility is a good example of a critical infrastructure. This facility may be affected by either a physical attack, a car bomb which causes massive fires and destruction, or a virtual attack, sending a virus through the central computer system which shuts down the entire electrical grid.

An important part of protecting the critical infrastructure is information sharing between CI entities concerning vulnerabilities and weaknesses. Critical infrastructure information is "information which is not customarily in the public domain and related to the security of critical infrastructure or protected systems."[5] It is the goal of the United States government to promote CII sharing among all levels of the government and the private sector.

Protecting our nation's critical infrastructure is an idea of recent origin; the history of the government's efforts to ensure CI system protection goes back a decade. Recognizing the need for the government to work with the private sector to protect our nation's critical infrastructure, President Bill Clinton, in 1996, signed executive order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP).[6] The Commission stated the nation must develop a plan to protect the nation's critical infrastructure, but declared there were no immediate threats.[7] Future growth in technology and the availability of the Internet, however, indicated to the Commission a future threat to CI systems. Solving this problem requires sharing and combining information between members of different sectors, thereby creating the means necessary to identify flaws,

predict attacks, and reduce the possibility of attacks.[8]

In 1998, President Clinton promulgated Presidential Decision Directive 63 (PDD-63), which created the Information Sharing and Analysis Centers (ISAC's).[9] The directive divided those activities associated with critical infrastructure into specific sectors,[10] each with an associated lead agency, a sector liaison official, and a private sector coordinator, all of whom would help to establish a National Infrastructure Assurance Plan (NIAP).[11] For example, the banking and finance sector would communicate and coordinate with the Department of Treasury. Finally, the directive empowered the Federal Bureau of Investigation to create a National Infrastructure Protection Center (NIPC), which would serve as a central location to deposit and analyze information to properly assess threats, provide timely warnings, and respond to attacks on critical infrastructure.[12] At this time, protection of private firm's confidential information was not a focal point of the discussion and only briefly mentioned.

The policies and programs associated with protecting critical infrastructure evolved when President George W. Bush entered the White House. Critical infrastructure moved to the forefront of national policy after the attacks of September 11, 2001. In response, President Bush created the Office of Homeland Security.[13] The Office of Homeland Security, headed by the Assistant to the President for Homeland Security, Tom Ridge, sought to establish a response plan to terrorist attacks and implement methods of protecting the nation's critical infrastructure, especially those related to energy production, transportation, and telecommunications.[14] A week later, President Bush signed Executive Order 13231 extending the policies laid out in PDD-63.[15] This order established methods and organizations, such as the President's Critical Infrastructure Protection Board (PCIPB) and National Infrastructure Advisory Council (NIAC), which would respond to and limit the damage of future CI attacks.

The USA PATRIOT Act furthered the protection of the critical infrastructure. The act promoted a public-private partnership, including corporate and non-governmental organizations, to ensure attacks are rare and brief with only a minimal impact on critical infrastructure.[16] Furthermore, the act established the National Infrastructure

Simulation and Analysis Center (NISAC) to "serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation."[17] Among NISAC's efforts is conducting modeling and simulations of CI systems to determine existing vulnerabilities.[18]

The July 2002 National Strategy for Homeland Security established a comprehensive plan to address all aspects associated with terrorist attacks. The new plan would attempt to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, minimize damage, and allow quick recovery from successful attacks.[19] Furthermore, the plan contained five initiatives to improve the flow of information from one organization to another via:

> (1) integration of information sharing across the federal government,
>
> (2) integration of information sharing across state and local governments, private industry, and citizens,
>
> (3) adoption of common "meta-data" standards for electronic information relevant to homeland security,
>
> (4) improvement of public safety emergency communication, and
>
> (5) guaranteeing reliable public health information.[20]

To further these goals, Congress passed and the President signed the Homeland Security Act of 2002 establishing the Department of Homeland Security (DHS). The new department consolidated previously overlapping organizations and continued to help establish, initiate, and formulate ways in which the government can protect and respond to terrorist attacks.[21] The Information Analysis and Infrastructure Protection Directorate (IAIP) is the entity charged with addressing critical infrastructure issues and problems.

In February of 2003, the Bush Administration promulgated two national strategies dealing specifically with the critical infrastructure. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets sets out an overall framework along with a litany of national goals to secure the infrastructure assets from terrorist attack.[22] Especially important to the national effort is the participation of private sector entities in information sharing. The Strategy also provides a sector-specific analysis of challenges facing the CI entities as well as any future initiatives the government will implement. The National Strategy to Secure Cyberspace focuses on protecting a major piece of the critical infrastructure especially susceptible to terrorist attack, the Internet. This new plan sought to:

> (1) prevent cyber attacks against America's critical infrastructure,
>
> (2) reduce national vulnerability to cyber attacks, and
>
> (3) minimize damage and recovery time from cyber attacks.[23]

Most recently, on December 17, 2003, President Bush issued Homeland Security Presidential Directive Seven. This directive outlines how the Secretary of Homeland Security will guide and instruct the government agencies in preventing and responding to various emergency situations, including terrorist attacks.[24] The country will be secured when federal agencies provide effective, efficient, and timely delivery of federal preparedness assistance to state and local governments and ensure responders have the necessary means and training to appropriately respond to terrorist actions.[25]

BENEFITS OF SHARING CRITICAL INFRASTRUCTURE INFORMATION

Sharing CII provides greater coordination among the levels of government, improvements in the technical expertise of the private sector, and a more efficient response and recovery time of CI systems during an attack.

Greater Coordination among the Levels of Government

At the federal level, DHS acts as the central depository for information associated with the critical infrastructure. A similar model exists at the state level with the added benefit of a more intimate relationship with local private sector entities. Through CII sharing, all levels of government will have a more complete and accurate picture of homeland defense.

The Homeland Security Act created five under secretaries with distinct mandates to meet the goals of the DHS. The Information Analysis and Infrastructure Protection Directorate (IAIP) is to make assessments of the critical infrastructure to determine the susceptibility to attack of any CI entities, develop a comprehensive national plan to secure the critical infrastructure, and recommend, in coordination with the other levels of government and the private sector, measures necessary to protect CI assets.[26] In order to accomplish this task efficiently, the IAIP has the power to access and analyze law enforcement information, intelligence information, and other information from all CI sectors to integrate, identify, and assess the nature and scope of terrorist threats to the homeland. Moreover, the IAIP has the ability to disseminate information analyzed by DHS to homeland security entities responsible for deterring, preventing, and responding to terrorist threats. In essence, the IAIP functions as a "CII warehouse." The IAIP will direct an effort to send and receive vast amounts of information necessary for CI protection. One central location for CII dissemination allows entities to receive information in an expedited manner and enhance CI system protection.

To facilitate its mission, the HSA of 2002 transferred to IAIP control of two federal organizations created under PDD-63, the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC).[27] The CIAO, previously under the Department of Commerce, is charged with establishing a national plan for CI protection. NIPC, formerly part of the FBI, pro-

vides warnings of international threats, conducts law enforcement investigations, and responds to CI threats and attacks.

The participation of state and local governments adds to the greater coordination among the levels of government. State and local governments have the unique position of being able to forge intimate relationships with the various CI entities within their borders to help facilitate CII sharing. Involvement by the states and CI entities will lead to more efficient sharing with the IAIP. In New York State, the entity responsible for critical infrastructure security is the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC).[28] CSCIC develops uniform standards of cyber preparedness for the state's CI systems, coordinates with the private sector to examine potential vulnerabilities to cyber attack, and eliminates redundancy between the private sector and state and federal initiatives.[29] CSCIC accomplishes these goals through the Public/Private Sector Cyber Security Workgroup (Public/Private Workgroup) and the Multi-State Information and Analysis Center (Multi-State ISAC).

The Public/Private Workgroup is an organization of representatives from government, academia, and the private sector that meets to determine the cyber readiness of New York State. To focus their efforts, the Workgroup has identified specific critical sectors that will receive priority attention, including financial and economic, telecommunications and utilities.[30] To protect CI assets, each sector is to conduct an inventory to know which CI assets deserve protection, determine whether vulnerabilities to an attack exist, and measure the risk associated with the vulnerability.

The Multi-State ISAC is an association of states focused on facilitating communication regarding cyber and CI readiness and response efforts. The efforts of the Multi-State ISAC center on providing a focal point for gathering information on cyber and physical threats to CI systems and encouraging two-way information sharing on CI threats and incidents between the states and the federal government. Through a monthly reporting system, the states will disseminate early warnings, share security incident information, provide trending, and distribute current proven security practices. Although not currently in every state, the eventual goal of the Multi-State ISAC is to extend to all fifty states.

Involving the Technical Expertise of the Private Sector

Involving the technical expertise of the private sector is integral to CI protection. Both federal and state governments have developed groups intent on bringing together various private sector entities with the government in order to share information. The federal government utilizes Information Sharing and Analysis Centers (ISAC's). PDD-63, in creating the ISAC's, identified the various sectors that make up the critical infrastructure.[31] The goal of the ISAC's is to serve as a clearinghouse where private sector and government officials can meet to gather, analyze, and disseminate CII between the different sectors as well as to the different levels of government. To provide an example on the state level, the aforementioned New York Public/Private Workgroup serves a comparable function to the ISAC's.

The expertise of medical and scientific personnel may have an impact on improving CI protection. For example, in order to respond to such threats as biological warfare, the Department of Health and Human Services, and other governmental agencies, will work together to improve the quality and strength of countermeasures like the smallpox vaccine.[32] Furthermore, having a central location where the information of various organizations, both governmental and private, can be pooled together may enhance scientific research and expertise. Implementation of a system of research centers modeled after the National Nuclear Security Administration laboratories will allow top scientists to test novel theories and technology to combat terrorist attacks.[33]

Implementing an effective information sharing program benefits the private sector in several ways. Programs that preempt and prevent damage to our critical infrastructure may lower the overall cost associated with a terrorist attack. Over the last several years, the costs relating to a CI attack have increased fourfold.[34] By investing in Internet and cyberspace protection, a business may be able to reduce the amount of money required to rebuild a system that lacks safety features.[35] Furthermore, businesses can receive federal aid in the form

of grants or tax breaks which will offset the money they invest in CI protection.[36]

Greater Response and Recovery

Increased information sharing will reduce the effects of a terrorist attack. Information sharing will allow discovery of patterns and trends of various organizations and increase the level of preparedness.[37] Personnel response time will dramatically decrease through coordinated information sharing by government entities such as the Critical Infrastructure Assurance Office.[38] The effective transfer of information will eliminate the mass confusion created when terrorists implement multiple attacks.[39] Furthermore, by increasing information sharing, the United States and our allies will be able to clearly form a plan to eliminate terrorist support in foreign nations.[40] Because all levels of government will have all the necessary information, the nation will be better able to anticipate, predict, and preempt terrorist attacks.

Defending the nation against terrorism is not limited to offensive strikes against terrorist cells and organizations. As Deputy Director of Homeland Security (now Secretary of the Navy) Gordon England stated in September of 2002, “You can’t wait for the first situation to arise and then react. The consequences would be horrendous.”[41] Through the implementation of defensive actions, such as warning systems and security and management plans, the government will be able to quickly and effectively respond to attacks, while at the same time deter our enemies.[42] Proper communication among government agencies will provide the government with an adequate method to assess the level of the nation’s preparedness. Implementing evaluation plans will allow the federal government to determine areas of concern and more productively use its money and labor.[43] Personnel issues have an impact on the overall ability to protect the homeland. The sharing of information will allow agencies to complement one another and eliminate the possibility of job redundancy.[44] The increased flow of CII will dramatically improve the way the nation can prevent and respond to terrorist attacks.

RISKS OF SHARING CRITICAL INFRASTRUCTURE INFORMATION

Although benefits of CII sharing do exist, several risks also make information sharing problematic. These risks include an increased vulnerability to attack on CI systems and the unauthorized release of CII shared by a critical infrastructure entity.

Increased Vulnerability

CII sharing, while beneficial, can also increase the vulnerability to an attack. The interconnectivity and interdependency of networks among all areas of the infrastructure leads to the greater risk of an attack. Information flowing between various entities can increase the likelihood of a terrorist organization accessing and exploiting that information. Once obtained, terrorists can use the information to multiply the effect and lethality of an attack.

The increasing technological proficiency of terrorists, resulting from greater access to better and more inexpensive technology, makes an attack upon critical systems and assets an increasing likelihood.[45] Terrorist attacks, moreover, have become increasingly complex and sophisticated. The trend is for terrorists to not only target physical structures but also the cyber systems that support those structures. Referred to as “swarming attacks,” terrorists will use coordinated attacks, often employing different methods, against physical targets and the surrounding infrastructure to cause multiplied or cascading effects.[46]

The goals of terrorists employing “swarming attacks” can be threefold:

1) to complicate response to the attack;

2) to widen the effects of the attack; and

3) to worsen the effects of an attack.[47]

First, in complicating the response, terrorists may focus on delaying notification of the attack or denying resources to effectively manage the consequences. For example, a terrorist organization can hack into a computer network to disable the distribution of water in an area, leaving the fire department without any water to combat fires resulting from a physical attack.[48] Second, in widening the attack, terrorists can increase the physical damage as well as the psychological damage to an area's populace. Applying the above water distribution example to the attacks of September 11th, the attack would not only incapacitate the fire department but also the rest of lower Manhattan – including emergency services like hospitals – for days, if not weeks.[49] Third, terrorists can employ swarming attacks to worsen the effects of an attack. Terrorists, for example, can disable the ventilation systems of a large city's subway system and then release a chemical or biological agent into the tunnels to increase the potency of an attack.

In order to mitigate the exploitation of interconnectivity resulting from CII sharing between public and private entities, it is necessary to implement an effective information security program. The result of such efforts, however, often ends in CI entities receiving outdated information or sometimes no information at all. This dichotomy will be more fully explained in the Barriers to Information Sharing section.

Unauthorized Release of Protected Information

CII sharing between the public and private sectors plays an integral role in decreasing the threat of terrorist attacks. The flow of information between so many entities can lead, however, to the release of information to the public that is both unintended and undesired. The release of such information will expose private sector entities to unwanted risks. This exposure will likely impede further information sharing between various CI entities.

The private sector, in general, is reluctant to share any CII with the government.[50] For a number of reasons these entities do not feel it is in their best interest to provide the government with information. This reluctance is not due to an aversion towards the government,

but rather because the private sector has not determined if the government can ensure the security of the information they are conveying. Information falling into the hands of competitors is often the most cited reason for the private sector's unwillingness to share information. Private sector entities do not want competitors obtaining important trade secrets and business information, inevitably harming their competitive advantage.[51] The private sector also fears an increase in exposure to liability because of the disclosure of CII by the government.[52] The possibility of facing numerous liability lawsuits from CII disclosure forces the private sector to remain reticent. The private sector entities feel the exposure to such risk is too great and it is better to "keep [their] mouth[s] shut."[53]

The private sector is not the only entity circumspect about the release of information. Government agencies also desire the confidentiality of certain information. The protection of current vulnerabilities within the critical infrastructure and the methods employed to rectify those vulnerabilities is particularly important to the government.[54] Releasing such information can expose existing vulnerabilities – or create new ones – for terrorists to exploit. Additionally, the government does not want to release information that would compromise existing intelligence activities and investigations.[55] Release of such material can, among other things, expose current investigations, and, perhaps more importantly, hinder future prosecutions.

BARRIERS TO SHARING CRITICAL INFRASTRUCTURE INFORMATION (AND ATTEMPTS TO DISSOLVE THEM)

Significant barriers to CII sharing exist. Among these barriers is the private sector's reluctance to share information, originator control principles for those entities submitting the information, and a lack of uniform information security procedures. This section also identifies any attempts to dissolve these barriers in order to facilitate CII sharing.

Private Sector Reluctance to Share Information

As previously mentioned, the private sector is reluctant to share CII with the government principally because the information might be released to the public. Consideration of competitive advantage, liability, and existing vulnerability issues force the private sector to hesitate in offering any information to the government. The information that the private sector can offer, however, is vital to the operation of DHS. The need for this information resulted in a section of the Homeland Security Act of 2002 providing an exemption from disclosure of the information under freedom of information laws.[56]

Public access to government information was the impetus behind the passage of the Freedom of Information Act (FOIA).[57] However, several exemptions written into the FOIA allow the government to withhold certain information from public disclosure. The exemptions relevant to the operation of the HSA are:

> 1) information exempted from disclosure by another statute[58] and,
>
> 2) trade secrets and commercial or financial information.[59]

The latter exemption appears to cover any CII a private sector entity would submit to the federal government. In fact, courts interpreting the trade secrets exemption have been deferential in granting a FOIA exemption for information voluntarily provided to the government when it is "of a kind not customarily released to the public."[60] But to meet this standard, the agency invoking the trade secrets exemption must "meet the burden of proving the provider's custom."[61] Though not an insurmountable burden for the government to satisfy, this standard likely led the authors of the HSA to seek an exemption elsewhere – by exempting disclosure through another statute.

Section 214 of the HSA applies to any CII "voluntarily submitted to a covered federal agency for use by that agency regarding the security of critical infrastructures and protected systems."[62] For purposes of the act, "critical infrastructure information" means "information not

customarily in the public domain and related" to:

> 1) an actual, potential, or threatened attack or interference of CI systems that violates federal or state law, harms interstate commerce, or threatens public safety;
>
> 2) the ability of any CI system to resist such interference or incapacitation; or
>
> 3) any planned or past operational problem or solution regarding CI systems.[63]

(This definition has received significant criticism for likely allowing any infrastructure information provided by a private sector entity to receive protected status.[64]) A "voluntary" submittal occurs when "in the absence of [an] agency's exercise of legal authority to compel access" to such information.[65] When a private sector entity submits such information accompanied by an express statement identifying it as CII and declaring it for CI protection, it shall be exempt from disclosure under FOIA. For example, a computer software manufacturer can provide DHS with information concerning the susceptibility of its software used by many electricity companies to certain types of viruses. Information such as this will likely receive protected status under the HSA.

In accordance with HSA requirements,[66] DHS, in April of 2003, proposed rules for handling CII.[67] The proposed rules set out criteria for accessing, sharing, and disseminating CII within DHS, among the federal, state and local governments, and the private sector. The DHS procedures note that it is DHS policy to "encourage [the] voluntary submission of CII by protecting that information from unauthorized disclosure."[68] CII receives "protected" status under the procedures when it is "voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose" while accompanied by an express statement indicating the desire of the submitter to have the information protected.[69] The proposed procedures do not place a burden upon the government to show a submitter's customary treatment of shared infor-

mation as espoused in the *Critical Mass* case. Rather, the procedures grant deference to a submitter's expectations of qualifying for protection.[70]

Members of the private sector and the government generally favor strong measures to protect voluntarily provided CII because they do not want to damage their competitive position or expose themselves to liability litigation. Therefore, they require strong assurance that any information provided will remain confidential and undisclosed. Consequently, some parties want to provide the strongest FOIA exemption possible to private sector entities. The focus should be on maximizing the private sector's confidence in the government's ability to protect CII.[71] This, it is argued, is the best way to ensure robust information sharing.

Conversely, several open government advocates have expressed their unease with what they feel is the evisceration of FOIA under the HSA and subsequent DHS procedures. The primary concern centers on corporate and governmental accountability to the public. Private sector actors, as well as the DHS, it is argued, can utilize the broad language of the FOIA exemption to shield any failures or exposed lack of security in the critical infrastructure.[72] The HSA prohibits the use of protected CII in any civil action arising under federal and state law.[73] The concern arising from this protection is that companies, once they become aware of a vulnerability that can result in injury, will dump documents on the government to protect themselves from legitimate liability claims.[74] Moreover, the protection will shield important information from the public regarding existing vulnerabilities within their community.[75] The alternative to secrecy and shielding information would be to encourage openness to foster remedial action to protect CI systems.

In addition to the FOIA exemption, the HSA also preempts the application of state freedom of information laws.[76] Many individual states also have freedom of information laws operating upon their state governments. New York State, for example, requires access to government records much the same as the federal law.[77] However, the HSA, in granting a FOIA exemption for CII, also includes language to preempt access to CII through state freedom of information laws. The

HSA states that any CII offered to a State or local government entity shall not "be made available pursuant to any State or local law requiring disclosure of information or records."[78] There is, however, one exception to the preemption of state freedom of information laws. Information "independently obtained" by a state or local government is not subject to the HSA and can be used in any manner permitted by law.[79] The DHS procedures echo this language both on the state law preemption and the "independently obtained" exception. A foreseeable problem can arise, however, when the phrase "independently obtained" is considered. The HSA and DHS procedures do not state which level of government, federal or state, determines if information is independently obtained. Moreover, the authority does not provide a definition of what "independently obtained" means.

Within the past year, both houses of Congress have offered legislation to replace the language of the HSA FOIA exemption.[80] The bills would amend the FOIA exemption by refining the definition of "furnished voluntarily" to essentially refer to records, as opposed to "information" under the HSA, not submitted under any authority or legal requirement of DHS. Additionally, the bills would require the submitter to affirmatively designate that the information would not be made available to the public. The new language, moreover, would not preempt the operation of state freedom of information laws concerning information obtained independently of DHS. At the time of this writing, both bills are still in their respective committees (and will probably not reach the floors of the House or the Senate for a vote).

Originator Control Principles

The principle of originator control, employed among those sharing information, can hinder the smooth distribution of information. Originator control works on the understanding that the release of information provided in confidence is prohibited, unless consented to by the provider.[81] This authority, for example, can be used by private sector entities to ensure that any CII they provide to the government remains undisclosed. Additionally, the practice of our government has been to grant the agency heads broad discretion in controlling the papers and documents of the various departments.[82] The implications of this departmental authority, allow department heads to dictate to

whom information is sent and to where other departments receiving the information can send it. The purpose of FOIA was to dilute this discretion, but as shown in the previous section, the HSA and the proposed DHS procedures can exempt the operation of FOIA regarding CII.

The DHS proposed rules for handling CII provide practical insight into the concept of originator control. Under the rules, DHS will create a Critical Infrastructure Information Program to implement the procedures. The CII Program Manager will have the authority to determine if submitted CII will receive protected status.[83] When the CII receives the protected designation, the Program Manager will determine which entities, Federal, State or local, may receive the CII, when such information is "shared for purposes of securing critical infrastructure and protected systems."[84] Further, for State and local governments to receive CII, they must enter into an agreement with the CII Program Manager to acknowledge the responsibilities that accompany receipt of the information. Any state or local entity wishing to share or disseminate the CII they receive under the DHS procedures must receive permission from the CII Program Manager. The CII Program Manager, in turn, must request and receive permission from the submitting entity before granting permission to the State or local government.

To make the intricacies of the proposed rules more understandable and concrete, a simple example should suffice. Company X, an electricity provider to several states within the northeast on an interconnected grid system, provides DHS with confidential information about certain problems with its power grid that could result in sudden blackouts across its region of coverage. The CII Program Manager determines the information meets the requirements of the DHS procedures and gives the information protected status. New York State, a customer of Company X, wanting to ensure that its computer systems will remain intact during a blackout, receives the information from DHS at its CSCIC office. Pennsylvania, another customer of Company X, requests New York to relay any information it knows about Company X's susceptibility to blackouts so it too can fortify its computer systems. While New York would like to convey this information, under the DHS procedures it cannot. New York must first

request the CII Program Manager to release the information. The Program Manager, in turn, must receive permission from Company X before the information may be released to Pennsylvania. The main problem inherent in this program is access to timely information. CI entities must wait for prior approval before gaining access to information that could help secure their CI assets. Moreover, there is a strong chance that the New York State grid would still be susceptible to black out because Pennsylvania does not possess the information required to secure its own grid.

Currently, no authority to deal with the problem of originator control exits. By mandating the approval of the release of CII, either through the Program Manager or the original submitter, the DHS procedures ensure the sanctity of a submitter's CII. Problems can arise, however, because the procedures employ a time consuming process that may not deliver the necessary information in time for it to be of any value in CI protection.

Varied Security Procedures for Information

As stated before, the interconnectivity and interdependency of the computer networks among the CI entities, both public and private, can lead to the exploitation of those system's vulnerabilities. Ensuring the integrity of information concerning the critical infrastructure is crucial in the effort to secure those systems. Previously, the security procedures within the various departments of the federal government lacked consistency. Recent legislative efforts from Congress, however, mandated the uniformity of security procedures among the federal departments. The problem, nevertheless, has been the haphazard implementation of the programs at the agency level.

The enactment of the Federal Information Security Management Act (FISMA), in late 2002, permanently authorized the Government Information Security Reform Act (GISRA).[85] The focus of FISMA, and the previous legislation, was to coordinate the various security procedures of the federal government agencies to ensure the sanctity of confidential information within those departments by establishing and maintaining "minimum controls" for the information.[86] FISMA allows each agency the independence to implement and apply its own

program. However, the National Institute of Standards and Technology (NIST) is to develop minimum standards and guidelines to aid each agency in the development of its own program.

Agency oversight is integral to the functioning of FISMA. The Inspector General of each agency or an independent auditor if an agency does not have an IG, is to conduct an annual evaluation of the agency program to document the progress – or lack thereof – under FISMA.[87] Once each agency conducts its own evaluation, the Office of Management and Budget (OMB) will annually report to Congress on the overall progress under FISMA.[88]

The implementation of the information security programs, while progressing, is not occurring as quickly as necessary. Several federal systems still lack adequate protection from security breaches that can harm critical systems.[89] The result is the continued weakness in CI systems – especially at the federal level – that put operations and assets at risk. Included in the several factors responsible for this are, among other things, the lack of senior management attention to information security, limited security training, and the inability to detect, report, and share information on vulnerabilities or intrusions.[90]

Additionally, not all the agencies follow the NIST standards and guidelines concerning their information security programs.[91] An agency can develop their own security methodology, but not incorporating the elements that the NIST offers leaves the agency prone to misidentifying – or not identifying at all – significant security weaknesses. It is important to note that a one size fits all model is impractical when dealing with the intricacies of security management, but a standard framework for assessing and correcting information security risks will help federal agencies appropriately protect shared data.[92]

The federal agencies could use some guidance on this point. It might be necessary to employ a system at the federal level to define the roles and responsibilities of the individual agencies, describe the interrelation between each, and assess agency accountability for successes and failures.[93] Some agencies are having difficulty with identifying and developing a plan to protect critical information systems. It is therefore necessary that agencies receive the necessary technical expertise

and support to accomplish this task.[94]

CONCLUSION

Securing the homeland is of critical importance to the government and the nation as a whole. Protection of our nation's most valued assets, specifically the critical infrastructure entities is integral to this endeavor Terrorists will seek to exploit any open vulnerability because the interconnected nature of the critical infrastructure within our nation makes these assets especially susceptible to terrorist attack. To properly secure the critical infrastructure from terrorist attack, the levels of government as well as the private sector must communicate forthrightly, frequently, and efficiently to eliminate vulnerabilities and create effective response plans.

Much has been accomplished in this regard as CI protection has continually moved forward over the last decade. A basic framework of a CII sharing network has been established and the government has built on this initial structure to increase participation by all CI entities. The benefits of this framework are clear: more information is being shared with all the CI entities to prevent attacks and improve response time to terrorist threats. However, much more work needs to be done. Existing barriers prevent the full implementation of a complete CII sharing regime. Attempts have been made to overcome these barriers, but legitimate questions concerning injury to the public interest have been raised. Only when these barriers are broken down, while at the same time respecting the public interest, will the nation reap the benefits of a complete and robust CII sharing framework.

ACRONYMS

CI	Critical Infrastructure
CIAO	Critical Infrastructure Assurance Office
CII	Critical Infrastructure Information
CSCIC	Office of Cyber Security and Critical Infrastructure Coordination
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GISRA	Government Information Security Reform Act
HSA	Homeland Security Act of 2002
HSPD	Homeland Security Presidential Directive
IAIP	Information Analysis and Infrastructure Protection Directorate
ISAC	Information Sharing Analysis Center
NIAC	National Infrastructure Advisory Council
NIAP	National Infrastructure Assurance Plan
NIPC	National Infrastructure Protection Center
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NNSAL	National Nuclear Security Administration Laboratories
ORCON	Originator Control
PCCIP	President's Commission on Critical Infrastructure Protection
PCIPB	President's Critical Infrastructure Protection Board
PDD	Presidential Decision Directive
USA PATRIOT ACT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

ENDNOTES

[1] The White House, *The National Strategy for Homeland Security*, 29 (July 2002) available at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, § 1016, 115 Stat. 401 (2001) [hereinafter USA PATRIOT Act].

[3] *Securing our Infrastructure: Public/Private Information Sharing Before the Senate Comm. on Governmental Affairs*, 107th Cong. (2002) (statement of Senator Joseph Lieberman, Chairman, Senate Governmental Affairs Committee) [hereinafter *Senate Hearing on the Infrastructure*].

[4] According to the CERT Coordination Center of Carnegie Mellon University, the private sector owns and operates 85% of CI assets.

[5] Homeland Security Act of 2002, Pub. L. No. 107-296, § 212(3), 116 Stat. 2151 (2002) (codified at 6 U.S.C. 131). [hereinafter HSA of 2002].

[6] Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

[7] John D. Moteff, Congressional Research Service, *Critical Infrastructures: Background, Policy, and Implementation*, RL30153 (Feb. 10, 2003).

[8] John D. Moteff and Gina Marie Stevens, Congressional Research Service, *Critical Infrastructure Information Disclosure and Homeland Security*, RL31547 (Jan. 29, 2003).

[9] Presidential Decision Directive 63 (May 22, 1998) available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm [hereinafter PDD-63].

[10] The sectors identified in PDD-63 are: Information and Communication, Banking and Finance, Water, Transportation, Emergency Law Enforcement, Emergency Fire Service, Emergency Medicine, Electric Power, Gas, and Oil, Law Enforcement and International Security, Intelligence, Foreign Affairs, and National Defense.

[11] PDD-63, supra note 9.

[12] Id.

[13] Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001).

[14] Id. at § 3.

[15] Exec. Order No. 13,231, 66 Fed. Reg. 53,061 (Oct. 18, 2001).

[16] USA PATRIOT Act, supra note 2, § 1016(c)(1), 115 Stat. 400.

[17] Id. at § 1016(d), 115 Stat 401.

[18] NISAC is a part of Sandia National Laboratories (SNL) and Los Alamos National Laboratories (LANL).

[19] *The National Strategy for Homeland Security*, supra note 1, at 3.

[20] *The National Strategy for Homeland Security*, supra note 1, at 3.

[21] HSA of 2002, supra note 5.

[22] The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003) available at http://www.whitehouse.gov/pcipb/physical_strategy.pdf.

[23] The White House, *The National Strategy to Secure Cyberspace* (Feb. 2003) available at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[24] The White House, Homeland Security Presidential Directive Number 7, §§ 3, 4, 5 (Dec. 17, 2003) available at http://www.fas.org/irp/offdocs/nspd/hspd-7.html [hereinafter HSPD-7].

[25] Id. at §§ 5(a) & (b).

[26] HSA of 2002, supra note 5, at § 201 et. seq, 116 Stat. 2145 (codified at 6 U.S.C. 121).

[27] Id. at § 201(g).

[28] Information on CSCIC is available at http://www.cscic.state.ny.us (last visited Jan. 29, 2004).

[29] Cyber Security Protecting New York State's Critical Infrastructure available at http://www.cscic.state.ny.us/reports/priv_public.htm.

[30] The eight "priority" sectors that CSCIC will focus their initial efforts on are: financial and economic, health, telecommunications, utilities, government, transportation, education and awareness, and public safety.

[31] PDD-63, supra note 9, Annex A.

[32] The National Strategy for Homeland Security, supra note 1, at 39.

[33] The National Strategy for Homeland Security, supra note 1, at 53.

[34] Id. at 34.

[35] Id. at 9-10.

36 U.S. General Accounting Office, Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues, GAO-03-1165T,

13 (Washington, D.C.: Sept. 17, 2003).

[37] Id. at 10.

[38] *The National Strategy for Homeland Security*, supra note 1, at 57.

[39] Benjamin Riley, *Information Sharing in Homeland Security and Homeland Defense: How the DOD is Helping*, The Journal of Homeland Security (Sept. 2003) available at http://www.homelandsecurity.org/journal/Riley.html.

[40] *The National Strategy for Homeland Security*, supra note 1, at 16.

[41] Riley, supra note 39.

[42] *The National Strategy for Homeland Security*, supra note 1, at 17.

[43] GAO-03-1165T, supra note 36, at 51.

[44] *The National Strategy for Homeland Security*, supra note 1, at 25.

[45] GAO-03-1165T, supra note 36, at 5.

[46] National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

[47] Id. at 6.

[48] NIPC, supra note 46, at 7.

[49] Id.

[50] Moteff and Stevens, supra note 8, at 2.

[51] Id. at 2. See also *Senate Hearing on the Infrastructure*, supra note 3, (statement of Harris N. Miller, President, Information Technology Association of America).

[52] *Senate Hearing on the Infrastructure*, supra note 3, (statement of Ty R. Sagalow, Board Member, Financial Services ISAC, and COO, AIG eBusiness Risk Solutions).

[53] Id.

[54] Moteff and Stevens, supra note 8, at 2.

[55] Id.

[56] HSA of 2002, supra note 5, at § 214 (a)(1)(A). The FOIA exemption is found in a piece of the HSA with the short title "Critical Infrastructure Information Act of 2002" and can also be referred to by that name or the acronym "CIIA". It is codified at 6 U.S.C. § 101, et seq.

[57] Freedom of Information Act, 5 U.S.C. § 552 [hereinafter FOIA].

[58] FOIA, at § 552 (b)(3).

[59] Id. at § 552 (b)(4).

[60] See *Critical Mass Energy Project v. Nuclear Regulatory Commission*, 975 F.2d 871, 879 (D.C. Cir. 1992). (It should be noted that not all of the circuits have adopted this interpretation.)

[61] Id.

[62] HSA of 2002, supra note 5, at § 214(a), 116 Stat. 2152.

[63] Id. at § 212(3), 116 Stat. 2151.

[64] See Rena Steinzor, *Democracies Die Behind Closed Doors: The Homeland Security Act and Corporate Accountability*, 12 KAN. J.L. PUB. POL'Y 641 (2003).

[65] HSA of 2002, supra note 5, at § 212(7), 116 Stat. 2152.

[66] Id. at § 214(e), 116 Stat. 2154.

[67] Procedures for Handling Critical Infrastructure Information, Proposed Rule, 68 Fed. Reg. 18523 (proposed April 15, 2003) (to be codified at 6 C.F.R. pt. 29)[hereinafter DHS Procedures].

[68] Id. at § 29.1.

[69] Id. at §§ 29.2(f), 29.5(b).

[70] DHS Procedures, supra note 67, at § 29.6(e).

[71] *Senate Hearing on the Infrastructure*, supra note 3, (statement of Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation).

[72] *ACLU Statement for the Record Concerning Public-Private Information Sharing and Critical Infrastructure Sharing*, June 5, 2002, available at http://www.aclu.org/NationalSecurity/NationalSecurity.cfm?ID=10424&c=108 (last visited Nov. 16, 2003); See also Steinzor, supra note 64.

[73] HSA of 2002, supra note 5, at § 214(a)(1)(C), 116 Stat. 2153.

[74] See Steinzor, supra note 64.

[75] *Senate Hearing on the Infrastructure*, supra note 3, (statement of David Sobel, General Counsel, Electronic Privacy Information Center).

[76] HSA of 2002, supra note 5, at § 214(a)(1)(E), 116 Stat. 2153.

[77] Pub. Off. Law, Art. 6 § 87.

[78] HSA of 2002, supra note 5, at § 214(a)(1)(E)(i), 116 Stat. 2153.

[79] HSA of 2002, supra note 5, at § 214 (c), 116 Stat. 2154.

[80] Restoration of Freedom of Information Act of 2003, S. 609, 108th Cong. (2003); Restoration of Freedom of Information Act of 2003, H.R. 2526, 108th Cong. (2003).

[81] Alasdair Roberts, *ORCON Creep: Networked Governance, Information Sharing, and the Threat to Government Accountability*, available at http://faculty.maxwell.syr.edu/asroberts/research.html (Forthcoming in Government Information Quarterly).

[82] Moteff and Stevens, supra note 8, at 4 (citing the Housekeeping Statute of 1789 and the Administrative Procedures Act (APA) of 1946).

[83] In making this determination, the CII Program Manager will give deference to the submitter's expectation of meeting CII protection.

[84] DHS Procedures, supra note 67, at § 29.8(b).

[85] Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347 (codified at 44 U.S.C. § 3541, et seq.) [hereinafter FISMA] This act superceded a section of the HSA under the same name.

[86] Id. at § 3541.

[87] Id. at § 3545(a).

[88] Id. at § 3545(g).

[89] U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington D.C.: April 8, 2003). (It should be noted that this report deals with an analysis of the federal government implementation of security procedures under GISRA, which preceded FISMA. Nevertheless, the similarities shared by the two acts make the report a good indicator of the direction of the federal government concerning information security.) See also U.S. General Accounting Office, *Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements*, GAO-03-852T (Washington D.C.: June 24, 2003).

[90] GAO-03-564T, supra note 89, at 22-24.

[91] Id. at 26.

[92] Id. at 40.

[93] GAO-03-564T, supra note 89, at 40.

[94] Id. at 41.

By sharing playbooks and threat information across CIKR, a kind of â€œherd immunityâ€ can be achieved that denies attackers the element of surprise or the reuse of attack vectors on new victims.Â Today, however, failure or malicious attack on critical infrastructure is real. So real, in fact, that U.S. Undersecretary of Defense Marcel Lettre declared that cyberattacks that result in the destruction of critical infrastructure or serious economic impact should be closely evaluated as to whether or not they would be considered an act of war. With the pace of innovation and digital transformation, the threat only continues to grow.