THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

LEGISLATIVE AND REGULATORY TASK FORCE REPORT

Barriers to Information Sharing

September 2003

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

1.0 INTRODUCTION AND CHARGE 1

1.1 Background 2
1.2 Approach 2
1.3 Scope of Study 2

2.0 CRITICAL INFRASTRUCTURE INFORMATION SHARING 3

2.1 Categories of Critical Infrastructure Protection Information 3
2.2 Current Baseline for Information Sharing 3
2.3 The DHS' Role in Handling CIP Information 5
2.4 The Evolving Information Sharing Environment 6

3.0 THE CRITICAL INFRASTRUCTURE INFORMATION ACT 7

3.1 Background 7
3.2 CII Act Conclusions 8
3.3 Business Concerns with CII Act 10
3.4 Interface with the Government 11
3.5 Draft Regulations for Handling CII 12
3.6 Summary of Comments in CII NPRM Proceeding 13

4.0 CONCLUSIONS 14

5.0 RECOMMENDATIONS 15

APPENDIX A: TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

EXECUTIVE SUMMARY

The private sector owns and operates more than 80 percent of the Nation's critical infrastructures.[1] To protect these key physical and cyber systems, the Government relies on the private sector for information about network vulnerabilities and threats. However, there may be barriers that hinder the private sector from sharing critical infrastructure information (CII) with the Government. The telecommunications and information technology sector, for example, has expressed concern that shared CII might be disclosed under *The Freedom of Information Act* (FOIA)[2]; that industry might be exposed to civil tort or contract liability for sharing such information in good faith; and that industry could face antitrust violations for sharing infrastructure information with other industry partners.

The Homeland Security Act of 2002's Critical Infrastructure Information Act,[3] Sections 211-215, 221, and 222, provides additional FOIA and liability protections to the private sector for sharing critical infrastructure information. Despite these new statutory protections, however, questions remain about whether the CII Act's provisions are strong enough to encourage information sharing between industry and the Federal Government.

The President's National Security Telecommunications Advisory Committee's (NSTAC) Legislative and Regulatory Task Force (LRTF) was tasked with analyzing the information-sharing environment since enactment of the CII Act to determine whether barriers to information sharing still exist between industry and the Federal Government. During its deliberations, the LRTF examined the CII Act. The LRTF then made a series of recommendations for improving the exchange of CII between industry and the Government and protecting CII that is voluntarily provided to the Government by critical infrastructure owners and operators.

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, and other existing authority, direct the appropriate departments and agencies, in coordination with industry, to:

- Develop a process to resolve multi-jurisdictional (Federal, State, and local) conflicts within the appropriate boundaries of federalism and national, homeland, and economic security.

- Work with Congress to modify the CII Act so that the Department of Homeland Security (DHS) is the clearinghouse and dispenser of CII information.

---

[1] General Accounting Office Report: *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, May 8, 2003.

[2] Codified at 5 USC §552.

[3] President George W. Bush signed *The Homeland Security Act* into law on November 25, 2002 (Public Law No. 107-296).

- Encourage Congress to extend the protections of the CII Act to cover departments and agencies other than the DHS and, if other agencies should be designated as such, the NSTAC recommends that they adopt the same rules and procedures as DHS for handling CII.

- Work diligently with Congress to ensure the CII Act's FOIA exemption and liability provisions remain intact.

1.0 INTRODUCTION AND CHARGE

The private sector has been reluctant to share critical infrastructure information (CII) with the Government because until recently, there were no assurances that voluntarily submitting such proprietary data to the Government would protect this information from misuse or public disclosure. Also, concerns about possible prosecution under antitrust law have discouraged some companies from fully participating in Information Sharing and Analysis Centers (ISACs), which help develop cooperative infrastructure security strategies.

The President's National Security Telecommunications Advisory Committee (NSTAC) has analyzed information-sharing issues for several cycles and advised the President that a law be enacted exempting shared critical infrastructure data from disclosure under the Freedom of Information Act (FOIA) and antitrust law, and to provide individual and aggregate disclosures with liability relief. Many of the NSTAC's FOIA recommendations were realized when President George W. Bush signed *The Homeland Security Act of 2002* into law on November 25, 2002.

In addition to establishing the Department of Homeland Security (DHS), the legislation included a provision to exempt CII from FOIA requests when the data is voluntarily shared with the DHS. Because the law covers information that is not normally in the public domain, preventing public disclosure promotes national security and homeland security by allowing the private sector and the Government to conduct better analyses of CII in order to prevent, detect, issue alerts, and respond to threats, attacks, and outages.

The telecommunications and information technology (IT) sectors' processes for sharing information among industry partners and with the Government are highly effective. The CII Act and the implementing regulations will be important for determining how the DHS information sharing mechanism will operate and, thus, help shape the future of information sharing between critical infrastructure operators and the DHS. It is important, therefore, to limit any ambiguities in the implementing rules so that a solid and trusted process can be established and to develop formal procedures that adequately safeguard the handling of CII that is voluntarily shared with the Government.

The implementation of safe and secure implementing policies and mechanisms under the CII Act would create a national model that other industries and Federal departments could emulate. This model could also be inclusive of State and local efforts and serve to rationalize and minimize the number of requests that industry receives for such information. In addition to facilitating industry/Government information sharing, this stands to have a positive effect on Federal interagency sharing.

1.1 Background

Discussion at the President's NSTAC XXVI Executive Session addressed the need for the NSTAC to continue its examination of the various barriers to, and the underpinnings of, information sharing.

During the NSTAC's Industry Executive Subcommittee's December 2, 2002, meeting, the Honorable Richard A. Clarke, then Special Advisor to the President for Cyberspace Security and Chairman of the Critical Infrastructure Protection (CIP) Board, requested that the NSTAC's LRTF undertake a review of the policy landscape in light of the CII Act's FOIA provisions. The goal of such a review would be to identify any remaining legal barriers to voluntary information exchanges from industry to the Government.

1.2 Approach

The LRTF members, subject matter experts from their respective companies, and Government participants contributed to this effort. Appendix A provides a list of task force members, Government personnel, and other participants. Also, to assist the task force in evaluating the information-sharing environment, the members developed an analytical tool mapping types of critical infrastructure information (e.g., outage information, threats, software problems) with potential types of barriers (FOIA, liability, anti-trust, and indirect impediments) for national security and homeland security purposes.

1.3 Scope of Study

The LRTF's jurisdiction in this tasking was to analyze the information-sharing environment, including the relevant provisions of the CII Act to determine whether barriers to information sharing still exist. The LRTF has comprehensively addressed these issues. In addition, the task force makes a series of recommendations to improve the exchange of CII between industry and the Government and to better protect CII that industry voluntarily provides to the Government. This report does not serve as the NSTAC's comment on the DHS Notice of Proposed Rulemaking (NPRM), *Procedures for Handling Critical Infrastructure Information*; however, the NSTAC acknowledges that this report was written during the NPRM comment period. To the extent to which points in the report are germane, the NSTAC hopes the DHS will consider that information when issuing its final rule.

2.0 CRITICAL INFRASTRUCTURE INFORMATION SHARING

2.1 Categories of Critical Infrastructure Protection Information

Two major categories of CII pertain to national security and emergency preparedness (NS/EP) matters: "Non-emergency CIP information" and "Emergency CIP information." Non-emergency CIP information, which is the more prevalent type, is generally used for planning purposes, such as threat assessments, risk analysis, mitigation planning, response and recovery planning, post-event studies, and program development. Examples of non-emergency CIP information that can be shared include infrastructure maps, locations of network assets, circuit routing information, logical routing algorithms, response and recovery strategies, physical and logical security practices, personnel contact information, unmitigated vulnerabilities, potential threats, risk analysis, post-event statistics, and lessons learned.

Emergency CIP information typically involves real-time operational type issues such as informing of imminent threats, informing of an event in progress, requesting corroboration, seeking assistance, suggesting or requesting that action be taken by others, and coordinating response and recovery. Emergency CIP information that may be shared in those instances includes all of the non-emergency CIP information examples (i.e., asset inventory data, event analysis), except for post-event analysis and lessons learned.

2.2 Current Baseline for Information Sharing

The telecommunications and IT sectors have shared emergency CIP information with the Government for years through various channels. IT companies, for example, can use systems such as the Distributed Intrusion Detection System (DShield), which is an open and free online service that provides an automated platform through which firewall users can share intrusion information and receive intrusion alerts and updates. IT companies can also use the North American Network (NANOG), which provides a forum for the exchange of technical information and promotes collaborative discussions among network entities, which can promote the stability of interconnected network services.

Additionally, the DHS National Communications System (NCS) is currently implementing the developmental Global Early Warning Information System (GEWIS), which is intended to be a global Internet health monitoring system and analysis function. GEWIS capabilities will seek to acquire data, analyze it, and potentially create actionable early warning information for dissemination to both industry and Government entities responsible for protecting critical infrastructure. ISACs also provide a coordinated and trusted mechanism for various industry sectors and the Government to exchange information.

The telecommunications sector's information sharing processes are effective. Data is exchanged between and among industry and the Government related to cyber incidents, physical vulnerabilities, and other emergency situations involving the telecommunications and cyber

infrastructures. In 1991, the NSTAC, working with the NCS, recommended establishing an industry/Government partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The Network Security Information Exchange (NSIE) process was established as a forum where industry and the Government could share information in a trusted and confidential environment. The NSIE process continues to function, demonstrating that industry and the Government will share sensitive security information if they find value in doing so. In 1998, Presidential Decision Directive 63 (PDD-63), *Protecting America's Critical Infrastructures*, called for the establishment of similar information exchange forums to reduce vulnerabilities in all critical infrastructures.

Since March 2000, the NCS' National Coordinating Center for Telecommunications (NCC) has served as the Telecommunications ISAC, which facilitates voluntary collaboration and information sharing among industry and the Government. Telecom ISAC participants daily gather emergency CIP-type information on vulnerabilities, threats, intrusions, and anomalies from the telecommunications industry, the Government, and other sources. The information is then analyzed with the goal of averting or mitigating impacts on the telecommunications infrastructure. The results are then sanitized and disseminated in accordance with sharing agreements established by the ISAC participants.

When responding to requests for critical infrastructure data, the NCC asks the inquiring organizations several questions to determine the appropriateness of their requests. These questions help establish the basis for the NCC's approach to information sharing. Some questions pertain to the type of information being requested, including:

1. What is the problem at issue?
2. Is the information vital to maintaining national/economic security? How?
3. Is specific information being requested? How will the receipt of this information solve the problem identified in Number 1?
4. What is the purpose for which the information will be used?
5. Has this information been requested from other organizations? What are the names of these organizations? What was the result?
6. Are there alternate methods that may be used to solve this problem?

The NCC also asks a series of questions related to how the information will be handled, including:

1. Who will be responsible for safeguarding this information?
2. How will it be protected?
3. Who will have access to this information inside/outside the organization?
4. Where will this information be stored?

The NCS transferred from the Department of Defense (DoD) to the DHS on March 1, 2003, and, as a result, the NCC/Telecom ISAC also became part of the DHS. The NCC is currently merging some of its capabilities with those of the other entities in the DHS' Information Analysis and Infrastructure Protection (IAIP) Directorate to meet IAIP's overall mission of assessing the vulnerabilities of the Nation's critical infrastructures, evaluating those

vulnerabilities, and coordinating a response with other Federal, State, local, and private entities. The NCC/Telecom ISAC is an information-sharing model that supports the Nation's NS/EP requirements. The sharing of non-emergency CIP information, which is a primary DHS objective, can be included in this model. The NCC's coordinated information sharing mechanism has been subsumed by the DHS, but the Department has not yet established its processes for sharing non-emergency or emergency CIP information.

2.3 The DHS' Role in Handling CIP Information

Effective sharing of CII will be dependent upon the establishment of formal procedures for handling CII that take into account the unique nature of the critical infrastructure sectors and foster a trusted environment for exchanging such data.

The Federal Government has identified 14 critical infrastructure sectors. Eight infrastructures were designated in PDD-63 based on the recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP): telecommunications and IT, banking and finance, electric power systems, gas and oil storage, transportation, water supply systems, emergency services, and continuity of Government. *The National Strategy for Homeland Security* designated six others: agriculture, food, public health, defense industrial base, chemical industry, and postal and shipping.

Although these infrastructures have some commonalities, they differ in terms of function, structure, culture, degrees of interconnection, degrees of interdependence, relationships with the Government, types of shared information, and the criticality of the timeliness of shared information. Accordingly, there is significant diversity among the ISACs. For example, the telecommunications, electric power, IT, and banking and finance ISACs have been in existence for a considerable period of time. Although they are organized and operate differently, they have been functioning efficiently and are effectively sharing information with the Government. Other ISACs, such as gas and oil storage transportation/surface, and water supply systems, are newer and are operating at various stages of implementation. And some ISACs are still in the planning stage, including the defense industrial base and the chemical industry ISACs.

The economic security–national security linkage of all infrastructures is unquestioned, but it is important to recognize the unique roles for telecommunications and IT networks in providing the fabric of relationships among most other institutions. In 1997, the PCCIP cited electric power and telecommunications as keystone technologies on which each sector is dependent. Since then, however, there has been a dramatic increase in the reliance of each sector on telecommunications among its members, between its members and vendor and customer communities, and between itself and Governmental entities at every level. Accordingly, the organizations that serve these different infrastructure communities have divergent views on the sensitivity of their exchanges of information among their members, with the media and public, and with the Government.

Because of the myriad of differences among infrastructure sectors, it should be apparent that "one size does not fit all" for ISAC operations and the processes for sharing information with the Government. Thus, if the DHS is going to establish effective procedures for handling CII, these procedures should be established on an infrastructure-by-infrastructure basis. The Federal Government should also establish individual partnerships with each sector to better tailor their processes to each sector.

2.4 The Evolving Information Sharing Environment

The information-sharing environment has grown more complex in recent years, as the various information-sharing stakeholders have created new mandates that affect the custodians of sensitive data. The Federal Government has enacted various regulatory requirements, including the "Gramm-Leach-Bliley Act," which affects security and privacy in financial services; *The Health Insurance Portability and Accountability Act*, affecting security and confidentiality of patient information; and the "Sarbanes-Oxley Act," affecting corporate governance compliance reporting integrity.

State and local jurisdictions have also responded to growing concerns over terrorism, fraud, identity theft, and other emerging threats with frequent, independent requests to critical infrastructure providers for structural and operational information. These requests are seldom coordinated or consistent. They can result in duplicative requests for essentially similar information, at different times, in different formats. California, for example, has enacted legislation that requires notification of affected persons whenever the holder of privacy information discovers that it may have been inappropriately released or accessed. Further, a bill has been introduced in the U.S. Senate that is modeled on this California law[1] and would extend similar requirements across the Nation.

The net effect of this increasing demand for information — coupled with the increased importance placed on the information, the potential for increasingly negative implications if it is misunderstood or misused out of context, and the increasing costs for open-ended compliance — has forced many companies to be even more cautious about sharing. As a result, some companies have been adhering closely to the letter of mandatory disclosure requirements and tightening up other, informal channels that have been used for years. The President, therefore, should direct the DHS to develop a process to resolve multi-jurisdictional (Federal, State, and local) conflicts within the appropriate boundaries of Federalism and national, homeland, and economic security.

In addition, ambiguity exists as to the interrelationship between the Federal Government and State regulators' ability to seek data from the industries they regulate. Indeed, a growing number of reports recount how CII owners and operators have received demands from their State regulators for disclosure of all of the DHS submissions. To avoid duplicative and conflicting CII requests, the President should work with the Congress to modify the CII Act so that the DHS is the clearinghouse and sole dispenser for CII Information.

[1] California Security Breach Notification Bill SB 1386, 2002 Leg. 2001-2002 session (Ral. 2002)

With the DHS as the clearinghouse, once CII is submitted to the Department, critical infrastructure owners and operators would not have to submit the same information to other areas of Federal, State, or local government. Instead, acting as the primary CII repository, the DHS would be the sole dispenser of CII information and would work with States and localities to fulfill their CII inquiries.

3.0 THE CRITICAL INFRASTRUCTURE INFORMATION ACT

3.1 Background

The CII Act has its origins conceptually in *The Year 2000 Information Readiness and Disclosure Act,*[2] which was designed to encourage a process through which industry in good faith could share data about potential year 2000 (Y2K) problems with the Government. The Y2K legislation was the model on which elements of the Congressional progenitors of the CII Act—commonly referred to as the "Davis-Moran" and "Bennett-Kyl" bills—were based.[3]

The purpose of the Y2K legislation was to encourage reticent custodians of critical infrastructure assets to provide the Government with timely information regarding Y2K computer date vulnerabilities and to provide opportunities for remediation of these system problems. A key element of this incentive was a limited exclusion from exposure to a FOIA release for qualifying data submissions. But, just as with the Y2K legislation, which spawned a specific further Congressional action to relieve industry informants of civil liability for failure to remediate Y2K problems, some infrastructure custodians today are seeking more than a privilege of private disclosure of sensitive information to the Government, believing that civil liability immunity is appropriate to incent full disclosure.

The CII Act provides additional protections to the private sector for sharing critical infrastructure information with the Government. The CII Act exempts information voluntarily submitted to the DHS from disclosure under FOIA; provides a general limitation on the use of the information for critical infrastructure protection purposes; includes liability protections by limiting use of the information in civil actions; and limits use of the information by State and local governments.

Specifically, the Act states that, "critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement:"

- Shall be exempt from disclosure under FOIA;

---

[2] 15 USC §1(note), 105 Stat. 271, 1998.

[3] Cyber Security Information Act of 2001, "Davis-Moran," H.R. 2435; see also Critical Infrastructure Information Security Act of 2001, "Bennett-Kyl," S. 1456.

- Shall not be subject to any agency rules or judicial doctrine regarding *ex parte* communications with a decision-making official;
- Shall not be directly used in any civil action arising under Federal or State law if such information is submitted in good faith;
- Shall not be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except in furtherance of an investigation or the prosecution of a criminal act or when disclosure of the information would be either to Congress or to the Comptroller General; and
- Shall not, if provided to a State or local Government or Government agency be made available pursuant to any State or local law requiring disclosure of information or records, otherwise be disclosed or distributed to any party by said State or local Government or Government agency, or be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.[4]

The Act also includes definitions of key terms, which better delimit its scope. The Act defines protected "critical infrastructure information" as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems." However, protection from FOIA requests applies only when that information is submitted to a "covered" Federal agency; a term that the Act applies only to the DHS. Also, when information is submitted, the Act states that a written "express statement" indicating that the information should be protected by the CII Act must accompany it. Specifically defined provisions, such as those included in the CII Act, will reduce the possibility of the Act's provisions being open to interpretation, which would create a risk that could hinder information sharing. Its broad scope will also help encourage information sharing by providing wide-ranging protections for shared information.

Over the past several years, the NSTAC has discussed elements that would be necessary for effective information sharing legislation. The LRTF has used its previous work as a baseline for analyzing the new protections in the CII Act. The LRTF has reviewed the CII Act and has made several observations about what the Act provides and what protections may still be necessary to facilitate information sharing. Its observations and conclusions regarding the effectiveness of the Act's provisions are included in this report.

3.2 CII Act Conclusions

After analyzing the CII Act's FOIA protections, the LRTF concludes that it is sufficient to protect CII that is voluntarily shared with the DHS from disclosure as long as the CII Act's provisions remain intact. Therefore, it is vital that the CII FOIA protections remain in place.

Legislation introduced in the 108th Congress would undo some of the CII Act's provisions, including the FOIA protection. Through this legislation, some members of Congress have expressed concern that the CII Act shields companies from lawsuits to compel disclosure, criminalizes otherwise legitimate whistleblower activity by the DHS employees, and preempts

[4] Language extracted and/or summarized from the CII Act, Section 214.

any State or local disclosure laws. A key objective of the legislation is to prevent companies from using the current FOIA exemption as a loophole to shelve CII in the DHS that they do not want made public. Several civil liberties groups support the introduced legislation, while various industry groups such as the Information Technology Association of America have opposed it.

The LRTF concluded that the notion that the CII Act might deter "whistleblowers" who become aware of unflattering information regarding threats, attacks, or vulnerabilities fails on several counts. First, industry whistleblowers are not in any way subject to the CII Act's provisions; and any disclosures made by, for example, an employee of a hacked bank would be a matter of civil liability between the bank and its employee unless customer data was involved that could implicate financial regulatory agencies. Moreover, Government whistleblowers would not be prevented by any provision of the CII Act or presumably the DHS implementing regulations (which, in Section 29.8[f], specifically addresses disclosure to the Inspector General) from making a disclosure of possible unlawful activity to the Inspector General, or, presumably, pursuant to the general obligation of Federal employees, to an appropriate official of the Department of Justice.

The task force reviewed the introduced legislation and concluded that it would pare down the CII Act's key information sharing provisions. The bill would essentially remove the FOIA and civil liability immunity exemptions from the CII Act for all critical infrastructures and thus stifle any information-sharing progress that has been made since its passage. Further, the task force believes that enactment of such legislation would discourage information sharing and introduce additional impediments. The President, therefore, should work diligently with the Congress to ensure that the CII Act's provisions remain intact.

The LRTF also examined the civil liability protections in the CII Act, which protects the submitter from liability and prohibits the direct use of voluntarily submitted CII against the submitting party in civil actions by any Federal, State, or local authority, or any third party. These liability protections, while laudatory, are not comprehensive. There are concerns that because the CII Act is a new statute, it has not been subject to judicial interpretation; and no case law precedent exists to determine how effective this provision will be at limiting liability exposure. Further, the liability protection applies only to information that is shared "in good faith"; this clause may be open to legal interpretation and create a liability risk.

The Act is also unclear about whether the statute supersedes State law governing breach of contracts. However, the clear public interest considerations for infrastructure protection should take precedence over any allegations of breach of contract, and the judicial concept of "void as against public policy" should serve to mitigate any State contract liability concerns. Perceived liability is also a barrier to sharing information. Because of these additional liability concerns, the LRTF concludes that some information sharing barriers may still exist. Implementation of the Act will not result in an unfettered release of CII to the Government, and legislation alone will not fully address all challenges for information sharing.

3.3 Business Concerns with CII Act

The CII Act is an important part of a strong and dynamic public private partnership. It is necessary for business and the Government to have clear and unambiguous procedures in place that highlight how information shared with the Federal Government will be managed. However, the simple existence of those procedures is not a universal remedy for facilitating information sharing.

Private businesses must strike a balance between doing what is good for the Nation and protecting their primary business interests—meeting the needs of their customers, protecting the interests of their shareholders and investors, and enhancing their corporate value. While much of industry believes that sharing information is likely to help protect the critical infrastructure, there has been no clear determination that the value of information sharing will be greater than the costs and risks to industry.

The process of providing information to the Government (e.g., collecting data, indexing it, and updating it) can prove costly for companies. To encourage information sharing, it must be clear for companies that the benefits of providing this information outweigh the costs. In addition, current corporate culture dictates that companies protect their corporate data, especially if sharing it could potentially harm the company in any way. Within corporations, employees have been inculcated to protect valuable corporate confidential information, and cultures are difficult to change. Also, companies may even be less likely to share information because information sharing for CIP has recently received so much public attention. Indirect information sharing impediments exist because companies fear information sharing could potentially lessen the company's value proposition for its customers or lessen goodwill if the company is harmed by the shared information. For successful information sharing to occur, a major shift in corporate thinking will be necessary, which will likely be possible only with a clear determination of the business case for sharing information.

One significant business concern is the issue of outsourcing. For example, if a company has data from a third party and has entered into a non-disclosure agreement, the company cannot share the data. As the trend to outsource increases, this becomes a barrier to information sharing. Infrastructure interdependencies also play a role in the information-sharing environment. As telecommunications services are outsourced, critical infrastructure data may not be releasable, which could affect other infrastructures that rely on those outsourced services.

Industry would be more willing to share information and participate in ISACs if four key notions were proven:

1. That centralized analysis of data from multiple sources will provide indicators of impending threats or current attacks that any individual contributor of the information could not have ascertained by working independently with access to only its own data;

2. That alerts and warnings resulting from centralized analysis of information from multiple sources will be of value to the contributors of the information;

3. That the value derived from participation in the information sharing process will return sufficient value to the participants to outweigh the risks inherent in sharing proprietary corporate information and the costs of doing so; and

4. That there is a single trusted place in which information can be shared, maintained, and protected, and that the shared information will only be used for critical infrastructure security purposes.

3.4 Interface with the Government

The Government should establish a centralized source at the Federal level to process information requests and collect information under the protections of the CII Act. This centralized source should establish a set of criteria to determine whether the information requests are "legitimate" and should have the ability to reject or modify any requests. Draft regulations currently being developed by the DHS would make the DHS the single point of contact for Federal agencies. If other agencies should be designated as covered agencies, the NSTAC recommends that they adopt the same rules and procedures as the DHS.

The NSTAC recognizes the Government is still working to clarify the purpose, scope, and breadth of information sought from industry in order to protect critical infrastructure. Industry, nonetheless, is still concerned about the vast amount of information that State and local authorities are requesting in developing State security plans. In many instances, the same information is available from the DHS' NCS. Under the CII Act and the DHS protection, critical asset information or infrastructure data is more easily protected, controlled, and secured. Duplicative and inconsistent databases with differing security controls and requirements create an embedded security risk to the Nation's infrastructure. Therefore, the Government should develop a coordinated mechanism for the control, protection, and dissemination of critical information. This approach will give industry confidence that the information is needed for critical purposes and prevent the inappropriate release of CII.

The Government also has not proven that its receipt of vast amounts of data will enable it to directly protect physical and cyber assets owned and operated by a myriad of companies across the Nation and around the world. Although it is important for the Federal Government to be a partner in security with industry, if the Government elects to play a direct role, it should take a business approach to sharing information and establish a logical strategy for how the information will be gathered and used to better protect industry owners and operators of critical infrastructures. The Government must convey that information sharing is either so important for the country or so good for companies (or both) to change the current corporate culture. The NSTAC understands the Government is still working out the information sharing responsibilities among the DHS, DoD, and other Cabinet-level agencies and may eventually review that interface. In a letter to the President,[5] the NSTAC has relayed its concerns about interagency information sharing.

[5] NSTAC letter to President George W. Bush, September 2003.

The Government can also reduce perceived risk and encourage information sharing by establishing a strategy for how it will use the information and disseminate it in the form of warnings, etc. As previously noted in this report, the NCC asks several very specific questions of organizations making requests for information. The NSTAC suggests that the DHS use similar questions when it receives requests for information to better solidify the process and reduce the perceived possibility that information may be disclosed improperly.

Also, questions remain about whether information sharing is considered a "two-way street." Some in industry believe that the Government should provide industry with more timely threat data to help demonstrate the value of information sharing and the need to protect the infrastructure that it operates. However, the most effective solution will be for the Government to embrace its role as a "partner" in the public–private partnership between the Government and infrastructure owners and operators.

3.5 Draft Regulations for Handling CII

The new FOIA and liability protections will play an important role in providing certainty that CII will be secure once it is shared. The DHS' regulations implementing the CII Act will also be important for determining exactly how the DHS' information sharing mechanism will operate and how the FOIA and liability protections will be implemented. However, the new FOIA and liability protections will not necessarily guarantee that information will be shared. The LRTF recognizes that non-legal impediments for information sharing also exist, such as judicial gag orders and non-disclosure agreements, as well as significant business-related concerns.

The CII Act directs the DHS to establish implementing procedures for the "receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government."[6] These procedures apply to all Federal agencies that receive, care for, or store CII voluntarily submitted to the Federal Government pursuant to the CII Act, including Government contractors, foreign, State, and local Governments, and government authorities, pursuant to their express agreements.[7]

The LRTF has analyzed the current DHS NPRM, *Procedures for Handling Critical Infrastructure Information*,[8] which implements the provisions above. The NPRM includes rules for protecting CII from disclosure under FOIA and from liability as directed in the CII Act. It also proposes procedures for the DHS to follow when handling CII. The NPRM states that the Secretary of the DHS will designate the Under Secretary of the IAIP Directorate "as the senior DHS official responsible for the direction and administration of the Critical Infrastructure Information Program."[9] The IAIP Under Secretary will then appoint a CII Program Manager within the Directorate to direct and administer the CII program. The Program Manager will be the primary point of contact and decision maker on which information is protected under the CII

[6] CII Act, Section 214 (e).

[7] Language extracted and summarized from the CII Act, Section 214 (e).

[8] *Federal Register*, April 15, 2003, Vol. 68, No. 72, p.18523–18529.

[9] DHS NPRM: *Procedures for Handling Critical Infrastructure Information.*

Act. The Program Manager is authorized to designate CII as protected information, and the information will retain its protected status unless the CII program manager renders a final decision that the information is not protected CII.

The NPRM stipulates that CII will be designated as protected only if it is submitted to the IAIP Directorate either directly or indirectly via another Federal agency, which on receipt of the CII will forward it to the DHS. The information must be intended for CIP use, and an express statement must be included that the information is submitted with the expectation that it will be deemed CII protected. Other Federal agencies cannot deem information CII protected. If information is submitted to another agency with this intent, the other agency must forward it to the CII Program Manager.

The NPRM also provides for the CII Program Manager to acknowledge the receipt of the information and determine if the information will be protected. It is the Program Manager's responsibility to notify the submitter if the information is not to be protected, and the submitting party can then further explain why the information should be protected, decide if the information should be used, or request that it be destroyed. The Program Manager can destroy the information unless the Program Manager determines that there is a need to retain it for law enforcement and/or national security reasons. If the CII Program Manager determines that any information is not submitted in good faith in accordance with the CII Act, the Program Manager is not required to notify the submitter that the information does not qualify as protected CII.

Protected CII may be made available to a State or local government entity only pursuant to an "express agreement" with the Program Manager that acknowledges the understanding and responsibilities of the recipient. State and local governments may not further disclose the CII protected information unless the Program Manager obtains written consent from the submitter to disclose the information beyond the CII Act's limitations.[10]

The CII Act's implementing regulations will be important for determining how the DHS information sharing mechanism will operate. It is important to limit any ambiguities in the rules so that a solid and trusted process can be established. A few ambiguities do exist, however. For example, the DHS may need to better define the term "express statement" so that submitters will know exactly how to mark their information for CII protection. "Express agreements" may also need to be better defined to ensure that information is protected when it is shared between Government entities. The deadline to submit comments on this NPRM was June 16, 2003. The LRTF will continue to monitor the process of the rules as they become final.

3.6 Summary of Comments in CII NPRM Proceeding

Dozens of parties filed comments in the proceeding, including power companies, public interests groups, water companies, and telecommunications and IT interests. Telecommunications and IT companies were generally supportive of the proposed CII rules but sought additional protections

[10] Language extracted and summarized from the DHS NPRM: *Procedures for Handling Critical Infrastructure Information*.

for the receipt and use of CII, including assurances that the DHS would not disseminate CII to foreign governments without adequate safeguards in place.

The proposed rules allow for CII to be shared with foreign governments, but several telecommunications and IT interests questioned whether the Homeland Security Act of 2002 authorized the DHS to exchange CII information with foreign governments. If indeed the DHS has the requisite authority to provide CII to a foreign government, telecommunications interests suggested that the Secretary of the DHS or a senior level designate within the Secretary's Office be the interface for the decision to make CII available and for the information exchange. And if a submitter's information is going to be exchanged with a foreign government, several companies suggested that the rules be modified to provide advance notice to the submitter and to give the submitter a chance to review that information to ensure that no confidential information is being released. Absent such a change to the proposed rules, permission for the DHS to share CI with foreign governments could pose another business restraint on full sharing with the DHS by U.S. companies.

Some telecommunications companies also recommended ways to improve the rules so they provide more incentives for companies to voluntarily share CII with the Federal Government. However, they also noted that while exempting CII from public disclosure under FOIA is an important step towards creating a trusted environment with which to share information with the Federal Government, that action does not represent a complete elimination of all barriers to information sharing.

Telecommunications carriers and IT interests also addressed the process for determining whether information is to be considered CII and thus qualifies for protection. Many carriers said the information should be returned to the submitter if it is deemed not protected CII, or if it is determined that the information has not been submitted in "good faith." Some also wanted the rules to be modified to give submitting parties a chance to present additional evidence for granting CII protection to a submission. Furthermore, if the CII Program Manager determines that the information is not protected CII but should be retained for law enforcement or national security reasons, several carriers said the information should be treated like CII and therefore exempt from FOIA disclosure.

4.0 CONCLUSIONS

The LRTF recognizes that a great deal of information sharing is occurring between industry and the Government. Because the CII Act and the final DHS information sharing rules will help shape the mechanism for future information sharing, they are critical to building on that success.

After analyzing the CII Act's FOIA protections, the LRTF concludes that the FOIA provision is sufficient to protect CII that is voluntarily shared with the DHS from disclosure as long as the CII Act's provisions remain intact. However, because the DHS is the only covered Federal agency under the Act, there are concerns that critical infrastructure data may be subject to disclosure under FOIA if it is shared with other Federal agencies. Information that is also shared between industry groups or that is unofficially shared, even when a Government representative is physically present in the room, may also be open to disclosure. Therefore, Congress should

consider extending the protections of the CII Act to cover departments and agencies other than the DHS and consider enacting legislation that addresses the need for procedures regarding information sharing with State and local entities.

Because of additional liability concerns, the LRTF concludes that some liability may still exist for disclosing this type of information, despite the CII Act's broad protection in Section 214 of *The Homeland Security Act*. As stated above, the most important component of a successful information sharing program will be a strong trust relationship among all parties in the public–private partnership, both industry and the Government alike.

5.0 RECOMMENDATIONS

NSTAC Recommendations to the President

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* and other existing authority, direct the appropriate departments and agencies, in coordination with industry to:

- Develop a process to resolve multi-jurisdictional (Federal, State, and local) conflicts within the appropriate boundaries of Federalism and national, homeland, and economic security.

- Work with Congress to modify the CII Act so that the DHS is the clearinghouse and sole dispenser of CII information.

- Encourage Congress to extend the protections of the CII Act to cover departments and agencies other than the DHS and, if other agencies should be designated as such, the NSTAC recommends that they adopt the same rules and procedures as the DHS for handling CII.

- Work diligently with Congress to ensure the CII Act's provisions remain intact.

APPENDIX A

TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Telcordia Technologies	Ms. Louise Tucker, Chair
Lockheed Martin	Mr. Gerald Harvey, Vice Chair
AT&T	Mr. Harry Underhill
Bank of America	Mr. Roger Callahan
BellSouth	Mr. David Barron
Boeing	Mr. Robert Steele
CSC	Mr. Guy Copeland
Lucent Technologies	Mr. Clyde McFarland
MCI	Ms. Cristin Flynn
Microsoft	Mr. Bill Guidera
Nortel Networks	Mr. Raymond Strassburger
Qwest Communications	Mr. Jon Lofstedt
Raytheon	Mr. David Fowler
Rockwell Collins	Mr. Ken Kato
SBC Communications	Ms. Rosemary Leffler
Sprint	Mr. Michael Fingerhut
VeriSign	Mr. Michael Aisenberg
Verizon Communications	Ms. Ernie Gormsen

OTHER PARTICIPANTS

Bank of America	Mr. John Huffstutler
BellSouth	Mr. Lloyd Nault
CSC	Mr. Daryl Savage
George Washington University	Dr. Jack Oslund
Lockheed Martin	Mr. Larry Duncan
Microsoft	Mr. Phillip Reitinger
SBC	Mr. Jonathan Boynton
Sprint	Mr. John Stogoski
USTA	Mr. David Kanupke
Verizon	Mr. Lowell Thomas

GOVERNMENT PARTICIPANTS

DISA Counsel	LtCol Keith Alich
DOJ	Mr. Scott Eltrington
OMNCS Counsel	Ms. Hilary Morgan