LEGAL IMPEDIMENTS TO INFORMATION SHARING

A "LEGAL FOUNDATIONS" STUDY

Report 10 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Contents

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the

possible approaches and conclusions that were presented to the PCCIP for its consideration. The series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Part One

Introduction

Data collection and information sharing are likely to play a key role in the protecting of our nation's critical infrastructures, whether it is to involve data and information originally compiled by government or by the private sector. The development of data collection and sharing capabilities between government (Federal, state and local) and the private sector can contribute, for example, to an effective threat and warning capability.

In attempting to forecast potential legal impediments to the broad sharing of information for the purpose of assuring the critical infrastructures, existing information-sharing activities and the legal issues implicated by them were studied.

The *Legal Foundations* study *Information-Sharing Models* is the companion volume to the *Legal Foundations* study *Legal Impediments to Information Sharing*. The two documents should be studied together to fully understand the issue of information sharing. *Information-Sharing Models* details the current approaches to information sharing and sets the stage for further understanding the concepts described in *Legal Impediments to Information Sharing*.

Research Issues

- What potential legal impediments (Federal or state statutes, regulations, or common law causes of action) could inhibit the flow of infrastructure assurance-related information between and among government bodies and the private sector?

- In light of these impediments, are there specific courses of action that could improve the information-sharing climate?

- How can an information-sharing mechanism best be structured to avoid these legal impediments?

Research Findings

Upon reviewing various Federal and state statutes, the following research findings were noted:

- Information collection, dissemination, and protection each implicate discrete legal issues, and hence pose potential legal impediments to information sharing. Relevant legal issues include, among others, antitrust, liability, national security concerns, and privacy.
- These impediments are generally manageable when they arise in conjunction with private sector-to-private sector or government-to-government transactions.
- These impediments are less manageable with respect to "mixed" transactions, i.e., government-to-private or private-to-government information collection, dissemination, and protection.
- An understanding of the legal issues implicated by these transactions is relevant, if not central, to the design and embodiment of an effective information-sharing capability.
- An appreciation for these legal issues can be gained through the study of existing information-sharing mechanisms, and models that can be abstracted from them.

Assumptions

This paper assumes that a successful information-sharing mechanism or mechanisms will contribute to infrastructure assurance.

Impediments to Information Sharing

Current data collection and information-sharing activities are underway in a number of sectors. These efforts range from informal discussions of industry executives about an emerging problem to statutorily required collections and mandated dissemination. Our study of these existing activities and mechanisms further suggested five theoretical models for information sharing.

(For further information on the individual models, *See Information Sharing Models*, a special study of the *Legal Foundations* series.) These models include:

1. Information Clearinghouse
2. Advisory Committee/Commission
3. Mandatory Provision of Information with Limited Exchange
4. Voluntary Cooperation or Exchange of Information
5. Threat and Hazard Detection and Notification

The models differ in terms of the degree of formality, the legal requirements relating to reporting and dissemination, and degrees of public and private participation. The attributes of a particular model may subject it to further legal impediments to information flow making some models more advantageous than others to achieve infrastructure assurance objectives.

The study of these models has revealed a series of legal issues that arise under each of these models to varying degrees. Antitrust, liability, national security, proprietary data and privacy concerns are potentially implicated no matter which option is employed. These issues may impede the sharing of information in the following ways:

- **Antitrust:** Federal antitrust and anti-competitive behavior statutes, and their state level counterparts are primarily intended to prevent price-fixing and market-splitting. Although many activities conducted by private companies to share information relating to critical infrastructure protection should not implicate antitrust concerns, many companies have raised antitrust as a potential "show-stopper" in information-sharing efforts.

- **Liability for Failure to Disclose or Inform:** Liability for failure to disclose information that could have prevented a critical infrastructure-related incident is a concern for government and private parties. Unless adequately addressed, concern over this form of liability may discourage robust collection of information, or may militate in favor of cautious dissemination among a narrow and well-defined field of participants.

    - **Federal Government:** The Federal government can make itself subject to suit under the Federal Tort Claims Act. The statute can permit recovery if the government negligently or intentionally withholds information that could have prevented a loss. There is an exception to this liability that would apply when a Federal employee was acting with due care in the execution of a statute or regulation. Some information-sharing statutes and executive orders are explicit that they do not create a right of action for failure to receive information.

    - **Private Parties:** To hold a private party liable for failure to provide information that could have prevented a loss, the plaintiff would have to show that the party had a duty-- whether statutory, regulatory, or common law-- to provide the information. This generally requires a relationship between the parties, a relationship that can be

adequately established, (either express or implied), through information-sharing activities or agreements.

- **National Security Concerns:** National security issues relate to the protections that certain classes of information receive by virtue of their relation to national security issues (e.g., intelligence sources) or the concerns that arise in relation to foreign access to sensitive, but not necessarily classified, critical infrastructure information. The government has regulations and specific statutes that punish improper disclosure of classified information. These statutes and regulations are of particular concern as they apply to "foreign persons." Generally, release of information to a foreign person is contingent on an evaluation of their country of origin and a satisfactory inspection of their background.

- **Government Protection of Private Sector Information:** The Federal and state governments operate under rules designed to allow openness and transparency in the democratic process. The most important of the legislation surrounding government disclosure of information is the Freedom of Information Act (FOIA). FOIA, and its state level counterparts, require the government to disclose all information that does not fall into a series of narrowly defined exemptions (e.g., on-going law enforcement investigations). Information disclosed by the private sector does receive some protection from disclosure under FOIA exemption b(4) if that information is either a trade secret or proprietary and voluntarily disclosed. Disclosure of information can also be prevented by independent statutory mechanisms. These may be tied to the mission of the organization collecting the information, to judicial procedures, or specific trade secret protections. However, without specific guarantees of confidentiality, the private sector may be unwilling to share information with government voluntarily.

- **Privacy:** Privacy issues are discussed in a separate paper in the Legal Foundations series: *Privacy Laws and the Employer-Employee Relationship*.

Part Two

Addressing Legal Impediments

Limiting Liability of the Federal Government

A specific statement of the Federal government's duties with respect to disclosure and notification could be included in executive orders or statutes relating to critical infrastructure information sharing in order to limit the liability of the Federal government under the Federal Tort Claims Act. By specifically delineating the government's responsibilities in an information-sharing mechanism, the government can limit its liability. If the legal vehicle by which the mechanism is established states in specific terms the parties with whom the government will share information, parties who are not enumerated will not be able to sue for failure to inform. However, the government will have some liability exposure with regard to the parties it has said that it will inform if it fails to share information due to negligence. The government may also avoid liability by specifically stating in the legal vehicle forming the information-sharing mechanism that it does not create a right of action against the government.

- **Pro:** This approach would allow the government to avoid the need to include *every* critical infrastructure owner and operator specifically in an information-sharing effort because of liability concerns, thus limiting the burden on the information-sharing process. The government could instead specifically decide the level of exposure to which it should be amenable and act accordingly.

- **Con:** The specific delineation of the government's responsibilities may raise opposition of those not included at the table. Eliminating liability concerns in this way may remove the incentive to try to include all interested parties in the information-sharing effort.

Antitrust Opinion From Department of Justice (DOJ) or Federal Trade Commission (FTC)

To respond to perceived antitrust concerns, the Department of Justice Antitrust Division or the Federal Trade Commission (FTC) could consider the propriety of rendering an opinion or providing guidelines clarifying for private industry the standards for communicating critical infrastructure information both through intermediaries and directly. Guidance from one of the agencies directly involved in enforcing antitrust violations as to appropriate processes for sharing information among private sector entities, particularly as it relates to infrastructure assurance issues, may alleviate apprehension of industry about engaging in such activities.

National Security Concerns

As part of its approach to infrastructure assurance, the Federal government will have to address the issue of sharing sensitive information with "foreign corporations" which may be either owned or controlled by non-U.S. citizens. The next two items describe the issues involved.

Developing Government-wide Guidelines for Sharing Sensitive Information with Foreign Corporations

The Federal government needs to study and consider developing comprehensive and centralized guidelines for sharing sensitive information with foreign corporations. Currently, many agencies have individual regulations defining and setting out rules for dealing with "foreign corporations." The definition is usually based on a percentage of foreign ownership. These percentages vary from agency to agency. Under this option, an interagency task force, perhaps under the guidance of the NSC, would study whether a uniform approach to defining who is and who is not a "foreign corporation" would be in the interest of national security and government efficiency. A government-wide study would allow foreign policy and economic implications to be taken into account. If found to be desirable, the body could also study where the proper percentage of foreign ownership for the entire government to share information should be set and whether there are any entities which should be exempt or for which the percentage should differ.

- **Pro:** This approach would bring the issue of foreign ownership to the Administration's and Congress' attention. All agency policies would be reviewed and potentially collapsed into one guideline. It would reduce complexity and uncertainty for foreign investors, and provide the Federal government an opportunity to revisit current regulations in light of critical infrastructure issues.

- **Con:** One set of regulations may not be able to adequately address the needs of all government agencies. Regulations may be too restrictive for some agencies and too lax for others. The study of foreign ownership is likely to be a difficult and controversial process, a process made exceptionally difficult to implement in an environment of rapid restructuring and globalization.

Developing Interim Guidelines for Sharing Information with Foreign Corporations

Notwithstanding resolution of the issue above, the information-sharing mechanism for critical infrastructure assurance should consider studying, and if necessary, setting guidelines for sharing critical infrastructure information with foreign corporations. If the immediately-preceding option is adopted, and uniform Federal guidelines are eventually created, the information-sharing mechanism may need to adopt those guidelines. Until such time, the mechanism should consider the proper way to include corporations with foreign owners in their process. This may result in guidelines that determine the percentage of foreign ownership that is allowed for participating entities to receive information. The guidelines could be specifically tailored by infrastructure or to provide for a sliding scale of ownership percentage according to the sensitivity of the information.

- **Pro:** This approach would allow the rules for sharing information with foreign corporations to be specifically tailored to critical infrastructures.

- **Con:** Current approaches of agencies connected to critical infrastructures will likely remain unchanged. This approach depends on the successful implementation of recommendations for an information-sharing mechanism or follow-on entity to come to fruition.

Government Protection of Private Sector Information

A potentially contentious set of issues having to do with infrastructure assurance relates to the Federal government's protection of private sector information. The next three items discuss the ramifications of different approaches and strategies.

Legal Vehicle to Protect Confidential Information

A legal vehicle could be established within the critical infrastructure information-sharing mechanism that would include specific provisions allowing the protection of confidential information. Under exemption b(3) of FOIA, information protected from disclosure under other statutes are also exempt from public disclosure under FOIA. If the information-sharing mechanism is established by Congressional legislation, a provision protecting information from disclosure would qualify for nondisclosure under exemption b(3). The provision would need to be carefully drawn to allow the information-sharing mechanism to disclose certain types of information or sanitized versions of information and also to meet the requirements for a b(3) statute.

- **Pro:** If a b(3) statute is in place, the private sector participants can be fairly certain that their information will not be disclosed under FOIA or otherwise. If Congress must act to create the information-sharing mechanism, it will be easy to insert the needed language to accomplish this sort of protection for confidential information.

- **Con:** Exemption b(3) requires a statute, thus an executive order will not be able to accomplish the same goal. If the information-sharing mechanism is to be established by executive order, this option will have to be accomplished separately and may not be addressed until well after that mechanism is up and running. The current administration stance on FOIA is very pro-disclosure, even when exemptions are available.

Impact of Classification

The critical infrastructure information-sharing mechanism might consider the need for classification of certain information and the impact classification would have on the information

dissemination process. Classified information has specific handling and dissemination rules and regulations that must be followed. Classified information can be sanitized and declassified to share with the private sector, or shared with a select group of private sector representatives who are able to qualify for a clearance. However, such a process is time-consuming and would limit the circle of participants in the information-sharing activity. In order to address this potential impediment, the information-sharing mechanism should study whether there will be information collected that will need to be classified, whether adequate authority currently exists to classify that type of information, and the process by which such information can and should be shared with other participants.

- **Pro:** This approach raises classification as an issue and allows for further study of whether it will act as an impediment to information sharing. Such a study is likely to produce recommendations specifically tailored to the information-sharing process.

- **Con:** The study approach does not specifically and immediately address classification as an impediment to information sharing.

Proper Procedures for Exchanging and Treating Information

The critical infrastructure information-sharing mechanism might consider proper procedures for exchanging and protecting trade secrets and proprietary information. Trade secrets currently receive protection by Federal law from theft and unauthorized disclosure (see e.g., 18 U.S.C. § 1831 (economic espionage); 18 U.S.C. § 1832 (theft of trade secrets); 18 U.S.C. § 1905 (disclosure of trade secrets). Most states have also adopted the Uniform Trade Secrets Act which provides an additional layer of protection. These protections provide a framework for recovery from losses that may be incurred from unauthorized sharing of confidential information with competitors. Trade secrets may also receive protection when shared with the government. In order to structure a process that provides the maximum protection to sensitive corporate information, the information-sharing mechanism should consider whether it will receive trade secrets or other forms of proprietary private-sector information, whether adequate procedures exist to protect the status of that information, and whether current legal sanctions are adequate to the protect them from unauthorized disclosure.

- **Pro:** This approach elevates the importance of addressing trade secrets as a potential impediment to information sharing. It allows the issue to be studied within the context of the actual information-sharing process that develops.

- **Con:** It does not specifically and immediately address trade secrets as an impediment to information sharing.

Part Three

Models For Information Sharing

Information Clearinghouse

An information clearinghouse may be public, private or mixed. It may collect information via voluntary or mandatory reporting. Its primary features are centralized collection and widespread dissemination of information. Information may also be accessed upon request rather than through a dissemination process. The Commercial Driver's License Information System is one model of an information clearinghouse.

- **Pro:** Widespread dissemination of information and availability upon request lower the potential liability issues associated with information sharing. Also, a clearinghouse with a large number of participants may raise fewer antitrust concerns (particularly if there is government involvement).

- **Con:** A clearinghouse may not provide the best protection for proprietary information. It may also raise privacy concerns if the information concerns individuals' medical, criminal, employment, or financial backgrounds. Liability could be implicated with regard to those records. Antitrust issues and issues regarding government handling of sensitive information are also implicated. National security concerns may arise due to the widespread availability of information from the clearinghouse.

Advisory Committee/Commission

Advisory Committees and commissions are generally established to handle a specific and focused issue for a limited duration or on a more permanent basis. While advisory committees and commissions are not an exclusively governmental creation, they are employed on a widespread basis within the Federal government. Federal advisory committees often have

private sector participants which usually will subject the committee to the Federal Advisory Committee Act which provides for open meetings and records. Advisory committees collect information related to their mission and may be specifically designed to further disseminate that information. But policy is generally their central focus.

- **Pro:** Federal advisory committees implicate fewer antitrust concerns than models that do not involve government creation or participation. An advisory committee is also more sheltered from liability for failure to disclose information because it is generally a limited exercise and seldom designed to handle "warning" type information. National security concerns are also diminished due to government involvement. The process of selecting participants and vetting participants allows screening for issues relating to "foreign persons" and clearances to be given to allow access to classified information.

- **Con:** Private sector advisory committees or commissions will have to deal with antitrust concerns. These are often small groups that represent companies which dominate an industry. Banding together to accomplish a particular mission without including other smaller members of the industry could give rise to an antitrust claim. It may also create some liability exposure. Antitrust does remain an issue if the body is government created but solely comprised of private sector participants. There will also be problems with protecting information from disclosure if the body is Federally created. FACA will require open records and meeting unless all members are full-time government employees or there is specific exemption.

Mandatory Provision of Information with Limited Exchange

Mandatory information-sharing models generally focus more on the collection of information than its dissemination. Usually, information is legally (by statute, subpoena, etc.) required to be provided to a specific body. Rarely is there any requirement that information be given in exchange or findings be reported anywhere but up the "chain of command." This model will almost always require some government action and most often involves government collection from the private sector and dissemination to government.

- **Pro:** Under a mandatory model there are few if any antitrust issues. Liability issues also are not a factor to the extent the information is not generally shared. Foreign ownership is also not a concern to the extent that the information is not disseminated outside the government.

- **Con:** The primary legal impediment encountered in such an option involves government protection of private sector information. This includes FOIA and trade secrets issues.

Voluntary Cooperation or Exchange of Information

Voluntary exchanges tend to be less formal than the other models considered. Information is collected through the voluntary provision of relevant information by willing participants. Dissemination may be limited to those participants or take more of a clearinghouse model where the information is generally accessible to a wider community. Voluntary information-sharing arrangements may be public, private or mixed.

- **Pro:** If there is government involvement in the process there will be few if any antitrust concerns. FOIA exemption b(4) extends special protection to private sector confidential information when voluntarily provided. Liability concerns are reduced in a model where information dissemination is limited to those who contribute or is generally accessible to interested parties.

- **Con:** Antitrust concerns will be implicated if this information-sharing mechanism is primarily or exclusively private. If it takes an informal shape, antitrust concerns will be heightened. Liability concerns may also be implicated by dissemination of information, if the groups to which it will be disseminated are not well-defined. This model, whether government or private, will have to handle trade secrets and privacy related information with care. If government is the collector and disseminator, it will have to address FOIA and foreign ownership issues.

Threat and Hazard Detection and Notification

A threat and hazard detection and notification model combines an information clearinghouse with a mandatory dissemination feature. The model involves the collection, analysis, and

dissemination of information. Dissemination plays a central role, though it may happen infrequently (i.e. only during emergencies). Dissemination also usually happens through predetermined channels and in this respect is more formal than some of the other models. Many threat detection and notification models occur within the Federal government. The Natural Oil and Hazard Substances Pollution warning mechanism is one such example.

- **Pro:** If government-sponsored, a threat detection and notification model will have no antitrust and few liability concerns. Liability concerns can be virtually eliminated by structuring the enabling legislation or executive order properly. Antitrust issues may also be limited in the private sector because such a model will likely have a limited focus that does not implicate price-fixing or market-splitting.

- **Con:** Liability will likely be a concern for the private sector and could be a concern for the government if special provisions are not made to limit it. Warning dissemination will raise special issues for the government with regard to classified information and foreign ownership.

Part Four

Conclusions

This paper postulates eight "principles" that ought to be considered in thinking about information sharing. The basic principles were derived from studying the five hypothetical information-sharing models that were themselves abstracted from existing information-sharing arrangements. These principles are summarized here as follows:

1. **Antitrust:** Crucial private sector participants have expressed reluctance to participate in the sharing of specific threat and vulnerability information because of impediments they perceive to arise from antitrust and unfair business practice laws. The Federal government might find it advantageous to offer limited assurances to the private sector that participation in information-sharing processes would not, at least under certain conditions, run afoul of such laws.

2. **Liability:** To limit potential government liability arising from its participation in an information sharing and threat warning program or process, the Federal government may wish to specifically enumerate its own duties and obligations arising out of such participation.

3. **Centralized Guidelines:** The Federal government might want to study whether centralized guidelines for sharing information with foreign corporations would serve the interests of national security and government efficiency.

4. **National Security:** Any mechanism established by the government to share information on threats to and vulnerabilities of the critical infrastructures (or to participate in such processes) must set guidelines for the sharing of such information with foreign corporations.

5. **Confidential Information:** Any mechanisms established by the government to share information on threats to and vulnerabilities of the critical infrastructures (or to participate in such processes) should allow for appropriate protection of specific private-sector information. This might require, for example, inclusion of a b(3) FOIA exemption in enabling legislation.

6. **State Government Participation:** Because state "government in the sunshine" laws could impede participation by state officials by requiring disclosure of information that comes into their possession, a study should research and identify legal impediments to information sharing at the state level. A study group could propose solutions and draft model legislation to maximize state government participation in information sharing.

7. **Classified Information:** Any mechanism established by the government to share information on threats to and vulnerabilities of the critical infrastructures (or to participate in such processes) ought to take into account the need for classification of certain information, or certain bodies of aggregated information, and the impact that classification would have on the dissemination process.

8. **Trade Secrets and Proprietary Information:** Any mechanism established by the government to share information on threats to and vulnerabilities of the critical infrastructures (or to participate in such processes) should allow for appropriate protection of information containing trade secrets or other forms of proprietary information.