Stanford University

C I S A C

Center for International Security and Arms Control

The Center for International Security and Arms Control, part of Stanford University's Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The Center brings together scholars, policymakers, scientists, area specialists, members of the business community, and other experts to examine a wide range of international security issues. CISAC publishes its own series of working papers and reports on its work and also sponsors a series, *Studies in International Security and Arms Control*, through Stanford University Press.

Center for International Security and Arms Control
Stanford University
320 Galvez Street
Stanford, California 94305-6165

(415) 723-9625

http://www-leland.stanford.edu/group/CISAC/

Workshop on Protecting and Assuring Critical National Infrastructure: Next Steps

February 26–27, 1998

David Alderson
David D. Elliott
Gregory Grove
Timothy Holliday
Stephen J. Lukasik
Seymour E. Goodman

Center for International Security and Arms Control, Stanford University
Center for Global Security Research, Lawrence Livermore National Laboratory

June 1998

David Alderson and **Timothy Holliday** are graduate students in the Department of Engineering–Economic Systems and Operations Research at Stanford University. **David D. Elliott** was staff director for science and technology at the National Security Council and then vice president at SAIC and SRI. **Gregory Grove** is with the legal staff of the U.S. Air Force. **Stephen J. Lukasik** is a former director of ARPA, a former chief scientist of the FCC, and has served as vice president at TRW, Inc., the Xerox Corp., and the Northrop Corp. **Seymour E. Goodman** is professor of management information systems and policy at the University of Arizona and director of the Project on Information Technology and National Security at the Center for International Security and Arms Control.

The Center is grateful to the Presidential Commission on Critical Infrastructure Protection and Lawrence Livermore National Laboratory for supporting this project. The opinions expressed here are those of the authors and do not necessarily represent positions of either center, the Presidential Commission, the U.S. Air Force, or Stanford University.

Printed in the United States of America

ISBN 0-935371-51-6

Contents

Preface

In July 1996, President Clinton established the Commission on Critical Infrastructure Protection (PCCIP), with a charter to designate critical infrastructures, to assess their vulnerabilities, to recommend a comprehensive national policy and implementation strategy for protecting those infrastructures from physical and cyber threats, and to propose statutory or regulatory actions to effect the recommended remedies. The charter gave examples of critical infrastructures and also noted the types of cyber threats of concern, including, most importantly from our perspective, computer-based attacks on the information or communications components that control critical infrastructures.

Some of the critical infrastructures are owned or controlled by the government, and hence the government can, in principle, harden and restructure these systems and control access to them to achieve a greater degree of robustness. However, the President's Executive Order recognized that many of the critical infrastructures are developed, owned, operated, or used by the private sector and that government and private sector cooperation will be required to define acceptable measures for the adequate protection and assurance of continued operation of these infrastructures.

The Stanford Center for International Security and Arms Control (CISAC), as part of its ongoing Program on Information Technology and National Security, and the Center for Global Security Research (CGSR) of the Lawrence Livermore National Laboratory (LLNL) conducted three workshops to examine many of the issues connected with the work of the Commission. In addition to the questions of vulnerabilities, threats, and possible remedies, we discussed the impact on the marketplace of possible protective actions, cost in terms of capital and functionality, legal constraints, and the probable need for international cooperation.

The first of these jointly sponsored workshops was held March 10–11, 1997, and included participation by members and staff of the PCCIP; the academic community; the information technology industry; and security specialists at infrastructure organizations, research companies, and the national laboratories. The results were published in two reports: "Workshop on Protecting and Assuring Critical National Infrastructure," CISAC, Stanford University, July 1997, and Stephen Lukasik's "Public and Private Roles in the Protection of Information-Dependent Infrastructure," CISAC, Stanford University, May 1997.

The second jointly sponsored workshop was held July 21–22, 1997, with a similarly diverse and expert group of participants, and again including extensive participation by PCCIP commissioners and staff. At this meeting particular emphasis was placed on legal, international, and economic issues, and on the need for new technical tools. The results were edited and reported in "Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda," CISAC, Stanford University, October 1997.

The PCCIP published its final report in late October 1997. Some of the participants in the first two workshops contributed to an assessment of this report in "Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection," Stephen J. Lukasik, CISAC Working Paper, Stanford University, January 1998.

The third joint workshop was held February 26–27, 1998. The PCCIP report, the CISAC Working Paper, and, in effect, the speeches by Commission Chairman Marsh and Attorney General Reno, served as input to the final workshop under the umbrella theme of "Next Steps." The workshop itself focused on producing a constructive response in four primary areas: deciding on priorities, the necessary government-industry partnership, legal issues, and research and development. The results of the panels and breakout sessions of this last workshop have been edited under these four primary headings in the following report.

We would like to thank all of the participants for the tremendous amounts of time and thought they put into these workshops over the course of more than a year. We are particularly grateful to William Perry, Bruce Tarter, Stephen Lukasik, David Elliott, Stan Trost, and Lawrence Greenberg for major contributions to all three workshops. Attorney General Reno and former PCCIP Chairman Marsh made much-appreciated special arrangements to participate in the last workshop. We hope that our cumulative efforts over the course of these workshops have moved this difficult problem a step toward resolution.

Last, but far from least, it is our pleasure to acknowledge the very substantial, long-term, all-purpose assistance of several staffers and students: Janet Abrams, Diane Goodman, Jan Grimm, Karen Kimball, Banani Santra, and Kevin Soo Hoo.

Michael M. May, Co-Director
Center for International Security and Arms Control
Stanford University

Ronald F. Lehman II, Director
Center for Global Security Research
Lawrence Livermore National Laboratory

Seymour E. Goodman, Director
Program on Information Technology and National Security
Center for International Security and Arms Control
Stanford University

Executive Summary

The third Stanford-Livermore workshop in the series examining the protection of critical national infrastructures against cyber attack was held at Lawrence Livermore National Laboratory on February 26–27, 1998. The first two workshops were intended to provide informed inputs to the work of the President's Commission on Critical Infrastructure Protection, and the third, which came soon after the publication of the Commission's report to the President (entitled *Critical Foundations*), was directed toward a critical review of that report and to developing suggestions for steps to implement its findings in four areas that are considered particularly important: criteria and priorities to guide near-term actions; creation of a public-private partnership; legal issues, with some emphasis on understanding impediments to cooperation; and facilitation of the formulation of an R&D plan, with a sub-theme on the robustness of complex systems. We were very pleased to have Attorney General Janet Reno participate in our workshop. She used this occasion to announce a major new FBI center that will be devoted to infrastructure protection and dealing with cyber crime.

The Commission Report

Commission Chairman Tom Marsh provided a synopsis of the Commission's report including some of the supporting reasoning behind its findings and recommendations. The Commission found no evidence of an impending cyber attack but did see that the capability to exploit infrastructure vulnerabilities is widespread and growing. They recognized that mitigating these vulnerabilities was not within the province of the government alone, but required a cooperative and voluntary partnership among government agencies, the infrastructure owners and operators, and those organizations which will devise technical solutions. And, though initial actions should be promptly undertaken, the problem is a long-term one. Among the other conclusions were:

- A first step in drawing the government and industry together is forthcoming information sharing.
- The government should lead by example by making the systems under its control more secure, and sharing these techniques with industry.
- Current research and development investment is inadequate to support infrastructure protection.
- The existing legal framework is not well structured to deal with cyber threat.
- A number of organizational steps should be taken within the government to give necessary focus and coherence to the efforts to protect critical infrastructure.

Remarks of the Attorney General

Janet Reno spoke at some length about the concern within the Department of Justice regarding the policing of cyber crime and law enforcement's role in protecting critical national infrastructure. She noted her activities with her counterparts in the P-8 countries in light of the highly international nature of cyber attack. She is looking for strong linkages between DOJ and the other agencies within the government with responsibilities and capabilities vis-à-vis infrastructure protection, and particularly noted the ongoing fruitful cooperation in technology development with the Department of Defense. She described her efforts to enhance substantially DOJ's R&D efforts. In particular, she hopes that there can be improvements in the technology and processes that will facilitate the gathering of legally usable evidence of criminal conduct and identification of those responsible, and also be able to distinguish rapidly between criminal activities and national security attacks.

With respect to the vital cooperative partnership with industry, she recognized that this will have to be build upon trust and shared objectives, and that there may be some inherent conflicts which will take work and understanding to solve.

The attorney general announced the formation of the National Infrastructure Protection Center within the FBI, which will have a broad charter including a watch and warning unit. She cautioned, however, that all of the actions aimed at protection will be shaped and constrained by the overriding freedoms guaranteed by the Fourth Amendment.

Prioritizing Actions

In considering implementing actions, attention was given mainly to those actions that can be started rather quickly, so that the enterprise can develop some momentum and support among those players who are important but agnostic at this stage.

Several criteria were put forward to help reduce the broad range of possible actions to a manageable number. Some of the key criteria were:

- There should be a clear implementation process and a reasonably short setup time.
- Where feasible, resources should be invested in areas where larger resources can be leveraged in order to achieve some useful early results with a relatively small outlay.
- Emphasis should be given to actions which have good promise of becoming self-sustaining (but not necessarily self-financing).
- Benefits need to be tangible to attract business involvement.

The panel recommended and provided rationales for a number of actions, primarily to be taken by the government to start a process of cooperation with the infrastructure and IT industries. These actions included:

- Start initially with two infrastructures—electric power and telecommunications (including Internet service providers)—because they underlie the other infrastructures and their interruption could potentially have the widest effects.
- Establish a central government entity to coordinate actions among the various government authorities and the voluntary industrial participants.
- Undertake quickly the development of a research plan that will rely mainly on government funding in the early stages, but which will be structured to attract non-government financial participation.
- A key ingredient of a government-industry partnership is information sharing. The first confidence-building step is for the government to provide data on threat and other pertinent intelligence in a limited but usable form.

- Offer expert government assistance to industry on a confidential basis to assess system vulnerabilities.
- Workable protective measures need to be adopted by the government for its own critical networks and these should be shared within the partnership.

The panel's final admonition was that perhaps the hardest but most critical step to take is to transform what is now a government initiative into one that is largely an industry initiative.

Government-Industry Partnership

One of the main themes of the Presidential Commission's report was the importance of creating a workable partnership between the government and industry to address critical national infrastructure protection. Without a viable partnership and the coherence it can offer, efforts to achieve greater protection will, at best, be fragmented and less effective. The workshop panel on the government-industry partnership considered three main issues: Who should be involved, what can the partnership be expected to do, at least in the near term, and how to form such an entity. The who and what questions come first because they will tend to determine the main options for how.

On the industry side would be representatives from owners/operators of the affected infrastructures (initially, presumably, telecommunications and electric power—see the preceding summary of priorities) as well as from the organizations that provide the potentially vulnerable services and systems to those infrastructures, and from the development community. The panel also felt that since many of the problems may have origins and consequences beyond U.S. borders, some limited foreign involvement would be desirable even at the earliest stage. On the government side, there will be participation by the law enforcement and intelligence communities, and from the federal regulators of the particular infrastructures. These agencies, however, do not represent a friendly interface for industry or a natural inducement for cooperation. The government membership should be expanded with this fact in mind. And since it is likely that the partnership will become a technical clearinghouse and a source for security research direction, DoD and the National Institute of Standards and Technology (NIST) would be important participants.

The focus of the partnership's initial effort should be to exchange information that may lead to some mutual understanding of the nature of the problem (vulnerabilities and risks) and of the options and costs (dollars, legal, competitive) for remediation. As options translate into actions, the partnership would undertake to lend support to improved standards and new systems development. There was a clear recognition that achieving objectives such as these will be difficult because of the need to reconcile the different imperatives and goals of the two sides, and that a lot of successful trust building would have to be done. The best approach, therefore, may be small but meaningful steps rather than attempting any grand design.

The panel assumed—as did the Commission—that industry involvement will be voluntary and based on a recognition of common interest. That assumption will presumably always be correct as far as the information technology companies' participation is concerned, and largely valid for almost all of the infrastructure companies, which operate in an increasingly deregulated environment. The primary issue, therefore, is how to create and nurture a sense of common interest around the question of cyber protection, given that not even a common perception—let alone interest—seems to exist today (a major lesson from the three Stanford-Livermore workshops). The panel made a number of useful observations and suggestions:

- There is no good existing model for such a partnership that might be imitated or co-opted, although the North American Electric Reliability Council (NERC) and the National Security Telecommunications Advisory Committee (NSTAC) may have useful elements that should be considered and other joint activities can offer lessons, including lessons about wrong steps.

- The incentives to join will have to be provided almost entirely by the government, at least at the outset. Incentives would include, inter alia, access to information; participation in a process that may create testing criteria and operational and technical security standards, probably in the form of published best practices; involvement in devising an R&D road map; and an opportunity to identify and mitigate regulatory and legal impediments.
- The work of the partnership will have to be guided by and constrained by the industry perspective. A good means perhaps to make this commitment clear is to request that an industry panel draft the first proposal for the partnership.
- The industry participants will include those responsible for security, but should also include senior leadership, such as the CIO, who have a broader business view and can make commitments.

Legal Issues

Of the core issues surrounding the initiative to protect national infrastructures, that commonly perceived by all those involved as requiring prompt attention relates to legal matters. There are questions of government responsibilities, including the status of regulatory authority, agreements for international cooperation, potential new tort liabilities, rights of privacy and public disclosure, and, probably the most concerning at this stage, legal impediments to drawing industry into the voluntary partnership with government, which was seen by the President's Commission as the *sine qua non* for progress.

The workshop's legal panel undertook to examine several of these issues, and their report represents both good scholarship and a perplexing picture. While offering possible options for solutions, their analysis will be particularly useful for highlighting where legal shortcomings and impediments exist and be a stimulus for early action.

- Protecting highly interconnected systems (the report uses the power grid as an example) may require a combination of personal security screening and imposition of operational and technical standards beyond current ones, and some recasting of the liabilities or immunities connected with damage from failures of inadequately protected systems.
- A priori, the legal impediments to information sharing in the public-private partnership are disconcerting. The report discusses such concerns and possible mitigating steps in the areas of antitrust, protection of proprietary and other competitive information, avoiding exposure of vulnerability and security data, and the risk of civil liability.

  As reasonably possible, the government needs to remove (real) barriers to cooperation, but the only positive impetus for industry to participate will be its recognition that there is a problem which must be addressed (for them to be competitive, reliable, and avoid new areas of liability), and that it is better to be involved in the information sharing, joint technology developments, and standard setting, than not.
- The question of responsibilities vis-à-vis insecure or infected software code were outlined, with a general conclusion that obviation lies with personnel trustworthiness and designers' care, impelled to a degree by changing interpretations of where liability lies.
- For the law to act as a deterrent, infrastructure control systems must include as a major design criterion effective technical forensics devices and software. This is of paramount importance in refuting plausible deniability of state sponsors of cyber terrorism.

Research and Development

Research on information-system security has tended to be concentrated on components and point-to-point solutions (such as encryption and firewalls) and less on the vulnerabilities and protection of complex internetted systems. Yet it is precisely the growth in the automated, interconnected character of large infrastructures that has led to concerns about their

robustness against cyber attack and the possibility of cascading failure. A first research priority is to determine the feasibility of building realistic simulations and models to provide greater insights into stressed infrastructure behavior and vulnerability pathways.

The federal government will have to be the source of much of the funding for infrastructure protection research. Since the funds will be expended by separate agencies, an R&D plan (road map) must be developed, jointly with industry, to give coherence to the various projects and to facilitate technology transfer to industry. The Department of Justice will have a major role in the infrastructure protection enterprise, so the panel suggested that DOJ go beyond its traditional level of research funding (perceived as small and with mainly a development focus) in order to be part of the broader R&D effort and dialogue on system security.

Some centers of excellence need to be established, at universities and within industry, to provide the requisite size for multifaceted research. In addition to research results, such centers would be training grounds for specialists in system security (now in woefully short supply) and could provide openly available test beds in which others can evaluate their products and security approaches.

In addition to the discussion of research objectives per se, several of the senior workshop participants also addressed questions related to large system robustness. In particular they noted a number of trends that may lessen the robustness of even current configurations.

- The inherent diversity and heterogeneity of systems that have evolved separately over time make them harder to attack broadly and less likely to propagate failures. It is important that efforts made to organize and coordinate large systems in the name of efficiency (or security) not unwittingly decrease this robustness.
- As technology and cost factors drive systems to more automated functioning, avoiding or recovering from failures will require greater awareness among operators and well-rehearsed contingency plans.
- The mergers of infrastructure companies involve risks of a number of kinds, including making systems control open to more people and the loss of informed memory as designers and operators diffuse.
- The ultimate robustness—redundancy—is not being taught to designers in training.

Unresolved Issues

Not surprisingly, given the nature of the proposed undertaking to protect national infrastructures, with its perhaps unprecedented sweep in terms of public-private policy, the Commission's effort, as well as that of the Stanford-Livermore workshops, identifies many more issues requiring further hard work than ones having reasonably clear answers.

A range of these "hard" issues is discussed at the conclusion of this workshop report. Some observations are:

- Efficient protective steps will (always) be limited by their impact on privacy and accepted freedoms.
- Collective and individual incentives to enhance security are not congruent.
- Deregulation and industry diversity translate into non-uniform security standards and unequal compliance.
- Development of protective techniques for industry-wide networks, including basic research, simulation, and test beds, will not be market-driven for decentralized infrastructures. This will be an important function for government-sponsored R&D.

- With respect to serious threat, the assumption is that it is not imminent and we still have time to act with deliberation, that internal threat may turn out to be the more concerning and difficult to address, and that for planning purposes some canonical threat characterization needs to be agreed upon early on.

- To avoid diffusion of effort, it is better not to try to encompass all of the eight or nine infrastructures in the beginning. Focusing on telecommunications and electric power would be a rational choice.

- The public-private partnership, seen as the key to organized progress, has been analyzed with different foci (organization, process, legal framework of incentives.). It is important to move quickly, with industry involvement or (hopefully) lead, to define a coherent, acceptable relationship. Also, the admonition to avoid a big program, big bureaucracy approach has universal adherence.

- It would be a mistake to delay bringing foreign entities into our process.

- The acute shortage of well-qualified cyber engineers will be a major hurdle.

- There are disparate time frames connected with this enterprise, ranging from seconds to years: attack recognition and response, evidence gathering, conforming legislation and protective measures, technology and system evolution, education of a new generation of designers having a system-security orientation, and several others. Because of this, even notional planning will be complex.

Tom Marsh's Opening Remarks

The Commission concluded its work on October 13, 1997, and submitted its report, *Critical Foundations*, to the White House on October 21. The Commission found no evidence of an impending cyber attack to debilitate our infrastructures; however, it did find that the capability to exploit infrastructure vulnerabilities is widespread and growing. Commission members recognized that most of the infrastructures operate within an existing framework of government policy and regulation. But they are also privately owned competitive industries; as such, it became clear that infrastructure protection recommendations must not adversely affect a company's competitive position. Consequently, the report recognized that all actions would have to be viable in the marketplace as well as the public policy arena. These concerns led the Commission to the following guiding principles.

First, this could not be another "Big Government" unilateral effort. Government must set the example, but the owners and operators are the keys to success. They have a strong economic stake in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and have experience in responding to disruptions.

Second, while our country may be undergoing an information revolution, utilizing the best ideas and processes from current structures and relationships is the preferred way to proceed. They will be easier and faster to implement, more effective, and more likely to be accepted than creating something new. This means building on existing organizations and relationships as well as promoting voluntary cooperation. Partnerships between industry and government will be far more effective than legislation or regulation.

Finally, this is a long-term effort which requires continuous improvement. We must take action in practical increments. There is no "magic bullet" solution. Infrastructure assurance must be an ongoing process, continually reviewed and updated to deal with emerging threats and vulnerabilities. We must aim not only to protect the infrastructures, but also to enhance them.

From these guiding principles, the Commission distilled a number of basic truths that form the backbone of its recommendations:

1. Information sharing is the most immediate need. There are many instances in which information is shared effectively between the private sector and government, but there are shortfalls. Increasing the sharing of strategic information within each infrastructure, across different sectors, and between sectors and the government will greatly assist owners and operators in identifying their vulnerabilities and acquiring tools needed for protection. There has been some resistance to this idea, based in part on the image of government as "Big Brother," and a lack of trust in the government's ability to safeguard information. Further dialogue is needed to assure that the nature and use of shared information is fully understood. Voluntary partnership to achieve this objective was thought by the Commission to be much better than new regulations or laws.

2. Responsibility is shared among owners and operators and the government. Traditionally, owners and operators have focused on protecting themselves from known established threats to their operations; it is obviously in their self interest to do so. The government's focus has been on protecting the nation from threats beyond the capabilities of private self-protection, such as terrorism or hostile acts of a foreign government. But when it comes to infrastructure protection, the Commission found that, in general, the same tools, techniques, and skills are utilized for attack, whether it is by a criminal, a terrorist, or an information warrior. This then gives rise to a concept of shared threats in which responsibility for finding solutions is shared between government and industry.

3. The federal government has an important role in the new alliance. The Commission believes that the federal government's role in infrastructure protection includes the traditional defense, law enforcement, intelligence, and other functions that have proved effective against physical attacks, as well as the additional effort, resources, and processes to respond to the cyber dimension. The government has access to intelligence and sensitive law enforcement information concerning threats to critical infrastructures that is not available to the private sector. For that reason, new means must be devised to make that information available to owners and operators in a timely manner. Of course, this must be done in a way that protects sensitive sources and preserves the protections of the judicial process, while still providing essential information.

4. The federal government should lead by example. The federal government is in a position to lead by example through adopting best practices, actively managing risk, and improving overall security in all of its information systems. Because of its national security mission, the federal government makes considerable investments in both R&D and the fielding of protection technologies in its national security related systems. The government should then, wherever possible, transfer these specialized capabilities into key components of critical infrastructures in the rest of government and into the private sector. The government should serve as the performance benchmark of infrastructure protection.

5. The existing legal framework is imperfectly attuned to deal with cyber threats. Laws change much more slowly than technology. The existing legal framework does not reflect current technology. Authorities need to be modified to allow for greater awareness of information security concerns, to enable response to and recovery from cyber events, to increase deterrence against computer crimes domestically and internationally, and to clarify roles and responsibilities in a cyber world where traditional geographical jurisdictional boundaries do not offer the same means of control and security they once did.

6. Current research and development investment is inadequate to support infrastructure protection. New challenges require new resources and new examination of how to protect ourselves. The Commission's proposed research and development program identifies specific areas for research to provide the needed technologies.

Because of these and other issues identified by the Commission, much needs to be done—and it requires government and industry to work together in a new partnership. The report proposes a set of structures and processes within the public and private sectors to facilitate infrastructure assurance functions and to complement existing law enforcement, regulatory, and other channels of communication between and among critical infrastructure providers and the government. These new structures and processes will provide trusted and protected channels for sharing public and private infrastructure assurance information, and provide a means for focusing, enhancing, and generating additional infrastructure assurance efforts throughout the federal government and private sector. The objective is effective partnership between the federal government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning, and programs. Thus, the Commission recommended:

- An Office of National Infrastructure Assurance in the White House to serve as the focal point for infrastructure assurance.
- A National Infrastructure Assurance Council of prominent infrastructure corporate leaders, representatives of state and local government, and cabinet officers to address infrastructure assurance policy issues and make appropriate recommendations to the President.
- An Infrastructure Assurance Support Office to provide functional support to the federal organizations involved in infrastructure assurance, as well as direct assistance to the public and private sector partnership effort.
- A federal Lead Agency for each sector to take the initiative in bringing together the owners and operators to create a means for sharing information that is acceptable to all.
- A Sector Infrastructure Assurance Coordinator for each infrastructure to function as a clearinghouse, organizing information-sharing activities, protecting the information provided by each participant, and acting as a channel for information to and from the government. In each sector, an association or consortium agreeable to owners and operators should be selected to become the Sector Coordinator. One example of such an organization might be the North American Electric Reliability Council.
- A private-sector Information Sharing and Analysis Center consisting of government and industry representatives working together to receive information from all sources, analyze it to draw conclusions about what is happening within the infrastructures, and disseminate information to both government and private-sector users.
- A Warning Center designed to provide operational warning of an attack on the infrastructures, physical or cyber.

In this, the third Stanford workshop, we must evaluate whether the report contains adequate encouragement for the private sector, and what your expectations are of the federal government. Receiving both public and private sector input at this early stage is essential, for just as the risks are shared between the public and the private sectors, so will the solutions be found. Our national and economic security has become a shared responsibility, one that requires a new kind of partnership between government and industry—one which encourages information sharing and one which requires the government to lead by example.

Protecting our infrastructures into the 21st century requires greater understanding of their vulnerabilities and decisive action to reduce them. Without increased attention and investment, particularly in cyber security areas, the situation will become far more serious than it is today. If we take prudent and creative steps now, however, the nation can prepare itself to meet the threats as they materialize—as they surely will. The Report's recommendations are essentially proactive. While there may not be a crisis today, these problems, left unaddressed, have the potential of becoming unmanageable in the future.

Attorney General Janet Reno's Remarks

This is an issue that is critically important to me: How we protect the systems and the networks of this nation that make its businesses run; how we create a system that can provide for the protection of our nation's defenses; how you get to the hospital emergency room on time; how we protect those whom we hold dear from a threat of chemical weapons in a subway.

Our energy production and distribution channels, our transportation networks, and our telecommunication systems are more vulnerable than ever before as we come to rely on technology more than ever.

This generation faces extraordinary challenges as we face the problems associated with weapons of mass destruction. This technology brings us a new century and a new world of incredible opportunities and of daunting challenges which, as Adlai Stevenson would say, stagger the imagination and convert vanity to prayer.

The government, including the Department of Justice, is facing these challenges head-on and taking steps to ensure the protection of our critical infrastructures, but we know full well that we cannot do it alone. To ensure the protection of our critical networks and systems, we must work as partners, true partners, with the private sector, with the academic world, with great institutions such as this, in this vitally critical effort for this nation.

I am here today to discuss what the Department of Justice, including the FBI, is doing to face the challenges. And I am here to hear from some of you what steps we can take to build a stronger, better, two-way, respectful, trusting partnership with everybody who has been so significantly involved in this effort, some for far longer than we have.

I want a partnership truly based on trust. In 1995 the President asked me to chair a cabinet committee that would assess the vulnerability of our nation's infrastructures and make recommendations as to how to protect them. The process we started led to the creation of the President's Commission on Critical Infrastructure Protection.

As you know, the Administration is presently engaged in determining how to implement this report, so this conference could not be more timely. But one thing is certain, and the commission made sure of that: it is vitally important to the success of any effort that it be based on the idea that infrastructure protection requires that we work together as never before.

It demands a partnership among all federal agencies with responsibilities for different sectors of the economy or for certain special functions, like law enforcement, intelligence, and defense. It also requires a partnership with private industry, which owns and operates most of the infrastructures. It calls for a partnership with academia and labs like the one hosting us today.

You have the scientific knowledge to develop technical solutions. I have already been through some of the processes that you have been involved in, some of the processes that are actually critical to solving and protecting some of the very critical infrastructures that we have talked about today.

It also requires a partnership with state and local law enforcement. They are used to robbers with guns, but there are new criminals out there who do not have guns. They have computers, and they may have other weapons of mass destruction.

The use of weapons of mass destruction or cyber attacks on infrastructures that could lead to events like power outages or telecommunications breakdowns are not hypothetical. They are not speculative. They can happen. And it requires, in the end, a partnership with the American people who have the right to expect that all of us, whether we are an attorney general or a general, whether we are a scientist or a business person, that all of us are going to work together to protect this nation.

The Department of Justice and the FBI, as I have indicated, want to be strong, good partners. Let me face up to an issue. Some people get suspicious of law enforcement. They say, "I do not want to cooperate. I do not want people to recognize my vulnerability. I do not understand the criminal justice system."

We have a responsibility to work through the concerns that people may have so that they trust us. And I am here today and have been involved in trying to do outreach to those responsible for critical infrastructures to make sure that we hear from you as to how we can be a better, stronger partner in the process. There are other concerns. For example, private business may be concerned about confidentiality. Business does not want to have proprietary information made public. The FBI, on the other hand, has a duty to provide an early warning to the community to prevent further attacks. We must work together to see how we can walk that narrow line and ensure that we do our duty in terms of preventing further attacks while at the same time maintaining the confidentiality of the person or institution or business involved.

The Department of Justice and the FBI have a duty to investigate and prosecute most attacks on the infrastructure, but there are constitutional and other legal limitations on what law enforcement can and cannot do. Fourth Amendment protection against unreasonable search and seizures is one of our citizens' most sacred protections.

We must work with scientists as partners to develop technologies and processes that enable us to obtain evidence in strict adherence to the fundamental protections guaranteed our citizens by the Constitution. The private company that is the victim of a cyber attack must likewise understand law enforcement's responsibility to the Constitution.

Some dare to suggest that the Constitution, the most remarkable document that humankind ever put to paper, cannot keep up with modern technology. I say we must not and we will not sacrifice any constitutional protection in order to adapt to new technology.

We must and we will work with you to ensure that we will master the technologies and that together, law enforcement working with the private sector, working with the scientist, will make sure that technology can be adapted to meet the constitutional protections that are so critically important. But to do this, it is going to require that we talk together, that we work together, and that we understand the problem. It may be a problem that a scientist can solve, but we need the Fourth Amendment expert working with the scientist to understand.

The FBI works daily to prevent attacks on the infrastructure. And it is prepared to immediately investigate if the attack occurs. United States attorneys and other Justice Department attorneys are available with technical expertise on a 24-hour basis to respond.

And if the plan is carried out, a cyber attack, if it is carried out by agents of a foreign state or international terrorist group, we have the responsibility as well under our foreign counter-intelligence authorities.

In the early stages of a cyber attack on an infrastructure or a power grid, we often have no way of knowing who was behind it, what their motive was, or where they attacked from. It is impossible to determine whether the attack is part of a terrorist plot, a probe by a foreign intelligence service, or a part of a national-level military assault by a hostile nation state; or is it simply the work of a disgruntled insider bent on revenge against a supervisor; or is it a young hacker out to test his skills against the latest firewalls.

At the outset, then, it may be premature to mobilize the military or redirect national intelligence assets. What we do know, however, is that regardless of the perpetrator, his intent or his whereabouts, the intrusion in most cases constitutes a federal crime. This means the Department of Justice and the FBI have the authority and responsibility to investigate it.

Whether the crime is physical or cyber, we need to ensure that as we investigate we are coordinating with other agencies as appropriate. If the attack appears to come from non-U.S. persons located abroad, we would want to call on the intelligence community to assist in

gathering information about the perpetrator's intentions; or if the attack seems to be part of a hostile nation's war plan or involves an attack on the Defense Department's own critical infrastructures, DoD obviously has a critical role to play.

Our challenge, our extraordinary challenge, is to identify the character of the attack.When is it a straight law-enforcement investigation that the FBI and the Assistant United States Attorney or Criminal Division lawyer control? When is it something that the National Security Council takes over? When is it something that clearly becomes international as opposed to domestic, and therefore the State Department controls?

What this means is that you do not have any ready answers, but you do have to develop a process—and we are in the process of doing that—to determine when we hand it off from one agency to the next, how we work together to make sure that we adhere to constitutional protections, how we adhere to Fourth Amendment issues, how we continue to adhere to the Constitution.

Civilian agencies also have important responsibilities and capabilities. Whether it is the Department of Energy in the event of an attack on a nuclear power plant or an electrical power grid, or the Department of Transportation in an attack on our air traffic control or rail systems, all these agencies have crucial roles in the event of a crisis. But the fact remains that law enforcement initially will have the lead responsibility for responding to an imminent or ongoing infrastructure incident.

One example of the partnerships that we need to foster can be found in a major New York hacker case. The FBI, Secret Service, NYNEX and Southwest Bell, and a number of private companies and universities worked together to identify and prosecute successfully individuals who had hacked into a telecommunications network, a credit-reporting company, and other systems.

Meeting our responsibility to protect critical infrastructures, in my view, is one of the central challenges for law enforcement as we face the 21st century. As our reliance on the Internet, on automated systems, and on other technological advances increases exponentially with every passing month, so do our vulnerabilities to infrastructure attacks. Law enforcement must be prepared to confront this challenge and be prepared to do so in partnership with other federal agencies, with the private sector, with academia, and with state and local agencies.

And thus today I am announcing the creation of the National Infrastructure Protection Center at the FBI. The NIPC's mission is to detect, to prevent, and to respond to cyber and physical attacks on our nation's critical infrastructures and to oversee FBI computer crime investigations conducted in the field.

The center will build on the important foundation laid down by the FBI's Computer Investigations and Infrastructure Threat Assessment Center, which has been subsumed into the NIPC.

To ensure the strong partnerships that I consider vital, the NIPC will include representatives from the Defense Department, the intelligence community, and other government agencies. We also very much want and hope that the private sector will be a participant in this center, very much like it participated in the President's commission.

This is the surest, best, quickest way to build understanding, to learn from each other, to understand the responsibilities, the duties, the processes, and the authorities that each agency or institution possesses. But let me be frank again. I know of the distrust that sometimes exists between agencies.

I want to hear from all concerned, all who are dedicated and vitally involved in the protection of our infrastructure; I want to know what we can do to build bridges of trust and understanding and communication, what we can do to better explain the role of law enforcement so that people can understand, what we can do to sit down with scientists and say, "Here is our law enforcement. How do we solve it?" We can do so much through this center if we work together.

To augment our partnership, we want to establish direct electronic connectivity with private industry and the Computer Emergency Response Team, or CERT, which is located across the country. This is a significant departure from the way law enforcement has

traditionally operated. But the challenges of infrastructure protection require imaginative solutions. And I consider our liaison and outreach to the private sector to be absolutely indispensable to our success.

One of the issues the private sector will raise is, "Why should we work with you in developing technology? How do we know that you will maintain confidentiality? What can we do?" It is fascinating what we can do if we will only sit down and talk together and build trust, recognizing that we all have one common objective which is the protection of this nation that we hold dear.

The partnerships that we envision will allow the NIPC to fulfill its responsibility as the government's lead mechanism for responding to an infrastructure attack. But the NIPC cannot just react from one crisis to the next. To do our job we will have to be able to prevent crises before they happen, and that requires analysis of information from all relevant sources including law enforcement investigations, intelligence gathering, and data provided by industry.

Through partnerships between federal agencies and private industry and with interagency and private sector representation in electronic connectivity to all of our partners, the NIPC will be able to achieve the broadest possible sharing of information and comprehensive analysis of potential threats and vulnerabilities. And through its Watch and Warning Unit, the NIPC will be able to disseminate its analysis and warnings of any imminent threats to a broad audience in and out of government.

This will enable private industry and government agencies to take protective steps before an attack. But, at the same time, we can take steps together to protect the interests of all concerned and balance the responsibilities of everyone involved.

As we build our partnerships, we must ensure that whenever possible we share equipment, technology, and know-how with each other and especially with state and local law enforcement who are on the front lines. Local police respond with guns now, but soon they will have to respond with cyber tools to detect an intrusion, to follow through, to find the person, to hold him accountable; and we must be there working with them.

This equipment will be expensive. You scientists will create so much new equipment so fast that it will be vital that we all work together in every forum possible to make sure that we avoid costly duplication, that we develop research according to sound plans that look both to the defense and the law enforcement and the scientific interest, and that we do as much as we can working together, sharing.

We have established a track record in this area, but we have much to learn, too. One of the most important technological partnerships is the one we have established with the Department of Defense. In 1994 Defense and Justice created a Special Joint Steering Program Group and staffed it with both Justice and Defense personnel.

We developed products such as the prototype see-through-the-wall radar; more affordable night vision devices, which have been instrumental in supporting and helping the Border Patrol; concealed weapons and contraband detection systems; and improved lightweight soft-body armor.

In addition to working with DoD, we have developed partnerships with the Department of Energy and with the National Aeronautics and Space Administration. We point out those as if they are unusual. We should come to accept such partnerships as a way of doing business in everything that those of us involved in the protection of the infrastructure do.

But all of this only begins to touch on the range of things under development and the technologies needed by federal, state, and local law enforcement. As technology becomes more essential to the mission of the U.S. criminal justice system, it has become more important that we better organize ourselves to fulfill these new requirements, because neither federal nor local law enforcement can afford to be isolated from scientific and technological developments.

Accordingly, I have directed the creation of a special working group to streamline the Department's management of research and technology development.

Finally, as many of you can sympathize, the information revolution has happened so quickly that kids in junior high school are often more familiar with the new technologies than

your local sheriff or the FBI agent. We need to build a law enforcement workforce that is educated and equipped to deal with the new technologies and knowledgeable and imaginative enough to think ahead to the next generation of problems.

The NIPC will help us do this by working closely with other interagency groups that are developing training for federal, state, and local law enforcement personnel on cyber investigations and weapons of mass destruction.

By creating the NIPC, the Department of Justice is taking an important step: We are creating new partnerships with the private sector and with other government agencies to combat threats to the critical infrastructure. I also have asked Congress to provide us with $64 million in increased funding to support our expanded efforts to protect the nation's infrastructure in fiscal year 1999. These additional resources will be critical to support the NIPC and will also allow the FBI to create six additional computer investigation and infrastructure threat assessment squads to be deployed in cities across the country. And it will allow us to hire additional prosecutors to target cyber criminals.

As I mentioned earlier, however, not every attack on a computer network or infrastructure that is used in the United States constitutes an attack on our national security and, in fact, most do not. An unauthorized cyber intrusion could very well be, as I indicated previously, from a little hacker or a disgruntled insider. We will pursue those investigations as part of our law enforcement authority. But, nonetheless, part of protecting our critical infrastructure means working closely with the national security community to fight cyber attacks.

Cyber attacks pose unique challenges. Because of the technological advancements, today's criminals can be more nimble and more elusive than ever before. If you can sit in a kitchen in St. Petersburg, Russia, and steal from a bank in New York, you understand the dimensions of the problem.

Cyber attacks create a special problem, because the evidence is fleeting. You may have gone through this computer 1,500 miles away to break through another computer 5,000 miles away. Simply put, cyber criminals can cross borders faster than law enforcement agents can, as hackers need not respect national sovereignty nor rely upon judicial process to get information from another country.

If we are to protect our infrastructure we must reach beyond our borders. Cyber threats ignore the borders. The attack can come from anywhere in the world. We must work with our allies around the world to build the same partnerships that we talk about here at home.

And to that end, a little over a year ago, I raised with my colleagues, the ministers of justice of the P8 countries, the eight predominant, largest industrial countries—Canada, France, Germany, the United Kingdom, Italy, Japan, Russia, and our government—the issue of cyber crime and urged that we join together in developing a common response. Experts from all our countries and departments worked together in the interim. And last December the ministers came to Washington to meet in a day-long meeting that produced agreement as to the dimension of the problem and produced an action plan that I hope can bring real results in the year to come.

We must join forces around the world if we are to begin to deal with the cyber crime that may affect one person or the cyber threat to our infrastructure that may affect the entire nation.

To do this we must work very closely with our colleagues in the defense and intelligence communities both here and among our allies. And this presents the new partnership. While I am building partnerships with the Department of Defense, I am getting to know the minister of justice and the minister of defense in another country. Sometimes the problem seems so big, but it is so critical that we address it and understand that this great, wide world is now one that can be traveled in seconds.

Together we will determine whether emerging developments are a national security problem, a law enforcement problem, how to attack it, how to proceed. But until evidence is obtained that an incident is a national security matter, it is important that we not jump to conclusions, that we not conclude that we must use extraordinary measures that defy our Constitution.

If it has been determined that an incident is an attack on national security, then the Justice Department has three distinct roles.

First, we can conduct a criminal investigation that runs on a parallel track with the national security elements of the case. Indeed, criminal investigations often yield vital information and leads for the President's national security advisors.

Secondly, we can utilize the FBI's counterintelligence authorities and techniques when our national security is under cyber attack from a foreign power.

And, third, we will ensure that any national strategy for dealing with a cyber attack is drawn up, executed, and assessed with strict fidelity to our Constitution and to our laws.

I think this is the most extraordinarily challenging time that law enforcement has ever faced. Boundaries in this world have shrunk. Technology has burgeoned beyond man's wildest imaginations. It is a time for us to come together and realize that if we work together, if we talk together, if we trust each other and understand that we have one common goal which is the defense of this nation, we can make all the difference. If each discipline goes its own way, ignoring the other, we will not solve the problem, and this nation will be at peril.

This has been, in this one visit and about a brief half-hour, extraordinarily enlightening to me. And I go back to Washington confirmed in the belief that, based on the example of what you do here, we can make a difference and we can translate what you do here to so many other arenas and forums around this country where law enforcement, the private sector, the scientists are going to work together.

Thank you so very much for setting an example.

Priority Issues

The report from the Presidential Commission on Critical Infrastructure Protection contains over seventy recommendations for enhancing the robustness and survivability of the nation's water supply, electrical power, transportation, oil and gas, banking and finance, emergency services, government services, and communications infrastructures. While these recommendations are thorough, their implementations appear daunting—particularly when one considers how and where to first tackle the problem of assuring critical infrastructures. An approach to this is to pare down the recommendations to a more manageable set, which can then be implemented in the near term as a starting point.

Assumptions

To facilitate the task at hand, it was assumed that much of the threatened infrastructures are owned by private industry; that system owners and operators would have a strong economic stake in protecting their assets and the security of their customers' operations; and that any attempt by the government to secure these infrastructures must have substantial support from industry.

Only actions that could be taken in the near term were considered. The idea was to propose an initial a set of actions and to provide the opportunity for industry and government leaders to decide where to take the program over the long term. This is not to say that the priority actions need be accomplished in the near term. In fact, several of the recommended priorities are to undertake long-term initiatives because they will take the most time to come to fruition.

Criteria for Prioritizing Recommendations

Early actions should satisfy the following six criteria.

1. All actions should have a clear implementation process.
2. Actions should have a short startup time and be in areas where larger resources can be leveraged to achieve useful early results for minimal outlay.
3. Industry suppliers and system operators must embrace any initial actions. Thus the government must pay particular attention to such concerns as competitiveness, security of proprietary information, and additional regulation.
4. Proposed actions should address significant, near-term issues.

5. Early actions have promise of becoming self-sustaining, although this is not to say that the action need be self-funding. Any action that requires continual government effort and dollars to sustain is doomed to failure.

6. There must be visible return on investment, some tangible benefits as an outcome.

Proposed Priority Actions

The six selection criteria were used to distinguish nine recommendations as actions to implement at the start of a national initiative on infrastructure assurance. As a starting point, the priorities selected from Stephen Lukasik's report, "Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection," were considered. These were discussed, augmented, or modified to produce the following recommendations for priority actions.

1. *Start with only two infrastructure systems, electrical power and telecommunications (including Internet service providers).* These two infrastructures were chosen for several reasons. Both are particularly complex, highly automated, and dependent on interconnected control facilities. They have relatively effective regulatory structures that could "serve as a location for the Commission's proposed sector coordination function."[1]

   The other infrastructures were excluded from early action for several reasons. The Commission concluded, and the workshop participants agreed, that the U.S. financial and banking infrastructure is "further ahead than most in employing sophisticated and, in some cases, unique defenses against loss of assets and corruption of core data systems."[2] Furthermore, enough money flows through the financial system that it should be able to fund any necessary security enhancements. Therefore, in the near term, the banking and finance industries can be left to their own devices simply because of their extensive practical experience in system protection. The other industries considered in the Commission's report (transportation, oil and gas, water, etc.) do not face as significant a threat and can be left alone for a few years pending a review of the effectiveness of a federal infrastructure assurance program.

2. *Establish the ONIA (Office of National Infrastructure Assurance).* The Commission's report strongly emphasizes that many of the infrastructure vulnerabilities lie in the interdependencies of systems. Therefore an effective plan to secure critical infrastructures will require a coordinated effort by all relevant industry and government entities. Hence a central government entity with the authority to coordinate actions related to the security of all infrastructures becomes vital. Not only would such an office provide a central point of contact within the federal government but it should also serve as an agent for much-needed marketing of the problem of infrastructure protection to industry.

3. *Recruit an individual who is credible to industry to lead ONIA.* The government must make an effort to overcome the image of "Big Brother" forcing a set of regulations on industry. Industry officials are more likely to trust "one of their own" instead of a political appointee.

4. *Expand government dialogue with industry.* Another way to garner industry support for government actions is to make a concerted effort to develop dialogue between the public and private sector. During its first year of operation, members of the ONIA should constantly be on the road to speak with infrastructure operators and suppliers. The intent of this extensive "face time" with industry is not only to transfer knowledge and ideas, but also to build a trusting relationship with industry. Representatives from the ONIA should focus their attention on people and groups who can provide the most leverage in

[1] "Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection," Stephen J. Lukasik, CISAC Working Paper, Stanford University, January 1998, 13.

[2] The Presidential Commission's report, A-37.

industry—for example, the CEOs and middle managers of the top twenty infrastructure operators and suppliers, and the heads of state and local public utility commissions. Representatives should also communicate to engineers and researchers through professional organizations and trade associations. The heightened communication between public and private sectors should result in enough interest in infrastructure assurance to make these initiatives self-sustaining.

5. *Increase the level of research and development.* As a first step toward funding new research, the ONIA should develop both internal and external mechanisms to plan a research program. Developing a research plan will take some time, which is why the process should be started immediately. Government funding should be directed to those areas that are unlikely to attract private funding. The ONIA should also encourage funding from private resources through cost-sharing projects, or through consortia with industry. Industry is likely to have a different research agenda than that of the government. Therefore, industry participation in research is important not only for funding purposes, but also to be a participant in the decision-making process. It should also be a goal of an R&D program that, as happened in the case of the Internet, much needed metrics and standards for system security evolve from the research community through a consensus process.
6. *Facilitate and expand information-sharing mechanisms.* The Commission determined that information sharing between government and industry is an immediate need, and workshop participants agreed. However, in view of the significant lack of trust in industry of the government's ability to safeguard proprietary information and to use it properly, a starting point could be essentially one-way, from the government to industry. The government could provide industry with threat data and also build trust in industry by demonstrating its commitment to an information-sharing partnership.
7. *Assist industry vulnerability assessments in areas of government expertise.* The government, in particular the DoD and NSA, has valuable skills in the area of systems vulnerability assessment or "Red Teaming." These services could be offered to private industry with the understanding that potentially damaging information remain the property of the company or companies involved.
8. *Increase intelligence community priority on information threats.* The U.S. intelligence community should also be involved in the efforts to secure critical infrastructure. Much like the DoD and "Red Teaming," the intelligence community can provide unique information to industry regarding foreign and domestic threats. One of the first steps taken by the ONIA should be to establish channels to industry for the distribution of threat information.
9. *Encourage the federal government to get its own house in order.* One of the Commission's recommendations was that the government should lead by example, thus demonstrating its commitment to infrastructure protection. The government could use the relationships with industry it might thereby develop to assist its own internal efforts to bring government systems up to par with the highest standards. This process will speed the upgrade of government systems as well as develop credibility with industry.

In Closing

Comparing the above proposed priority actions with the Commission's recommendations, the first eight address eighteen of those of the Commission. The list was designed so that substantial progress could be expected in the first year of a national initiative. If this is the case, the national initiative can become self-sustaining. But as General Marsh noted in his opening remarks, "There is no magic bullet solution." Infrastructure assurance is a long-term effort that requires continuous improvement. Constant dialogue and review between industry and government will be required to develop a coherent and effective long-term plan.

To gain industry support and trust, it was recommended that the national infrastructure protection initiative be transformed from that of a federal program, as recommended by the Commission, to one "owned" by industry. The heavy focus the Commission puts on matters of federal government structure and organization needs to be replaced by one having an industry-centric focus.

Government-Industry Partnership

This discussion is focused on the resolution of issues and the opportunity for follow-on action from the Commission report, rather than on any particular strength or weakness of the report. Specifically, it is intended to address the following issues:

- *Who are the partners?* It is clear that the federal government is not a unified entity with regard to the disparate needs and interests of the partnership. Similarly, the industry entities also have disparate interests.
- *What is the partnership, and what is it to accomplish?* What are its goals, its principles, its vision? Consider trade-offs between risk management versus risk avoidance, business performance versus national security, relative versus absolute levels of protection.
- *How can the partnership be implemented?* What is the process for these partnerships? Specifically, how to address information sharing issues as well as action issues?
- *What are the deterrents, and how can they be overcome?* What are the incentives for the partners? What are the barriers to implementation? What initiatives can be taken?

As an introduction to the discussion, representatives from the PCCIP informally presented the perspective and intent of the Commission in planning for partnership:

> One of the concerns that the PCCIP had was that while it was evident to the Commission that the vulnerabilities to infrastructure exist, there seemed to be little awareness among private industry. One way of dealing with these perceived vulnerabilities would have been to institute a policy that mandates and regulates it. However, this was widely recognized by the PCCIP as a bad way to proceed. The alternative was to create some form of partnership to foster the flow of information between industry and government. However, in order for this to happen, there must be an understanding of mutual responsibility.
>
> The focus of the PCCIP was to have different lead agencies within the government foster individual partnerships with private industry, because each of the infrastructures is very different. The intent was to try to get a government agency to be the lead and work to tailor the partnership. The Commission understood that this approach would not be sufficient, but would serve as a good first step.

Both the content and spirit of the Commission report were broadly endorsed.

Who Are the Partners?

In its report, the PCCIP proposed a partnership between government and infrastructure owners and operators. However, many recommendations were made to extend representation from the private sector to include more than just the owner-operators of the critical infrastructures. For example, academia will have key roles in performing cutting-edge R&D, and it should therefore be considered from the beginning. In addition, the private sector is more than just industry and academia. There are personal-privacy advocacy groups or end-user advocacy groups who have a stake in the ongoing relationship between government and industry. At the same time, the notion of industry itself might be extended beyond owner-operators to include secondary service providers for the critical infrastructures as well as major businesses who are heavily dependent on them. It was noted that academia could also be considered a critical infrastructure. Its role includes cutting-edge research and development.

It was widely understood that government representation in the partnership would primarily include law enforcement officials and members of the intelligence community. However, diverse participation was encouraged. It was suggested that representation from law enforcement should contain officers, prosecutors, and judges. Likewise, the intelligence community should contribute information security specialists as well as policy experts. Likewise, the individual critical infrastructures are diverse and care must be taken to include broad representation from the affected stakeholders.

It was proposed that international partners be included in the partnership from the beginning because they will be important in the long-term solution to this problem. While the importance of these overseas partners was generally recognized, existing, complex problems with economic competition, politics, and trust among international parties kept this element out of the discussion of near-term needs.

In considering examples of partnership between industry and the government, a number of similarities between them were identified.

- As mentioned in the opening challenges, *neither the federal government nor private industry is unified in its needs*. There is often a lack of support between the executive and management levels within each entity.
- Despite the disparate needs within each group, *both government and private industry are already partnering internally at many different levels*. While much of this partnership is informal, it is already becoming a heavily relied upon source of information and strength for its participants.
- *Actions of both government and industry are driven by survival*, although the respective government and business imperatives that ensure their survival are quite different.
- *Both business and government are strongly influenced by issues of cost*.

Similarly, these partnership examples demonstrated two important differences between industry and government.

- *There is a mismatch of imperatives between the government and business.* Survival for businesses is very different from survival for government. Business imperatives are largely concerned with the growth and security of company value. This company value comes from traditional notions of costs, profits, productivity, and market share, but it is also driven by reputation and credibility. In this context, the government imperative is largely restricted to national security (including economic security) and organizational survival.
- *Business and government speak largely different languages*. Business executives are likely to ask, "What are the least amounts of security that we can implement without being negligent?" whereas government officials are likely to ask, "What is the highest amount of security that we can impose on industry to ensure national security?" This barrier creates

problems in understanding issues and focusing on solutions, even when industry and government are in agreement.

What Is the Partnership?

In trying to understand the partnership itself, a number of existing partnerships within industry and the government were presented and discussed. The conclusion of these discussions was that there are some examples of existing relationships that might serve as a model for this proposed partnership. One of the problems with these examples of partnership is that the industries that they represent are all undergoing major changes in the current Information Age. These industries and their participants are in a period of significant transition, which makes them hard to understand or predict. Examples of industries undergoing this type of transition are the telecommunications, information services, and electric power industries. Other shortcomings of most existing partnerships are that they are limited and do not produce awareness among all the players in their sector, or they do not have enough buy-in of their respective sector.

While no one presented a single, compelling model of a high-level operating partnership between industry and government, the discussion raised many examples of successful partnerships. The President's National Security Telecommunications Advisory Committee (NSTAC) was discussed as an example of a formally appointed group that is often cited as a model, albeit limited, for successful industry and government sharing of information. In particular, there are examples of NSTAC "spin-offs" in the operational Network Coordinating Center (NCC) and the Network Security Information Exchange (NSIE). In the NCC, industry liaison personnel work side by side with government personnel to ensure timely communications provisioning and recovery for National Security and Emergency Preparedness situations. In existence since the early '80s, the NCC represents a very successful, focused sharing of critical information. The NSIE is more of a deliberative body. Government and industry each have an NSIE. They meet jointly, under individually signed non-disclosure agreements, every two months, to share sensitive information on incidents, intelligence, and lessons learned.

Despite the disparate needs within industry, information security professionals from competing businesses and government are finding the need to share information and work collectively for their survival. An example of this type of partnership is the Agora Group, which is an informal organization for cyber security professionals in the state of Washington. Members of the Agora meet frequently to share without attribution information about attacks on their infrastructures. In addition, members have formed an informal emergency response network by which they voluntarily help each other during or after an attack. The business imperative for these security professionals is to share information with one another to ensure their survival, both private and public.

Within the public sector, similar organizations have been formed to meet similar needs. For example, the High Technology Crime Investigation Association (HTCIA) works "to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership."[3] Membership of this organization is largely comprised of individual law enforcement officials from many levels within government who recognize the need to help one another.

In considering these and other examples of partnership, a number of common elements were identified as essential to their continued success. Among these partnership principles are:

1. *Participation must be voluntary*. It is not possible to mandate the commitment to a working partnership.
2. *There needs to be a clear, precise objective or outcome*. The partnership needs to identify mutual issues of concern, and the interaction should be focused on the solutions to

[3] See <http://htcia.org>.

problems related to these issues. There should be a recognized need for one another to solve these problems.

3. *There must be internal support and trust within each of the partners*. Support from senior leadership is essential for the partnership to work. Similarly, the collective workforce must be supportive of this leadership.
4. *There is a need for an institutionalized process to provide lasting effect and benefit*. This allows management to turn over without hindering the partnership. Also, it provides for the empowerment of newcomer individuals within the partnership.
5. *There needs to be frequent interaction of working members of the partnership*. This interaction facilitates the exchange of information and also serves to build trust.
6. *Trust is essential.* Building trust among partners takes time. Confidence-building measures in international relations are a possible example of how to build trust between adversaries.
7. *The partnership needs to be an evolving relationship*. Circumstances (business drivers, technology, etc.) surrounding the partnership are likely to be in constant change. Thus, the partnership must not be a one-time revolution but an evolving relationship. Members must be flexible and adjust over time.
8. *Legal and liability issues can be powerful tools for aligning the interests of the partners.* Among these issues are contracts, audits, liabilities, and insurance.
9. *The partnership needs champions*. There is a need for highly credible, visible individuals or leaders who are trusted by all partners and who can serve as champions for fostering and preserving the partnership.

While these principles are general and not necessarily complete, their identification immediately led to the following list of goals for the intended partnership between government and industry:

- Identify and agree on mutual vulnerabilities.
- Enhance flows of information to promote education and awareness.
- Provide cost savings for all.
- Maintain the public trust.
- Maintain and enhance economic security.
- Overcome false perceptions and other deterrents.

What Initiatives Can Be Implemented?

It was recognized that the first steps in implementing this partnership must occur in a timely manner. Therefore, the intent in considering initiatives to achieve these goals was to begin by picking the low-hanging fruit. To this end, the group favored proposals that did not require an overwhelming effort and could be implemented in a short time horizon. Along these lines, the most favored recommendations were those that leveraged already existing efforts. Minimally, it was agreed that any new initiatives must not disrupt or discourage existing efforts. This approach is consistent with one principle from confidence-building measures. Start with easily agreed upon, easily achieved goals to gain early benefit and start building trust. These initiatives can be loosely grouped into categories of information sharing and action issues.

Some of the proposed first steps toward information sharing include:

- *Identify stakeholders*. As previously mentioned, the direct participants should be those who have a stake in the success of the partnership. Identifying these individuals is the first step to engaging them in partnership.

- *Build on existing groups*. Extend the scope and membership of existing partnerships where appropriate. This builds on existing, trusted relationships. There is an immediate need to provide a bridge between existing partnerships to facilitate their interaction. Perhaps there is a need for a private-sector task force, including representatives from industry, law enforcement, and government officials.
- *Create a clearinghouse for information*. This clearinghouse would serve as a policy collection and retrieval board. It would not be involved in policy formation. One of the clear advantages for this type of clearinghouse is that it would allow for a single point of contact by partners from both government and industry. It would also help to identify and promote a codified set of best practices. These practices must be relatively transparent to users and be easy to use because the business and operational imperatives take over. The clearinghouse should be cataloged by industry, but collected across all sectors.
- *Significant efforts need to be undertaken by the government in order for information sharing to occur*. The federal government needs to figure out what it is going to share, and it then needs to get together all the information it has in order to share it. This is a nontrivial task, and it may require some reorganization of government.
- *Increase the amount of training in information security*. Similarly, there is a need to professionalize the role of information security personnel within government and industry organizations.
- *Identify a senior champion or panel*. A key to success will be to have someone who is trusted and respected by all parties and will work passionately to make the partnership work.

Some of the proposed first action items are:

- *Pursue government outreach to industry at both executive and management levels*. The successful participation of organizations from either government or industry will depend on support at both the mid-level management and executive levels. It is important that both mid-level management and executives buy into the partnership wholly and support the allocation of resources for its success.

  It was proposed that the direct participants at the management level should be those who have a stake in the success of the partnership, i.e. the people with responsibility for security or who operate systems or applications for which security and reliability are crucial. Within the public sector, this group is comprised of law enforcement, intelligence, and security officials from many different organizations and levels within government. Within industry, this group is primarily comprised of CIOs and cyber security professionals. It also includes CEOs and COOs who are becoming more concerned with cyber security issues as incidents get increasing publicity. It was suggested that these individuals be targeted as a foundation for building the trusted relationship between industry and government.
- *Promote the findings of the PCCIP report in common language*. It was agreed that while the PCCIP report was on target in terms of its content, the findings were largely written in the language of government. Non-government national goals were not explicitly mentioned. There is a responsibility to translate the findings of the report into a language understood by business executives and other non-government participants.
- *Have industry draft the first proposals for partnership*. This will help to promote trust and might also be used as a first step toward a joint memorandum of understanding between industry and government. It will also help to bridge the gap in terms of differences in language.
- *Encourage the use of exchange programs whenever possible*. The group felt there was value in greater use of exchange programs between government and industry. Such

programs would allow employees on both sides to “switch places” with their counterparts for a period (6–12 months) to gain valuable experience of the opposite perspective.

- *Where possible, resolve the mismatch of imperatives between business and government*. There were a number of proposals for incentives that the government could use to encourage participation from business. They include:

  Reduce costs of security (shared costs) to members of the partnership, resulting in cost savings and economic advantage over non-members.

  Encourage the establishment of best practices by the private sector, resulting in increased credibility for security managers to executives. An example discussed by the group was the private-sector-organized and -funded Information Systems Security Board proposed by the NSTAC about eighteen months ago.

  Encourage transfer of liability risk for having met guidelines for minimal best practices. One approach to this goal will be to encourage or incentivize the insurance industry to provide coverage for information-related losses as long as industry-agreed best practices are followed.

Partnership Summary

Strong agreement was reached that the first step in building partnership between the government and the private sector is the establishment of information-sharing practices among them. One key finding was that the interests of the government and industry are not as disparate as initially believed. Rather, differences in language and driving forces between the two entities result in gaps of understanding and trust, even when there is agreement among the partners. While there was broad endorsement of both the content and spirit of the PCCIP report, it was concluded that the report was written in the language of government, and it therefore remains largely misunderstood at the executive levels of industry. One of the initial objectives of the education and outreach initiatives should be to translate the findings of the report into a language understandable by business executives and other non-government participants.

In order to have a successful and self-sustaining partnership, the participants must voluntarily come together out of a recognized need to work together to achieve a common goal. Furthermore, senior leadership support among all of the partners is essential. Government outreach to industry should occur at both the executive and management levels. In particular, the liability stakeholders—the individuals responsible for information security—were identified as a potential foundation for building a relationship of trust between industry and government. These individuals are already partnering in many contexts and at many levels within both the public and private sector. Efforts to institutionalize this cooperation should leverage these existing efforts whenever possible.

There are a number of immediate steps that can be taken to foster the flow of information and the building of trust between the government and industry. One such initiative is to create a clearinghouse for information about incidents, best practices, and policies. While this clearinghouse would not be involved in policy formation, it would provide a single point of contact for members of both the government and industry to understand what information is available. In addition, members of industry should draft the first proposals for partnership. This will force a reconciliation of the language barrier and can be used as a first step toward a joint memorandum of understanding.

Other long-term initiatives should be undertaken to help institutionalize the partnership process. For example, the use of exchange programs between the government and industry can facilitate information sharing as well as trust building. In addition, the government needs to reorganize itself to better share information both internally and externally. Furthermore, efforts should be initiated to resolve the mismatch of imperatives between the government and industry. These initiatives might take the form of industry incentives that appeal to reduced costs or a transfer of liability for having met government guidelines.

One of the hardest yet essential components to the success of this proposed partnership will be to identify a senior champion or panel that has “fire in the belly” and can enlist the trust and support of the many players in the public and private arena.

Legal Issues

The Legal Working Group discussed minimum security requirements to decrease interconnectivity risk, legal impediments to sharing sensitive information, prohibitions against Department of Defense involvement in law enforcement, improvement of the deterrent effect of criminal laws, international legal issues, and the ability of laws to provide incentives for participation in the proposed public-private partnership.

Interconnectivity

Legal panel participants touched upon potential tensions between movement toward deregulation and enhanced security. For example, grid-control systems allow transfer of power from one area of the North American power grid to another; however, the interconnected nature of the grid exposes it to the risk of a wide-scale propagating failure. A local power provider could cause a local outage by providing power of an inappropriate voltage to the grid, but security measures in place protect grid-control systems from wide-scale propagating failures that might otherwise result from such local problems. Grid-wide failures could result, however, if an individual system manager, administrator, designer, or maintainer with grid-level access were to commit an act of malfeasance with the intent of creating a propagating failure over a large geographic region. The electric power industry must address this personnel security risk.

In addition, deregulation of electric utilities may result in broader access to the control systems of the North American power grid. It may therefore be in the interests of all operators to have certain minimum security standards in place. If personnel and control-system access security risks are not properly countered, a person (or small group) conceivably could intentionally leverage the interconnected grid to unbalance it and cause a cascading failure over a large geographic region.

Two of the possible solutions to personnel security risks are to (1) limit the security risks at a local level and (2) limit the security risks at a regional or grid-wide level. Imposing minimum security standards on each infrastructure operator, where personnel and control-system access security risks may be most easily identified, is a method of containing those risks quickly. Such standards would increase costs of infrastructure operation, so the challenge will lie in balancing the value of decreased risk against the value of avoiding cost pressure in the electric power industry. Identifying individual security risks at the grid-wide level would be more difficult; therefore, limiting security risks at that level could profitably concentrate on making the grid less susceptible to attacks, perhaps by identifying attacks in progress and erecting software barriers to isolate the attacker. Such modifications may be expensive relative to local controls and could require more time to implement than local controls.

The possibility of local outages and widespread propagating failures raises several issues regarding who should bear legal liability for failures. Power suppliers and grid-control system operators could be held responsible in tort for damages resulting from outages; however, the

movement toward deregulation in the electric power industry may suffer if suppliers are subject to such liability. A single outage caused by a careless or malicious employee may be sufficient to bankrupt a small power supplier. To counter this problem, immunity could be granted to small suppliers in the interest of competition and deregulation; however, immunity could promote carelessness in operation and hiring. Even if such immunity is not granted, the deterrent benefit of holding small suppliers liable may not be as significant as some would expect. Small companies may fail to protect against possible tort exposure and, instead, concentrate scarce resources on growth. For this reason, small companies may have the least robust operating procedures and hiring practices. If tort liability proves ineffective or impractical, establishing criminal liability for causing outages may have greater deterrent effect on those who would seek to cause failures.

The best approach could come from combining local operator security measures with grid-wide access security measures. Regulating some minimum local controls in the near term with a view toward decreasing interconnectivity vulnerability of the grid in the longer term appears to be the best method for containing risks quickly. These legal questions are also applicable to other infrastructures, such as telecommunications infrastructures, that may be susceptible to cascading failures due to overuse or misinformation or propagation of errors or viruses.[4]

Removing Legal Impediments to Public-Private Partnership: Information Sharing

Legal panel participants focused on legal impediments to information sharing, as highlighted in the PCCIP report. They include the threat of antitrust liability, release of confidential information, loss of proprietary ownership of information, and civil liability. A recurring concern in the discussion of legal impediments focused on the inherent problem with voluntary submissions: Even if all impediments to information sharing are removed, industry may choose not to share useful information. For that reason, incentives[5] or regulated requirements to submit information may eventually be called for to achieve adequate compliance.

Antitrust Liability

Industry has cited concerns regarding possible antitrust liability resulting from the sharing of cyber attack data and information relating to vulnerability and protection; however, without an agreement in restraint of trade,[6] such a threat is largely illusory. An agreement to report and share cyber attack incidents, best security practices, and vulnerabilities to a central information collection and distribution organization does not restrain trade if all competitors in the relevant market can voluntarily participate and receive submitted information.[7] Instead, sharing enhances the competitiveness of all who participate. If the collection and distribution organization selectively advantaged some competitors over others, an antitrust problem could develop.

Two ways selective advantage could occur are through embarkation upon exclusive joint R&D projects and establishment of exclusive standards. If some competitors are excluded from participating in joint R&D, perhaps because they cannot pay an equal share of the expenses, those who benefit from increased security resulting from the project may have agreed to restrain trade. Moreover, even if R&D results are shared with all competitors, some competitors may not be financially capable of implementing those security measures and may complain of antitrust violations. Likewise, if standards are agreed upon by only a portion of an

---

[4] See generally, infra, nn. 43–52 and accompanying text (discussing liability for malicious code).

[5] See The President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, 87 (1997) [hereinafter the "PCCIP Report"].

[6] The Sherman Act prohibits contracts, combinations, and conspiracies in restraint of trade. 15 U.S.C. § 1 (1997).

[7] Open participation and distribution of shared information to all competitors who desire such information could also thwart a claim of unfair competition or deceptive acts or practices under the Federal Trade Commission Act. See 15 U.S.C. § 45(a)(1) (1997).

industry, or if agreed-upon standards are beyond the financial grasp of some competitors, those excluded could complain of antitrust violations, especially where such financial incapacity is foreseen at the time of agreement. If a liaison from the Department of Justice oversees joint R&D efforts, the potential for antitrust problems may be lessened. A perception by industry of antitrust risk could thwart joint research initiatives and sharing of ingenuity and resources among competitors to increase infrastructure security.

If industry monies or trade secrets are used to develop security measures, those who contribute to the effort will be concerned about who is entitled to intellectual property rights. In these matters, cooperative research and development agreements[8] (CRADAs) may be used to protect intellectual property rights. CRADAs permit private companies to cooperate with and contribute to government research laboratory efforts.[9] In exchange for the efforts of private companies and a non-exclusive license permitting the government to practice resulting inventions, the government may agree to license or assign resulting laboratory employee patents to the company[10] and to ensure the company retains title to inventions made by its own employees.[11] The CRADA statute also permits laboratory employees to participate in commercialization of an invention, even while employed by the government.[12] Further, the statute expressly protects trade secrets and commercial or financial information under the Freedom of Information Act (FOIA),[13] and permits a laboratory director or agency to provide "appropriate protections, including exemption from the Freedom of Information Act."[14] If the details of a cooperative R&D effort do not fit precisely within the strictures of the CRADA statute, the statute may serve as a model for the development of provisions that would better serve the public-private partnership's needs.

In addition to encouraging cooperative research efforts between industry and government laboratories with the CRADA statute, Congress has lessened the chilling effect of the antitrust laws on wholly private cooperative research joint ventures by enacting law that grants special treatment to certain joint ventures, including joint ventures for the purpose of producing a product, process, or service and joint ventures for the purpose of collection, exchange, and analysis of research of production information.[15] That special treatment includes judging possible antitrust violations of joint ventures under a "rule of reason" standard, instead of a much harsher "per se illegality" standard.[16] Such special treatment also includes limiting damages for an antitrust violation to actual damages incurred, rather than subjecting joint venture participants to the possibility of paying treble damages.[17] In exchange for these protections, the joint venture must disclose its identity and purpose to the attorney general and the Federal Trade Commission and permit publication of that disclosure in the Federal Register.[18]

Industry may be using an antitrust liability theory, however attenuated, as a convenient reason to avoid costs and risks associated with voluntary submission of sensitive information.

---

[8] 15 U.S.C. § 3710a (1998).

[9] Id. § 3710a(a).

[10] Id. § 3710a(b)(1).

[11] Id. § 3710a(b)(2).

[12] Id. § 3710a(b)(3)(C).

[13] Id. § 3710a(c)(7)(A) (referring to 5 U.S.C. § 522(b)(4) (1996)); see generally, infra, nn. 14–27 and accompanying text (discussing FOIA).

[14] Id. § 3710a(c)(7)(B) (providing an exemption under 5 U.S.C. § 522(b)(3) (1996)); see generally, infra, nn. 14–27 and accompanying text (discussing FOIA).

[15] Id. § 4301 (a)(6)(D), (F). Importantly, the statute prohibits exchange of cost, sales, profit, price, marketing, and other information if such information exchange or actions are not "reasonably required" to effect the purpose of the joint venture. Id. § 4301(b). Other potentially desirable production and marketing actions are also prohibited under certain circumstances. Id.

[16] Id. § 4302.

[17] See Id. § 4303.

[18] Id. § 4305.

Some level of assurance from the Department of Justice[19] may ease industry's most immediate antitrust objections, but more fundamental objections, described below, may remain.

Compromise of Confidential Information [20]

Information describing threats to and vulnerabilities of critical infrastructures may contain trade secrets or confidential commercial information which, if released, could prove damaging to a company's reputation or provide advantage to competitors. In addition, industry may submit sensitive information about security measures in place or measures being implemented or considered for implementation. Infrastructure operators may object to sharing competitively important commercial information with the federal government for fear that the information will become public under laws such as FOIA.[21] Similar concerns may impede sharing of information with state and local governments.[22]

Information submitted to the government could be disclosed following a properly made request by an outside party to the government agency holding the information (assuming it is an agency subject to the disclosure laws). The agency FOIA officer processes such requests, first searching for records described in the request and then applying FOIA exemptions to determine whether information in each record is releasable. If the information was submitted by a non-governmental entity and the FOIA officer determines the information is releasable, the FOIA officer must give the entity notice and an opportunity to object to the release of the information.[23]

Guidance to government agencies generally favors release of information under FOIA.[24] The burden falls upon the government to prove that information should not be released when an exemption applies; however, as a practical matter, the government places that burden upon the submitter, who must engage legal counsel and respond promptly to the agency's intent-to-disclose notice with a detailed objection and justification. Ultimately, litigation, at the submitter's expense, may be necessary to protect submitted information from disclosure. These regulatory and litigation expenses concern industry.

To limit uncertainty and contain litigation expense, a "Reverse FOIA" practice has grown up around the submission of information to government agencies. At the time of submission, in anticipation of future FOIA requests, many submitting entities engage counsel to negotiate with the FOIA officer to secure an advance determination of non-disclosure. This hidden regulatory expense also concerns industry.

Exemption 4 of the FOIA protects "trade secrets and commercial or financial information obtained from a person [provided that information is] privileged or confidential."[25] Trade secret information is defined narrowly under the FOIA;[26] however, commercial information is defined more broadly.[27] A great deal of infrastructure compromise information is not of the "secret formula" type of information protected under the trade secret definition, so many infrastructure operators would be forced to rely upon the commercial information portion of Exemption 4.

---

[19] See PCCIP Report at 32.

[20] See Id.

[21] 5 U.S.C. 552 (1996).

[22] See, e.g., Cal. Gov't. Code §§ 6250–6268 (containing the California Public Records Act). For a list of other state freedom of information laws, see also, University of Missouri–Columbia, Freedom of Information Center Home Page [visited April 7, 1998] <http://www.missouri.edu/~foiwww/citelist.html>.

[23] E.g., Air Force Instruction 37–131 ¶ 10.4.1 (16 Feb 1995).

[24] E.g., Id. ¶ 1.

[25] 5 U.S.C. 522(b)(4) (1996).

[26] A trade secret is "a secret, commercially valuable plan, formula, process, or device . . . used for the making, preparing, compounding or processing of trade commodities and that [is] the end product of either innovation or substantial effort. . . ." Public Citizen Health Research Group v. FDA, 704 F.2d 1280, 1288 (D.C. Cir. 1983).

[27] Commercial information includes all information "pertaining to or relating to or dealing with commerce. . . ." American Airlines, Inc. v. National Mediation Bd., 588 F.2d 863, 870 (2 Cir. 1978).

Trade secret or commercial information must be confidential to fall within Exemption 4, and the definition of confidential varies depending on whether the information was submitted voluntarily[28] or involuntarily.[29] Submitted information is generally better protected from disclosure when it is voluntarily submitted; however, a submission will be evaluated under the less protective involuntary standard if it is required to participate in what is usually a voluntary activity.[30] Therefore, if each competitor is required to submit vulnerability information as a condition of access to pooled information, then submission is mandatory (to participate in a voluntary activity) and not "voluntary." Importantly, even if evaluated under the more protective voluntary standard, the burden of proving confidentiality lies with the government, and the agency invoking the exemption "must meet the burden of proving the provider's custom" (and therefore the burden is passed to the submitter, as discussed above).[31] If a voluntary submitter does not conduct its information security program properly, or it does not document that program sufficiently to provide evidence necessary to permit the government to prove the submitter's customary practices regarding release of similar information, the information could be released. Industry seeks freedom from these disclosure pitfalls and freedom from this kind of regulation, and particularly seeks freedom from having to prove complicated standards have been met.

Possible Resolutions without Legislation

- Involuntary submission to government agency, no regulatory change—To prevent release, operators must prove disclosure would result in competitive harm or impairment of the government information collection effort.[32]
- Voluntary submission to government agency, no regulatory change—To prevent release, operators must prove they do not customarily publicly disclose information of the type submitted.[33]
- Voluntary submission to a non-governmental organization (NGO)—FOIA does not require release by NGOs; however, antitrust action is less likely if a government agency collects information, and NGO submission may impair the goal of public-private partnership.
- Government officials contract with submitting entities not to release information,[34] except in summary form as necessary to warn others of attack—Individual contracts could prove cumbersome and the same standards under FOIA apply for voluntary and involuntary submissions.

---

[28] Voluntarily submitted information is exempt from disclosure "if it is of a kind that would customarily not be disclosed to the public by the person from whom it is obtained." Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871, 879 (D.C. Cir. 1992).

[29] Involuntarily submitted information is exempt from disclosure if disclosure is likely "(1) to impair the Government's ability to obtain necessary information in the future or (2) to cause substantial [competitive] harm [to the submitter]." National Parks and Conservation Ass'n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

[30] Lykes Bros. Steamship Co. v. Pena, No. 92–2780, slip op. at 9 (D.D.C. Sept. 2, 1993).

[31] 975 F.2d at 879.

[32] "Competitive harm" is derived from the phrase "likely…to cause substantial harm to the competitive position of the person from whom the information was obtained." 498 F.2d at 770 (describing one of the two alternative prongs in the National Parks test); see also, supra, n.22 (discussing the involuntary standard). Security is important to ensuring competitiveness and continuing operation of a company; therefore, submitters of information about infrastructure control system security measures could argue that substantial competitive harm would result if such information were released.

[33] See, supra, n.21 (discussing the voluntary standard).

[34] An agency's promise not to release information does not guarantee that the information will be protected from release under FOIA. See 498 F.2d at 767. But see Id. at 768 (emphasis omitted) (quoting S. Rep. No. 813, 89th Cong., 1st Sess. 9) (1965) ("[W]here the government has obligated itself in good faith not to disclose documents or information …it should be able to honor such obligations.") and Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1008 (1984) (implying that the government's express promise might improve a submitter's prospects for protection).

Limitations on Use of Information

The last possible resolution listed above, releasing information only "in summary form as necessary to warn others of attack," hints at another possible road to agreement between industry and government. Limiting the uses of the submitted information or setting time periods of non-disclosure may satisfy industry's confidentiality concerns while preventing such information from assisting potential bad actors.

Legal panel participants believed that industry would appear comfortable with the following uses of pooled infrastructure compromise information:

- Risk assessment of threats and vulnerabilities that have national-level implications or impact
- Creation and improvement of national test beds to test security products
- Research and development of security products and standards
- Development of actuarial models to facilitate development of products by the insurance industry to create a market for risk-mitigating insurance policies

Legal panel participants believed that possible limitations on the use of infrastructure compromise information should include:

- Prohibiting use of information to establish civil[35] or criminal liability of the submitter, perhaps by forbidding third parties from using submitted information to show that the submitter was on notice regarding a particular vulnerability[36]
- Prohibiting the opening of law enforcement or adverse regulatory investigations that were not otherwise initiated at the time regarding misconduct revealed by disclosure of information[37]
- Prohibiting use for marketing of security or other products
- Permitting government disclosure of information only after a certain time period, necessary to ensure competitive obsolescence, had expired

Regarding competitive obsolescence: Some types of information could remain competitively damaging for short periods only. Other types may remain competitively damaging for many years. Track participants suggest that some future effort be directed toward determining a schedule for non-disclosure periods for different types of information.

Government recordkeeping expense may be contained by prescribing record disposition regulations that provide a fixed time after which records will be destroyed. This fixed time should provide a window of opportunity for the public to request information under FOIA after the period of non-disclosure has run out, but before the records are destroyed.

A Regulatory Resolution—One Possible Next Step

It appears that government and industry agree that "trick" or "gimmick" information is the most important type of infrastructure compromise and vulnerability information to share. These tricks or gimmicks, which allow unauthorized access to or control of infrastructure

---

[35] Precedent exists for this kind of public-policy exception. See, e.g., Fed. R. Evid. 407 (precluding introduction of evidence of subsequent remedial measures as proof of negligence or culpable conduct).

[36] See, infra, nn. 40–41 and accompanying text (discussing Red Team vulnerability assessments).

[37] Precedent exists for such restrictions on use in adverse regulatory actions for minor violations upon self-reporting. For example, to encourage voluntary reporting of aviation safety incidents, pilots who violate Federal Aviation Regulations can anonymously report those violations under the National Aeronautics and Space Administration ("NASA") Aviation Safety Reporting System. Pursuant to 14 C.F.R. 91.25 (1997), the Federal Aviation Administration ("FAA") cannot use reports submitted to the NASA program (or information derived therefrom) in any enforcement action, except information concerning accidents or criminal offenses.

computer systems, work only until system administrators protect against them. During the period that operators are unaware of these vulnerabilities, attackers can do great damage; therefore, this vulnerability information is extremely time sensitive. Improving the response time for identifying and eliminating these vulnerabilities is a good next step toward forging a public-private partnership.

Some members of industry have indicated that while release of information relating to infrastructure compromise would not be commercially damaging, release of the identity of the company that had been compromised would be damaging. An infrastructure operator's reputation among its customers could suffer if those customers learned that the company's provision of critical services had been threatened. Those customers might choose different infrastructure operators to increase perceived reliability. In short, industry seeks an anonymous submission policy.

Assuming that only identity needs be protected to encourage sharing of attack information regarding new tricks or gimmicks, a good solution would encourage sharing by improving industry's ability to inhibit attacks while minimizing additional regulatory expense by carefully and inexpensively protecting the identity of the submitter. One such solution would be the creation of a narrow statutory prohibition, which would result in a narrow exemption under section 552(b)(3) of the FOIA,[38] that withholds from disclosure to the public potentially damaging or objectionable elements, such as the identity of the submitter, if (a) the information submitted relates to infrastructure compromise and (b) the information is submitted to a particularly identified government entity (or its regulatory successor) tasked with the responsibility for collecting such information.[39] This solution is very narrowly drawn to protect a specific type of information (identity) gathered through a specific, identifiable process.[40]

This regulatory solution permits use and disclosure of the technical information submitted. Only the most immediately harmful information, such as the identity of the submitter, would be redacted from a FOIA release, unless another currently extant exemption were applied to withhold additional information. Importantly, it should be simple for submitters to prove that the exemption applies; therefore, regulatory expense and the potential threat of expensive litigation to protect identity are minimized. It is possible to lessen protection afforded by the exemption by prescribing a fixed time period of anonymity, perhaps five or ten years, although any disclosure of identity may discourage voluntary participation.

Broader exemptions may permit the sharing of security information, information which may lead to the development of standards and joint R&D information. The uniquely sensitive nature of security measures may justify focused FOIA exemptions to avoid the possibility that a court or agency may limit the broad definition of "commercial information" (in error or otherwise) and release security information to the public.[41]

---

[38] Section 552(b)(3) exempts

> matters that are specifically exempted from disclosure by statute…provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.

[39] See PCCIP Report at 31.

[40] See supra n. 30 (discussing the NASA Aviation Safety Reporting System for an analogous regulatory solution to the anonymous self-reporting problem).

[41] See, e.g., 42 U.S.C. 2167(a), 2168(a) (1994) (containing an exemption permitting the Atomic Energy Commission to prescribe regulations forbidding disclosure under FOIA of atomic energy security measures, even if such information is unclassified, when "unauthorized disclosure…could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of …theft, diversion or sabotage….."

Loss of Trade Secret Protection[42]

Those who wish to retain proprietary interest in trade secrets must take reasonable precautions to protect them from disclosure to others.[43] Disclosure of trade secrets to the government may be reasonable in light of FOIA exemptions, but disclosure to a non-governmental organization, especially one made up of competitors in one's own industry, may result in loss of trade secret protection.

In addition, even though FOIA Exemption 4 exists to protect trade secrets, a government agency may choose to exercise its discretion to disclose a trade secret.[44] In such a circumstance, trade secret protection is lost, and the owner's only remedy is against the government in a suit alleging that the disclosure was an unlawful taking without compensation under the Fifth Amendment to the U.S. Constitution. In such a case, the submitter would be required to show that it had a "reasonable, investment-backed expectation that [the government] would keep the data confidential …" at the time it submitted the trade secret.[45] Such an expectation is possible in highly regulated industries only when a statute prohibits disclosure.[46] If the submitter cannot show such an expectation, it will receive no compensation for its loss of trade secret protection.

Any information collection effort should also consider the possibility that infrastructure operators may possess trade secrets of software manufacturers and others who provide equipment to operators. Infrastructure operators may incur civil liability for disclosing trade secrets of third parties, particularly where an operator has agreed to protect that information under a non-disclosure agreement.

Civil Liability [47]

Vulnerability Assessments, "Red Teams," and Information Sharing

So-called "Red Teams"—teams to ferret out vulnerabilities by attempting to break into control systems—facilitate best practices, but industry is concerned that Red Teams may assemble damaging evidence that could be used against a company in civil litigation. When its investigation is complete, a Red Team presents a list of vulnerabilities. If a company chooses to ignore some of the vulnerabilities, perhaps because of scarce resources and a business need to spend those resources elsewhere, one of those ignored vulnerabilities may cause or contribute to a serious system failure. In such event, the Red Team has placed management on notice and management has ignored the problem. A case can then be made for negligence. One can imagine a number of circumstances under which a company would be placed in a worse position than if it had never requested the vulnerability assessment at all. One possible result is that some Red Teams may be asked to reveal to a business only readily remediable vulnerabilities, thus decreasing their overall effectiveness. A resolution to this concern may come through prohibiting the use of shared Red Team information to establish civil liability.[48]

In a similar vein, if vulnerability information is collected and shared with all competitors in an industry, some may not possess the resources to protect against all vulnerabilities disclosed. If most adopt a particular protective measure and a few do not, those who do not

---

[42] See PCCIP Report at 32.

[43] See, e.g., Cal. Civ. Code § 3426.1(d)(2) (Bender 1995).

[44] Discretionary release of trade secrets is generally discouraged. See, e.g., Air Force Instruction 37–131 ¶ 1.

[45] Ruckelshaus, 467 U.S. at 1006.

[46] See Id. at 1008, 10–11. Where a statute permits disclosure, the submitter is on notice that it may be disclosed. See Id. at 1006–07. Where there is no statute that either requires or prohibits disclosure, the submitter has no reasonable investment-backed expectation of confidentiality, because the government may determine disclosure is in the public interest. Id. at 1008–09.

[47] See PCCIP Report at 32.

[48] See, supra, nn. 28–30 and accompanying text (discussing limitations on the use of submitted infrastructure compromise information).

may be violating a duty of due care established by industry standard or custom. If damage follows breach, liability to customers or stockholders may result.

Malicious Code

Malicious coders, insiders who intentionally insert damaging code or back doors[49] into infrastructure control systems, can cause security vulnerabilities that result in infrastructure control system failures. When end users, consumers of the service or good provided by the infrastructure operator, are adversely impacted, the judicial system needs to be prepared to assign liability.

Theoretically, liability for damage caused to end users could work its way backward up the supply chain under a products liability or contract theory. A manufacturer who sells an unreasonably dangerous defective product is strictly liable for physical harm caused to the end user.[50] In addition, manufacturers have a duty to design against reasonably foreseeable hazards. Negligent design may subject a manufacturer to negligence liability.[51] Finally, a manufacturer may be liable for breach of contract or of express or implied warranty that a product is fit for its intended use.[52] Especially where the defect is latent, as software defects are prone to be, defenses to liability, such as assumption of risk, are less likely to succeed. Therefore, when an end user sues an infrastructure operator for interruption in service and perhaps for consequential damages, the infrastructure operator can seek indemnity from the control system manufacturer under a products liability or contract theory. The control system manufacturer could seek indemnity from the software subcontractor (if there is one) and the software subcontractor could sue the malicious code perpetrator.

A number of considerations may, as a practical matter, stop liability short and prevent the passing of liability from hand to hand. First, liability may rest with the infrastructure operator because the operator is unaware of the cause of the failure. The operator may not have the expertise to diagnose a software or firmware failure. The operator may not have contracted for access to the source code, and reverse engineering object code may be difficult and expensive, if that is even permitted under any applicable license. It is an open question whether, by alleging nothing but an unexplained failure of a complex system, the operator should be permitted to engage upon a discovery fishing expedition through the manufacturer's proprietary trade secrets to locate a possible products liability claim.

A second consideration, the anonymity of software design, may stop the liability short with the manufacturer (or software subcontractor). If the malicious coder cannot be located, the manufacturer has no party to sue. Often hundreds of software engineers from many countries contribute to a complex software product. Many could have access to the code fragment in which the malicious code was found. A clever perpetrator may leave a confusing trail or no trail whatsoever. Moreover, if the perpetrator is discovered, the existence of back doors for software development and maintenance may make proving malicious intent (as opposed to inadvertence) extremely difficult.[53]

A third consideration, shallow pockets, may stop liability at the deep pocket farthest along the chain. The perpetrator, if found, or the software subcontractor or the manufacturer may be judgment proof. This consideration places liability upon the party who can pay, most likely the infrastructure operator. Considering that a perpetrator will usually be unable to pay for damage caused, invocation of criminal liability against malicious coders may be appropriate.

---

[49] Back doors permit a user with knowledge to bypass ordinary security measures. Back doors can be employed intentionally for software development, maintenance, upgrading or testing, but they are removed or secured before publication and distribution of the final release. Intentionally failing to remove legitimate back doors after they have served their legitimate purpose can be as damaging as maliciously inserting back doors.

[50] See, e.g., Briney v. Sears, Roebuck & Co., 782 F.2d 585, 589 (6 Cir. 1986) (enumerating a set of elements for establishment of strict liability). See also Restatement (Second) of Torts § 402A.

[51] See, e.g., 782 F.2d at 587 (enumerating a set of elements for establishment of negligence liability).

[52] See Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 84 (N.J. 1960).

[53] An element of intent or knowledge of prospective harm would almost certainly be required if such conduct were made a criminal offense.

All these civil actions are influenced by governing contracts, although it is important to note that warranties against personal injury cannot be disclaimed.[54] If the operator's contract with the end user disclaims liability for consequential damages or interruptions in service, then risk (liability) rests with the end user. Perhaps, from a policy perspective, the end user should bear the risk of loss. In that way, risk is spread across a broad base and is unlikely to cause catastrophic financial collapse of an infrastructure operator following a catastrophic network failure. While disclaimers of pure economic loss are generally permitted,[55] it is an open question whether courts would consider intent to produce harm by an employee of the company benefiting from the disclaimer. Permitting disclaimer in such circumstances could result in careless hiring policies and security measures. If such intent were considered to reduce the scope of disclaimers, then disclaimers for software bugs would be permitted, but disclaimers for malicious code would not be enforced.

Reducing the scope of disclaimable damages would increase the deterrent effect upon software manufacturers, but may have an unintended consequence. Rather than increasing personnel security measures and encouraging software audits, software manufacturers may choose to stop selling software to infrastructure operators to avoid litigation risk. Balancing increased security measures against adverse economic impact resulting from decreased availability of software products to infrastructure operators is an important consideration when determining the permitted scope of disclaimers.

A problem of similar scope to the insertion of malicious code by an insider is the potential for an insider to exploit security vulnerabilities in existing code. The nature of complicated software products makes detection and elimination of every security loophole extremely difficult. The law may treat such "undetected" security loopholes differently than intentional insertion of malicious code, perhaps because bugs are expected in complicated software programs. Differing treatment is more likely if exploitation of a security loophole cannot be effectively traced to disclosure or use of the loophole by an insider.

Track participants saw three mechanisms available to decide liability options: (1) take no legislative action and let the courts decide liability issues, (2) enact preemptive federal legislation to control liability issues, or (3) follow a state legislature workshop model, possibly followed by a model uniform act effort or federal legislation.[56]

Preventing Malicious Code[57]

Hiring new, untried software engineers using limited pre-employment information is a personnel security risk. Control system manufacturers and infrastructure operators could discover potential personnel security risks by considering the criminal record, credit history, and employment history of applicants; however, the state laws in some jurisdictions prohibit access to such information. In some states, employers may be prohibited from asking applicants to voluntarily provide such information, or applicants themselves may be incapable of obtaining such information for use by the employer.

The PCCIP recommended careful study of these issues by a panel of experts representing state and federal government, labor and management, and the privacy community to consider ways of balancing employers' needs and employees' privacy interests. Such a panel could recommend a number of courses of action, including, for example, preemptive federal legislation that would permit employers to request, and employees to consensually provide, such information when applying for positions of particular sensitivity. Alternatively, state legislature lobbying efforts could seek to accomplish the same result in states that prohibit such action. Union resistance to a federal or state lawmaking effort would likely be strong and persistent. Aside from employee screening, employers may increasingly rely on more intrusive

---

[54] See Id. at 95. Tort law regarding defective products provides greater protection for personal injury and physical property damage than for pure economic loss. The remedy for pure economic loss arises in action for contract or breach of warranty. See East River Steamship Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 875–76 (1986).

[55] See Id.

[56] See PCCIP Report at 33.

[57] See PCCIP Report at 87–88.

workplace monitoring. Increased on-the-job monitoring may also help improve personnel security, although it may be expensive and even more likely to precipitate privacy complaints by employees.

One possible model for improving personnel screening procedures is the nuclear power industry. Operators of atomic power plants are carefully screened and trained. Federal statutes exist to prevent government disclosure of sensitive nuclear energy information to persons who have not yet completed a character, associations, and loyalty investigation.[58] Administrative rules promulgated by the Atomic Energy Commission provide for careful screening and personnel monitoring to prevent sabotage.[59] Such measures may provide useful lessons for owners and operators seeking to build a more secure population of system operators, managers, and maintainers in other infrastructures.

Even if legislation is passed, some problems are foreseeable. First, those who ask for information may lose employees to those who do not ask. Given the shortage of trained computer scientists and electrical engineers, those employers may suffer financially upon loss of employees and possible recruits who would prefer not to answer. Second, if employers determine that some national origins pose a security risk, discrimination lawsuits may result.

Conclusion

In this section we have identified a number of financial and information risks to industry. These risks present strong disincentives for industry to engage in information sharing through the proposed public-private partnership, and government must address these risks to encourage participation.

Posse Comitatus

Not all cyber attacks are national security threats. Cyber attacks can be directed against particular individuals, companies, or organizations and not against the United States as a whole. United States military forces are prohibited from executing civil laws,[60] but military forces can respond to a national security threat. A line must be drawn between prohibited law enforcement and permitted protection from national-level threats. Track participants suggested two paths that would avoid violating the prohibition on using the military as a *posse comitatus*.

First, Congress could expressly authorize DoD assistance to protect against cyber attacks. Congress used a similar vehicle to permit DoD personnel and resources to assist counterdrug efforts.[61]

Second, an appropriate government agency could provide regulatory guidance to help DoD determine when a cyber attack rises to the level of a national security threat. Track participants suggested several factors to consider when determining whether a national security threat exists: (1) whether the attack was conducted against a DoD system, (2) the gravity of the attack, (3) whether the system attacked contained classified information, (4) whether the goal of the attack was for information or control, and (5) the importance of the system attacked to the nation's defense, economy, and other priorities.

---

[58] See 42 U.S.C. 2165(b) (1994).

[59] Telephone interview with A. David Rossin (Apr. 17, 1998).

[60] 18 U.S.C. § 1385 (Supp. 1997) (prohibiting use of the Air Force and Army to execute the laws). See also 10 U.S.C. § 375 (Supp. 1997) (prohibiting direct participation of military members "in a search and seizure, arrest, or other similar activity….").

[61] See 10 U.S.C. § 374(a), (b)(1) and (b)(4)(A)(i) (Supp. 1997) (permitting the Secretary of Defense to assign DoD personnel to operate and maintain equipment loaned under 10 U.S.C § 372 for purposes of enforcing the Controlled Substances Act or the Controlled Substances Import and Export Act).

Law As a Deterrent

Identifying people who attack infrastructure systems presently requires the cooperation of many government and private entities and great expenditure of resources. Often, the expenditure of investigative monies greatly exceeds the damage dealt by the attacker. To ameliorate the arduous duty of tracking and apprehending attackers and to improve the ability of prosecutors to secure convictions of those apprehended, better technical forensics are required to identify a perpetrator's location and secure evidence that is admissible under the Federal Rules of Evidence. If law enforcement is to serve as a genuine deterrent, infrastructure control systems must include, as a major design criterion, effective technical forensics devices and software.

International Issues[62]

Communications technologies allow hostile persons to attack infrastructure across national borders without regard to customs inspections and other traditional security measures. The interconnected nature of some systems, such as the North American power grid, makes American infrastructure dependent on physical structures located in other countries, or on organizations having foreign ownership. Issues of jurisdiction and sovereignty will need diplomatic attention, and building international cooperative structures will require significant time.

Eventually, information sharing and common defense measures will improve infrastructure protection worldwide. Now, the United States must champion infrastructure security by finding shared values and common international goals to encourage international development of effective security measures.

Cultural and political barriers may impair development of international consensus. Protection of infrastructure has different meanings in different countries. In the United States, availability of infrastructure networks to transmit and receive communications is a high priority. In some other countries, availability is far less important than ensuring that the content transmitted via such networks is state-sanctioned. Some countries might prefer a network shutdown to dissemination of political dissent or pornography.

Next Step toward Shared Values [63]

Track participants agreed that information sharing among law enforcement structures in different nations would likely be the first profitable government-sector overture to developing international cooperation. Such cooperation would focus on capturing computer criminals and bringing them to justice. Agreements regarding extradition of such criminals would be a probable following step. On December 9–10, 1997, a Meeting of Justice and Interior Ministers of the Eight issued a communiqué including ten principles and a ten-point action plan to combat high-technology crime. The principles included shared values among the Eight of "confidentiality, integrity and availability of data…and ensuring that serious abuse is penalized."[64] Establishment of structures to support these shared values may lead to cooperation in other areas.

Possible private-sector sources of shared values and support structures for those values are the International Telecommunications Union (ITU)[65] and the International Air Transport Association (IATA).[66] These international industry associations contain groups and companies with a shared interest in protecting particular infrastructure networks and, in addition, contain

---

[62][55]Time did not permit extensive consideration of international issues. Several participants later wrote a paper on this topic for the *Comm. of the ACM*. This paper is reprinted, with permission of the ACM, in Appendix A.

[63] PCCIP Report at 85.

[64] Meeting of Justice and Interior Ministers of the Eight, Dec. 10, 1997, U.S.-Can.-Fr.-Ger.-Italy-Japan-U.K.-E.U., Communiqué 6, principle IV [hereinafter "Communiqué"].

[65] International Telecommunications Union, ITU Home Page (visited March 7, 1998) <http://info.itu.int>.

[66] International Air Transport Association, IATA Home Page (visited March 7, 1998) <http://www.iata.org>.

the knowledge and resources necessary to define and investigate infrastructure network vulnerabilities.[67]

International Information Sharing

Increasingly, United States law enforcement shares case-specific information with foreign law enforcement agencies as an essential part of successful investigations and prosecutions. But potentially widespread dissemination of sensitive information among the international law enforcement community may provide industry an additional disincentive to voluntarily submission of sensitive commercial information. Industry is not likely to immediately entrust the law enforcement arm of a foreign sovereign with trade secrets or other competitive information that could be used to benefit a foreign competitor in that country. While industry generally trusts United States law enforcement, foreign law enforcement personnel may not yet have earned an equivalent level of trust. International agreements and international cooperative arrangements should be structured to avoid building in disincentives to compliance, at least where highly sensitive commercial information is involved.

State-Sponsored Cyber Terrorism

Short of strategic information warfare, the ultimate source of state-sponsored computer terrorism is unlikely to reside within a major industrialized nation. So long as hostile nations can maintain plausible deniability of sponsorship of such terrorists, civil and criminal remedies cannot promise deterrence. Development of tracing technology[68] may be necessary to gather evidence and bring diplomatic pressure on offending nations, but such technology can only be deployed in a cooperative environment that demonstrates utmost respect for issues of national sovereignty.

Incentives for Participation

To encourage industry cooperation in the proposed public-private partnership, the law must not only remove obstacles to participation, but also provide incentives to participate. For example, if information submitted to the information sharing mechanism of the partnership insulates the submitter in some way from civil suit related to the information shared, industry can reduce its litigation risk by sharing vulnerability information. Another possible incentive could be immunity from malicious code tort liability for participants in joint R&D efforts to produce audit software targeted to discovering damaging code. Immunity from suit for negligent hiring is a possibility for those who implement specified personnel security measures. Those who attempt joint R&D or standards-development projects outside the umbrella of the partnership may be subject to antitrust liability. With DOJ oversight, the partnership's R&D efforts can be free of that risk. Those who adopt partnership-developed security standards are less likely to suffer negligence liability in the area covered by the standards; therefore, the partnership could provide industry with an incentive to participate in the development of standards. If a CRADA model of research and development[69] is adopted, industry may be able to leverage its own R&D efforts with government personnel and monies and obtain intellectual property rights to profitable developments. Attention to developing and publicizing these and other industry incentives will be required to realize a vital public-private partnership.

---

[67] See PCCIP Report at 33.

[68] Communiqué at 6, principle IX. See also PCCIP Report at 85.

[69] See, supra, n. 5–11 and accompanying text.

Research and Development Issues

The Presidential Commission determined that our nation's critical infrastructures face significant threats from many different sources. Of particular concern to the Commission were the interconnections between systems that might allow for cascading failures. Many decades of research and development have brought us to this point, where technology advances faster than it can be secured. Now, the R&D community has a new challenge—to develop methods for protecting the technologies and systems it has created. The goal of the R&D working group was to determine the priorities, division of responsibilities, and benefits from near-term and long-term research and development.

Ultimately, seven priorities were identified for the focus of research and development in the next few years to help protect critical infrastructure.

Priorities and Recommendations

The Presidential Commission identified six areas on which to focus research and development efforts.

(1) Information assurance

(2) Monitoring and threat detection

(3) Vulnerability assessment and systems analysis

(4) Risk management and decision support

(5) Protection and mitigation

(6) Contingency planning, incident response, and recovery

A discussion of these items resulted in the following seven recommendations.

- *Of the six areas listed by the Commission, the most important area is information assurance*. Significant research needs to be conducted to ensure the security of information while it is stored, while it is in transit, and while it is being processed. Up until now, most of the research in this area has been in the form of components and point-to-point solutions, such as encryption methods and firewalls. However, the R&D community has done little to ensure comprehensive system and infrastructure security.
- *Priority should be placed on developing comprehensive R&D*. The Commission identified the interconnections between systems as a major security concern, and the problem will only get worse. With the current level of deregulation, many systems are becoming even more interdependent—to the point where automated actions can affect several companies. Yet we have very little knowledge of what will happen when part of these interdependent

systems fails. What really happens in a cascaded failure? How can we prevent or mitigate a cascaded failure? The R&D community should fund some research and modeling initiatives to help answer these questions.

- *Invest in centers of excellence at the research level*. Universities and industry have developed many of these centers in the past with significant success, particularly in the semiconductor industry. Similar centers should be developed to address the issues associated with infrastructure and information security. A center of some size can provide several benefits that an individual or small program cannot. For example, a large center will be more on par with industry and will be able to have significant dialogue with many corporations. Centers of excellence can also be used to set up realistic test beds, using industrial advice and support.
- *The R&D community should make an effort to raise the level of best practice in industry*. Over the last decade, the process of software development has become quantifiably better, in part due to the efforts of the R&D community. The same thing should be done for survivable infrastructures. At the moment, it is unclear what specific actions the R&D community should take. The issue of best practices is specifically addressed below.
- *The federal government needs to come up with the funding for R&D in the fields related to information and infrastructure security*. Traditionally, the government distributes funds to different agencies and each agency then funds research to support its own mission. The agencies with the largest funding tend to be the DoD, DOE, NSA, and NSF. The DOJ may also want to consider funding some research, not only to garner funding but to bring DOJ into the dialogue with the R&D community.
- *Develop a technology road map*. Since most federal funding is distributed through separate agencies, there needs to be a common basis for these agencies to ensure they are covering all of the necessary research. Furthermore, industry should develop this technology road map and tell the government what research is needed. Perhaps most importantly, a technology road map can be used as a framework to facilitate technology transfer.
- *Finally, the R&D community needs to make a concerted effort to train more people in the skills required to solve infrastructure security problems*. Many people at the conference commented on the declining number of technical majors in this country's universities. While technical majors are declining, students with the skills to address security issues are almost nonexistent. The government needs to institute some programs to catalyze the training of the people we are going to need in the future.

Critical Issues to Be Addressed by R&D

An attempt was made to identify the general priorities for ongoing research and development in the protection of critical infrastructures. The topic of effective R&D was popular during all the sessions of this workshop. Specifically, panel discussions each day addressed, in some fashion, topics that are considered to be burning issues for the R&D community. Some of the critical issues from these panel discussions are included here.

System Robustness

This material represents the findings of a separate industry panel on the robustness of computer-based infrastructure systems. The discussion was largely centered on the analysis of areas related to robustness for which more R&D needs to be done.

- *Diversity and heterogeneity are critical for the robustness of existing and future infrastructures*. As the R&D community looks for new methods to increase the resilience of the various infrastructures, it is important that they not disrupt the current stability of the existing systems. In particular, one important technical aspect of the infrastructures is that they achieve increased robustness and reliability through diversity and heterogeneity. For example, consider the distinction between local failures and global failures of the

infrastructure. Local failures can only be prevented through appropriate hardening of the individual systems. Global failure, however, can be prevented through the design of a system that allows diversity and redundancy to be used effectively to provide alternatives to the failed components.

Diversity for robustness is important in all aspects of the infrastructure. The provision of "core global" functions (for example, root name servers in the Internet) must be done with an eye to robustness through diversity. The collaboration between a diverse set of providers (for example, the Internet service providers connected through routers) provides robustness through alternate routing. Applications that run across the infrastructure (for example, shipping across various transportation media) must be designed to both exploit the diversity in the underlying infrastructure as well as themselves designed with such diversity.

As new tools and methods are developed, it is important that such efforts not decrease the fundamental robustness that is achieved through diversity and heterogeneity and the looseness in the coordination and management mechanisms that leads to that diversity.

- *Best practices provide effective motivation for increased robustness*. There is a critical human element to infrastructure robustness which comes from having people sufficiently motivated to protect the systems and the information for which they have responsibility. The establishment of appropriate best practices or "standards of due care" is critical in providing this motivation.

  Standards of due care are effective in cases where quantified risk assessment does not work. Consider the use of network firewalls, which have become an important and popular defense against external attack. The risk of attack is incalculable because there are an unknown number of actors, an unknown number of actions, and because attacks will occur under unknown circumstances and at unknown times. Yet, because firewalls are a standard of due care, it is evident that not using them might constitute negligence.

  The use of due care and best practices is already working in many organizations and industries. Again, the motivation is to avoid negligence. However, a common problem is how to get industry participants to use them. To the extent that new R&D efforts can help to establish and promote these best practices, one can expect corresponding improvements in robustness.

- *There is a need for greater awareness among operators and owners of our infrastructures of the impact and consequences of possible failures due to vulnerabilities induced by automation*. Market forces are currently driving industry toward greater efficiency, and much of this efficiency comes in the form of increased automation. This automation compounds the complexity of interdependencies between infrastructures and yields increased risks of cascading failures. The Western power outage and the AT&T network failure of 1991 are examples of cascading effects both within and across infrastructures. In both cases, the real causes were the result of process or human failures rather than failures in the technology itself. In the case of the Western power outage, this breakdown was largely the result of the demands for rapid decisions on the part of operators, who did not respond as quickly as the situation demanded. Imagine what the possibilities would be if this warning and balancing system were totally automated, and someone hacked into the system. R&D efforts should be considered to promote a greater understanding and awareness of the problems compounded by increased automation.

  As with any other new features of a product or service, automation systems need to be assessed by industry to determine whether or not it is necessary to install protections and contingency plans to assure reliability and availability. R&D efforts at the systems level will need to consider the compounding effects of increasing automation. In addition, automation systems themselves should be designed with an understanding of system interdependencies.

Modeling and Simulation

In each workshop, there has been strong endorsement for modeling and simulation as tools for understanding the problem of infrastructure protection. There has, however, been little progress made in the direction of developing and implementing such tools. It was suggested that there are three primary reasons for the lack of progress:

(1) The inherent difficulty in modeling complex, nonlinear systems.

(2) The problem is not enough in the public eye to attract investment.

(3) There is an overwhelming need for an intellectual infrastructure, a community that is working and thinking about it.

Progress in developing a research community to address this problem has been slow. So have attempts to raise public awareness to stimulate private investment. The real issue is to understand how to deal with combinations of mega-state systems that behave in unpredictable ways and how to design systems that are resilient to misbehaviors of individual components.

There are some researchers of nonlinear systems who consider the problem to be insoluble and a waste of effort. Others are more optimistic about the applicability of modeling and analysis to this problem. However, if modeling is to be used successfully, test facilities that permit real-time simulation must also be developed. Much of the model development in other disciplines has centered on a repeated cycle of modeling design and testing.

If realistic models can be built, there is no guarantee that they will provide the necessary information for predicting large-scale failures. That is, the models might yield information that is interesting but not useful to the problem at hand. The study of systems in the presence of deliberate attacks is even more complicated. It may be possible to model networks and also attacks on them. But then the question becomes not whether or not the network can be compromised, but how long will it take to do so and how the intelligent attackers will evolve. Hackers are becoming increasingly creative and patient. How does one search for attacks that nobody has yet thought of?

A commonly proposed solution is to have government fund the development of these modeling and simulation tools. The degree and duration of this funding remains an open question, however.

The Competition in Contracting Act

Among the legal issues that are relevant to ongoing research and development, elements of the Competition in Contracting Act were identified by some as a roadblock to effective investment by government. Specifically, it was cited that the Competition in Contracting Act diminishes DARPA program managers' ability to focus research programs. It was suggested that a waiver be given to the organization that handles R&D for infrastructure security in order that it be able to select contracts quickly and disseminate information immediately.

There was disagreement, however, as to whether or not this waiver was appropriate, even for infrastructure security issues. Specifically, some felt that because the government spends taxpayer money, it must be careful about waiving safeguards. It was agreed that organizations such as DARPA must maintain public trust.

Education and Training

The Commission's report identified a deficiency in the number of technically trained people who are available to address the information-security problem. National Science Foundation statistics reveal that the number of computer science and electrical engineering degrees awarded has dropped significantly in the last decade. In addition, a large percentage of these degrees are awarded to foreign students, most of whom return to their home countries. At the same time, worsening elementary and secondary education is providing a smaller and smaller crop of students for the universities to work with.

Information is the capital commodity of the future. The utility of information is controlled not only by its accuracy but, increasingly, by its timeliness. The half-life of information

technology knowledge of electrical engineering and computer science graduates is very short. Universities are not equipping scientists and engineers to deal with this problem. Continuing education was proposed as the answer, but most universities are not equipped to teach continuing education. Furthermore, there is a perception that real professors do not teach continuing education. Business schools, on the other hand, have excellent executive education programs. There is a need for something similar to the business school model in the science and engineering fields.

It was proposed that there is a need to change the information-security aspect of computer science culture. Few professors work on information security, with one exception, encryption theory, where computer science meets mathematics. There is a need to develop specific training programs for Ph.D., master's, and undergraduate specialists in infrastructure security.

Time is critical in addressing this problem. This shortage of information-technology trained people is already inhibiting progress nationwide. Industry needs 200,000 to 600,000 information science workers to fill existing positions. Because industry is not allowed to import skilled people, it is looking to build businesses offshore to satisfy these needs. In order that it might adequately govern an information-technology-intensive society, the government also has a strong need for people trained in this area. For example, the FBI and other law enforcement agencies need people who can pursue criminal investigations in the arena of infrastructure protection. This need for information technologists within both the public and private sector will continue to grow.

In Summary

The Presidential Commission concluded that while a failure of our most critical infrastructures is not imminent, the danger and number of threats are increasing. Most industries are in a period of significant transition, resulting either from an adjustment to the Information Age, industry deregulation, or both. The time is appropriate for the research and development community to face the challenge and responsibility of securing the nation's critical infrastructure. R&D in systems security will likely take several years to come to fruition. In particular, there is a strong need to take a comprehensive view of R&D for this problem. One point that was noted throughout the workshop was the significance of interconnection between critical systems and how those interconnections require extensive partnership between many groups and agencies. Research and development is no different. This R&D problem must be addressed by the entire R&D community (universities, government, and industry) at a comprehensive level in order to develop effective and timely solutions.

Concluding Thoughts on Unresolved Issues

The focus of the workshop was on the implementation of the Commission's findings. It is possible to view the presentations of the numerous individuals and the several panels at the workshop as contributions from which points of consensus and, more importantly, areas of unresolved issues can be identified. Forward motion is possible in areas of consensus but will be impeded by inconsistencies, contradictions, and unresolved issues, especially when the fact of their existence is not widely recognized. While the former can be readily discerned from a reading of the report, the latter are perhaps less immediately evident. It is the intent of this section to identify such areas where early resolution will assist in furthering progress in critical national infrastructure protection.

This discussion is organized in three parts:

- Defining Long-Term Goals
- Steps for Reaching These Goals
- Issues in the Functioning of an International Infrastructure Protection Regime

Defining Long-Term Goals

How Much Infrastructure Protection Does the Nation Want?

In the treatment of infrastructure protection to date, much of the discussion deals with infrastructure protection as an absolute, a desired state of "protection" to be reached. The protection of infrastructure is, however, not an absolute. Most importantly, as Attorney General Reno observed, "Some dare to suggest that the Constitution, the most remarkable document that humankind ever put to paper, cannot keep up with modern technology. I say we must not and we will not sacrifice any constitutional protection in order to adapt to new technology."

While from a national perspective enhanced infrastructure protection (whatever that may mean in detail) is highly desirable, it is less clear how individual competitors view collective action that *uniformly* lifts the level of security. The continuing relationship of a provider to a customer is based on trust, and thus the degree of trust is a product and service differentiator. Companies in the financial services industry, for example, are acutely conscious of this, and recognize that *differences* in trust that offer competitive advantage are directly related to their future. Thus collective and individual incentives to increase security are not necessarily congruent.

The legal group noted the potential conflict between deregulation, cost, and enhanced security. In the case of the deregulation of electric utilities, more rather than fewer providers will have access to the North American power grid, and their varying security standards introduce growing numbers of potentially weak links. The group notes, "[Imposing minimum] standards on each infrastructure operator would increase costs of infrastructure operation, so the challenge will lie in balancing the value of decreased risk against the value of avoiding cost pressure in the electric power industry."

The legal group also discussed at length issues of information sharing as an aspect of collective action among infrastructure operators. With regard to the protection of proprietary information in the light of the Freedom of Information Act, as just one example, the group reports that, " as a practical matter, the government places the burden [of preventing disclosure of proprietary information] upon the submitter."

Similar legal costs related to incurring civil liability through well-meaning vulnerability assessments, product liability deriving from alleged malicious code, and possible privacy violation and discrimination suits by employees deriving from intrusive workplace monitoring, all suggest that there are unpleasant denizens under the infrastructure security rock.

What Is the Nature of the "Public-Private Partnership"?

"Partnership" can be viewed from at least three perspectives. One is "partnership as organization." This is the view of the Commission's report, where the organizational functions and relationships in the public and private sectors are presented in some detail. It is also an important part of Attorney General Reno's presentation announcing the establishment of the National Infrastructure Protection Center in the FBI and its proposed electronic connectivity to private industry and Computer Emergency Response Teams nationally.

An alternative, although not necessarily incompatible, view is that of "partnership as process." The partnership group, in its enumeration of "partnership principles," defined important dimensions of the process:

- Voluntary participation
- Clear and precise objectives or expected outcomes
- Support within each partner's organization
- Institutionalized process that allows for management turnover
- Frequent interaction of working members
- Trust among the participating organizations
- An evolving relationship
- Use of such legal tools as contracts, audits, liabilities, and insurance
- Champions of the process

The priorities group reflected a similar perspective when it noted that "Infrastructure assurance is a long-term effort that requires continuous improvement. Constant dialogue and review between industry and government will be required to develop a coherent and effective long-term plan."

A third perspective, that of "partnership as a legal framework of incentives," is offered by the legal group. They noted that "the law must not only remove obstacles to participation, but also provide incentives [to private industry] to participate." These, they suggest, include insulating the voluntary submitter of information from civil suits related to the information; immunity from malicious code tort liability for participants in joint R&D to produce audit software targeted to discovering such code; immunity from suit for negligent hiring for those who implement specified personnel hiring measures; antitrust immunity for those who undertake joint R&D or standards development under DOJ oversight; protection from negligence liability for those who adopt partnership-developed security standards; protection of intellectual property rights for those who leverage their own R&D with CRADA relationships with government; and the like. In this view, the terms of the partnership are that the government establishes a legal framework for enhancing infrastructure security and thereafter is a participating partner with a yet-to-be-defined role, possibly ranging from observer to very active.

It is easy to say, "Yes, we mean all of the above." But it should be recognized that there are positives and negatives to every action. Absent clearly defined government intentions, the private sector may, of necessity, prepare for the worst and react to the expectation of more regulation, higher imposed costs, and greater civil and criminal liability.

How Much New Organization Is Needed and Who "Owns" It?

The proposal by the Commission is for what may be perceived by a large part of the private sector as a sizeable addition to the federal bureaucracy with the likelihood, based on past experience, of more downside cost than upside value. This, while it will be seen as an issue, need not be the central issue. The recommendation, by both the partnership and the priorities groups, is to build on what is already available, using existing exchange programs wherever possible, and minimizing new organization until tangible benefits have been realized with the resources at hand.

The more important issue, as put by the priorities group, is who "owns" the infrastructure protection program. The impression to date is that infrastructure protection is a federal government program. The partnership group suggests that the Commission's proposals be rewritten in "common language" rather than in the language of government; and that proposed relations with the private sector be in the form of memoranda of understanding, drafted initially by the private sector. The priorities group suggested that early actions be designed to become self-sustaining, generating enough value to both public and private sector participants as to offer the prospect of their being continued without extraordinary annual selling. The point is not necessarily to recover the costs of what is done to enhance infrastructure protection as it is to provide enough near term value that the necessary resources will continue to be provided by mutual consent.

Private sector "buy-in" into whatever is done to improve infrastructure assurance will be facilitated to the extent that the program is seen as an industry program. Not only will that help ensure that obligations of the participants will be matters of mutual agreement rather than government fiat, but it will also encourage the private sector to evolve the program in directions that can be value-enhancing rather than cost-imposing. These, for example, include reducing the costs of security through more efficient use of resources; increasing the reliability of service, which translates to increased customer satisfaction; and increasing the likelihood that commercial rather than government practices will be employed.

Steps for Reaching These Goals

Where Is the Element of Time?

When presented with an argument to undertake a task, it is natural to ask, "When do you need it?" Thus the element of time is critical, not only to establish the degree of urgency and to lay out milestones in time, but even to rule certain classes of actions in or out. For example, if the essence of the problem of infrastructure assurance rests with technical difficulties for which solutions are not known, the relevant time scale is that for the setting of requirements, the funding of R&D, and achieving results. If the critical deficiency is the availability of scarce technical skills, the relevant time scale is that to recruit and train people, possibly as far back as K–12 and the baccalaureate level. The degree to which either of these factors will limit the progress that must be made has yet to be established.

Time plays another more insidious role in infrastructure assurance. Holes and bugs in information systems derive from the current state of information hardware and software technology and this is, of course, rapidly changing. It does no good to understand and fix problems in last year's systems if they are upgraded and changed in ways that introduce new flaws and new entry paths for intruders. Nor is it helpful if the time to test and debug new systems is greater than the time for them to become obsolete. And, one must uncomfortably admit, information systems undergoing the installation of software are most vulnerable, due to the unplanned nature of the resulting configuration, the necessity of suspending some system protection, and the potential for the introduction of malicious code.

Another time scale mismatch derives from the speed with which intruders can penetrate and move compared with the speed of response of law enforcement that due process imposes. Even longer times can be involved if intelligence collection and analysis, executive branch decision making, and international coordination of national security responses is required. Time favors the attacker.

At the other end of the time scale is the speed of information processing, where machines operate at Gigahertz rates. Attorney General Reno notes this fleeting characteristic of the "evidence" of cyber crimes. Lacking bodies and ballistics, entirely new approaches to forensics must be taken.

How Imminent Is the Threat?

In programmatic terms, the central issue is the imminence of the threat. The Commission wanted to avoid a cyber equivalent of the Cold War "the Russians are coming" ploy, yet they recognized that if the threat is put into a distant and indefinite future it will lose any claim on policy makers' attention. To be sure, hacking occurs constantly, infrastructure systems fail for a variety of reasons, and theft and fraud abound. But the Commission's statements are ambiguous and the workshop shed little light on this key issue, beyond the bureaucratic evidence that *something* is happening in Washington.

Governments naturally take long-term views, but the private sector is less inclined when daily stock prices, monthly sales, quarterly earnings, and yesterday's competitor product announcements are major inputs to strategic planning. All four of the working groups at the meeting tended to adopt a long-term outlook (not having to react to an imminent attack), but this is not to say that nasty surprises are not in store. But even to governments, invasions, revolutions, satellite launches, and foreign nuclear developments seem always to be greeted with surprise and shock. Crippling information attacks may be no different, and the first definitive indication of the threat could be the "flaming datum." But the current level of activity within the federal government reflects at least prudent concern. The challenge will be to communicate this to the private sector. Attorney General Reno and the partnership and priorities groups all reflected the need for outreach and trust building among the participants. The R&D group calls for the development of

technology road maps which can serve to coordinate, if not increase, public and private sector long-term investments in infrastructure assurance.

Aren't the Attackers Already Inside?

While the basis for most discussion of the prevention of information attacks centers on blocking access by intruders external to information and automated control systems, the bulk of cyber crimes today are committed by insiders who have legitimate access to the system. The legal group addressed remedies for malicious code. Two approaches were discussed. The first is based on the concept of caution because of liability and the assignment of liability for consequent damage to operators, vendors, users, or perpetrators. The legal group noted that the assumption of risk by the system user may be the only feasible policy option.

A more constructive approach is that of prevention. The proposition is that personnel with system privileges be subject to vetting to a degree not currently undertaken in the private sector. This will require redefining the relationship between employer and employee, despite the large body of labor law and precedent, and could thus amount to introducing the equivalent of security clearances into commercial environments. The extent to which such intrusion of the employer into personal privacy would be tolerated by workers is unclear. Certainly, employees are becoming adjusted to the monitoring of their interactions with customers, and professionals could accept the licensing and certification. In the final analysis, much depends on the degree to which employees are willing to recognize the seriousness of threats to and the nation accepts the special need to protect critical facilities. And since employees are unlikely to be inclined to make sacrifices that are not matched by the behavior of their employer, a perceived commitment by private-sector infrastructure managers will be critical. Nor, as the legal group notes, is there likely to be a uniform level of vetting within an industry, with the more lax companies thereby securing a competitive advantage in hiring scarce skills.

Are Some Critical Infrastructure Systems More Critical Than Others?

The infrastructure systems the Commission examined were identified in the Executive Order creating it. As was appropriate at that point in the development of national policy, the Commission studied that entire set of systems from the viewpoint of understanding their various characteristics and vulnerabilities. It recommended a set of initiatives intending that they be applied to the complete set of infrastructure systems. The priorities group examined the opportunities for cyber attacks on these systems, bearing in mind not only the nature of each infrastructure system individually but, most importantly, the extent of the interdependencies among them. It concluded that, although they all have dependencies on one another, two infrastructure systems occupy central positions, those for telecommunications and electric power.

Since the national resources that are likely to be made available for infrastructure protection are not unlimited, nor are they likely to scale with the number of infrastructure systems to be treated, it would seem most efficient and prudent to focus available resources on the most critical and vulnerable systems. Such a view is consistent with both the "partnership as process" and the "partnership as legal framework" perspectives noted earlier. As distributed control systems spread to those infrastructure systems currently less highly integrated, they too will acquire the characteristics of the two systems identified by the priorities group. And the techniques developed for the protection of the telecommunication and electric power systems can be naturally extended as appropriate. To do otherwise runs the risk of reducing the resources that would otherwise be available to address the currently more pressing needs.

Why Discourage the Use of Strong Encryption to Protect Infrastructure?

Preserving the government's ability to intercept communications related to illegal activities has been and is an important tool in the protection of its citizens and the preservation of public order. So is the protection of the nation's critical infrastructure. The issue, then, is

the harm that can be done to its citizens through widescale attacks on insecure infrastructure systems compared with the harm to them from organized crime and foreign intelligence activities.

A number of attendees at the workshop spoke to this point, noting that while law enforcement could be denied an important technical capability should the use of strong encryption become widespread, rapid advances in other areas of technology are providing compensating benefits. Thus it would seem that to deny the use of an important capability for infrastructure protection is inconsistent with the government's stated concerns. While domestic infrastructures can use strong encryption, they must apply for waivers to use encryption internationally. The alternative offered by the government, that of key escrow, is simply not viable internationally and the offer is disingenuous.

Why Should the Government Support R&D for the Commercial Security Industry?

The bulk of the nation's infrastructure is privately owned. Its protection, through the purchase of products and services, is provided by a commercial security industry. The issue is what failure in this market does the government seek to remedy through its proposed expansion of current efforts in information-assurance R&D?

The answer derives from the decentralized nature of infrastructure, encouraged in part by the government's antitrust and deregulation policies. As a result, commercial offerings tend to focus on individual facilities and to go no further than the network the customer controls. Thus the R&D on the protection of industry-wide networks and supporting activities such as basic research, simulation, and test beds for the development of experimental prototypes is unlikely to receive funding by the security industry. It is R&D activities such as these that the commercial market fails to address. This is the sense of the R&D group's call for a *comprehensive* approach to network security. Should the Commission's recommendations for a significant increase in the level of R&D be adopted, there will, of course, be a natural bureaucratic tendency to use it for any number of pet projects. This should be resisted in order to secure the maximum benefits from the increased R&D for the nation's critical commercial infrastructure systems, particularly those noted above.

The R&D group's recommendations in other areas such as the examination of system interdependencies and understanding better the idea of system robustness are also important and should not be ignored.

Do We Have Enough People with the Right Skills to Support Infrastructure Protection?

There was broad consensus among the participants at the workshop that current concerns about the security of infrastructure reflect strongly into the education sector. There were a number of factors implicated in the shortage of personnel, including poor K–12 education; decreasing numbers of students graduating in computer science and engineering; lack of focus in graduate programs in computer science on information security; inability to retain foreign nationals trained in information technology fields in U.S. universities; needs for continuing education to enable professionals to retrain themselves to work on information security problems; and shortages of people knowledgeable in information technology in law enforcement. It was noted that because of such labor shortages in the United States, work in areas of information technology is increasingly migrating to foreign countries.

Since there are always temporary shortages of people in "hot" areas, the above concerns have a high degree of plausibility. But several of the above, if correct, raise particular concerns. Where domestic labor shortages force the outsourcing of security-sensitive work overseas, it means that personnel vetting of the software engineers doing the work is far more difficult than it would be were it done in the United States; that sensitive design and implementation information related to United States information systems lies outside the control of its ostensible owners; and that sensitive system code is being transmitted on international communication links under conditions of uncertain security. This has been exacerbated during the last few years by the need to outsource Year 2000 problem-fixing to foreign locations.

It might also be noted there is a certain one-sidedness to the expressed need for information security specialists, obviously intended to add to the people who will work at protecting information. But not all who will benefit from this increased level of technical sophistication will work on the side of law and order. Some will join the ranks of penetrators and attackers.

Issues in the Functioning of an International Infrastructure Protection Regime

How Is the International Dimension of Infrastructure Protection Best Addressed?

Just as the insider/outsider separation of the protection problem is important to focus resources on the most critical part of the problem, the same issue can be raised with regard to the domestic/international separation. If it is difficult to motivate government and management domestically, where numerous opportunities exist for intervention, it would appear to be even more challenging to secure the cooperation of other nations in pursuing attackers where the impact of our concerns is far less. Thus, the combination of less control over intruders operating from other countries and generally less awareness of the threat in the places where they might be located appear to have resulted in a heavily domestic focus of U.S. planning. Nevertheless, as both the Commission and Attorney General Reno note, geographical boundaries are far less effective in screening information systems from "foreign" influences.

There is also a sense of getting one's own house in order, and being able to lead by example, before approaching other countries for assistance in tracking intruders operating in or through their territory. But in view of the ease with which cyber attacks can be routed through other nations, thereby creating sanctuaries for attackers, the disproportionate importance of the international aspect of the problem cannot be overemphasized. As a minimum, the international side of the issue deserves equal emphasis to the domestic side. The Commission was not able to explore these issues adequately during its deliberations. In an appendix, the international concerns are addressed at somewhat greater length.

How Will the Handoff Between Law Enforcement and National Security Work?

Organizations frequently experience intrusion attempts and have some type of operational procedure in place to deal with them. Thus the initial response is that of the private system operator who, even in the case of a serious intrusion, can refrain from reporting it. But should the private operator choose to escalate the incident, it will, according to Attorney General Janet Reno, initially be treated as a violation of a federal statute and hence a matter of law enforcement. Reno explains that if upon investigation evidence of a non-U.S. person located abroad is uncovered, the intelligence community will be called upon to determine the intent of the intruder. If the intrusion appears the work of a sovereign state, control of the investigation and the response to the intrusion shifts to the national security decision structure.

This is not unlike the sequence of events in the investigation of any crime, where jurisdiction will shift depending on findings at earlier stages. But the evidence of cyber crimes and cyber attacks is far from unambiguous, and may, in fact, require some considerable effort and cooperation across a number of jurisdictions to even assemble. Thus there are major structural impediments to the investigation of cyber attacks. The attack will unfold quickly, yet the time needed for sensing, investigating, and assessing it can preclude actions intended to limit damage. Clearly, there are fundamental matters of procedure and doctrine to be settled before organizational initiatives can be effective. These should be high on R&D agendas.

Appendix A. Infrastructure Protection: An International Perspective

To appear in the Communications of the ACM, June 1998.

With permission from the Association for Computing Machinery.

INFRASTRUCTURE PROTECTION: AN INTERNATIONAL PERSPECTIVE

S. J. Lukasik, L. T. Greenberg, S. E. Goodman

"Infrastructure" is defined as "the basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions." Societies invest in infrastructure to meet their current and future needs and thus infrastructure reflects the evolution of technology from simpler to more complex, and, in many parts of the world, in the directions of lower cost to users, increased efficiency for its operators, greater safety for society as a whole, and greater consumer choice.

Diminishing infrastructure moves the society it supports toward less comfort and safety, from plenty to scarcity, from richness to want. Societies recognize their critical dependence on these "commons" and adopt policies and processes to distribute infrastructure and services and to protect them from damage and misuse. Conversely, attacking a society implies threatening its people and infrastructure systems. Denial of access to such basics as water, energy, and transit is a form of international conflict that threatens a nation's security and often leads to war.

The industrial revolution greatly increased the extent and the complexity of the world's infrastructure, its connectivity, and its technical and economic interdependencies. Developed nations have, over the past generation, entered a second, equally significant, period, that of the information revolution. Information technology (IT) penetrates into many aspects of life for an increasing number of people throughout the world, enriching us but also producing systems of such complexity that they create new dependencies and risks to society.

Attacking Infrastructure

Since World War II there have been two primary ways in which attacks on infrastructure proceed: aerial bombardment and economic sanctions by nation-states. Both require substantial resources, the former in military capacity, the latter in political and economic strength.

Concerns about the integrity of modern IT-based infrastructure systems go beyond the two primary traditional threats, because even limited failures in extensive and interconnected

systems can cause widespread disruption and damage. In addition to hostile nation-states, international and domestic terrorism and organized crime have the demonstrated potential to undermine societies and diminish confidence in the ability of social and political structures to fulfill their expected roles. These emerging concerns over the vulnerabilities of modern infrastructures have been highlighted by the President's Commission on Critical Infrastructure Protection (PCCIP) in the United States and a similar group under the Ministry of International Trade and Industry (MITI) in Japan [2,6].

The industrial revolution had as a basis mechanical and electromagnetic technologies in the generation and control of power and transportation. But the control of such systems remained largely mechanical, and always with manual backup. The information revolution has expanded the sophistication of control systems. Sensing of system status, signal processing, hardware and software control logic, system optimization, and fault diagnosis are heavily automated. Operators are remote from the systems they "control." Systems do not always behave as their designers intended, nor is their essential software necessarily understood in all its details. As control facilities are interconnected to increase capital and labor productivity, as already complex systems become linked to other complex systems to produce ever more intricate structures, and as rapidly developing IT drives changes that defy effective configuration management, control inevitably slips away. Failure modes and the consequences of failure cannot be foreseen.

Infrastructure systems are tested daily by accidents, natural disasters, and human error, and thus engineers and managers have substantial opportunity to harden their systems, learn from errors, and prepare for future stresses. Were this the only concern, societies might take comfort in relying on professional and economic drivers for greater infrastructure safety and reliability.

But infrastructure systems face not only the random processes of failure and error, they also can be maliciously attacked through the very devices that otherwise enhance their operation. Centralized architectures provide opportunities to disable the heart of a system, inducing disruption over large operating areas. Decentralized architectures provide vulnerable points of entry at the periphery. In both cases, what happens at the interfaces between the large numbers and types of computers, operating systems, control software, and communication systems can be exploited by an attacker. Exacerbating the problem of cyber attacks is the global availability of penetration tools and information on their use, and a deficient sense of responsibility among many computer-literate people who view information systems as fair game and fun to penetrate.

But are these hypothesized threats real? Are they more serious than the other risks societies and individuals already necessarily assume?

There are two types of answers to these questions. The first, empirical in nature, is that malicious attacks on infrastructures are taking place as you read this. In national security terms, so far they have been "low level," but they impose costs on society. These are attacks by white-collar criminals, by disgruntled employees and former employees, and by hackers. They have increased the level of activity in the security industry, and added the need for cyber security to that of physical security. They are increasing the market for insurance products to protect against loss, including extensive self-insurance, by operators of such as the banking and finance and transportation infrastructures. So attacks are real, and they can be quantified, at least to the extent that they are detected and reported. They involve theft of service, theft of information, reduced integrity of data, and invasions of privacy.

The second type of answer is to anticipate that worst-case scenarios of widespread attacks on national and international infrastructures by state-supported adversaries, the "high level" national security threats, will eventually happen if we allow them to. In this sense, the PCCIP's report may be viewed as a call for prudent action, lest these concerns eventually be demonstrated to have been accurate.

Protecting Infrastructure

What, then, are these prudent actions? Some of them are of a "terminal defense" nature, undertaken by owners and operators, to protect the individual nodes in a network. These include hardening nodes against physical and electromagnetic attack, erecting firewalls, backing up operational information, providing redundant capacity, and other "best practices." Relying solely on such measures, however, ignores Sun Tzu's admonition that a passive defense is futile.

The total system is greater than the sum of its nodes. Focus on the system aspects of protection calls for collective actions, such as undertaking audits of system operation and exchanging the information with other operators to facilitate detecting patterns of distributed attacks, providing redundant system capacity, preparing to reallocate system load if attacked, preparing plans to ration diminished system capacity, and assisting system reconstitution. But even more important than these largely post-attack measures are those intended to prevent attack. Among these are steps to deter attacks, to take cooperative measures within the infrastructure industry to promote improving the state of the art in system security, and to exchange threat information so that operators can make investments commensurate with the risks they face.

The thrust of the present discussion is the domain of collective action, especially on collective international actions to diminish the likelihood and consequences of cyber attacks on infrastructure.

A question to be addressed, therefore, is what are the bounds of infrastructure systems and what organizations are critical for collective action? The bounds on an infrastructure system naturally depend on the specifics of each system. The charter of the PCCIP identified eight critical infrastructures: telecommunications, electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services (including medical, police, fire, and rescue), and continuity of government [3]. These vary greatly in the extent of their connectivity and the relationship of each to political and legal jurisdictions.

In many countries, some infrastructures, like water supply, can be local, or within or among first-tier domestic political jurisidictions, i.e., states or provinces. Emergency services are provided at the local or provincial level, although there can be a need for intranational coordination as in the case of disasters near the boundaries of different jurisdictions. Others, such as transportation, tend to be organized at state or national levels, although important aspects of air and marine transport are international in character. But many infrastructures are inherently international, e.g., telecommunications, electrical power, gas and oil storage and transportation, and banking and finance. Thus dealing with their protection is necessarily a matter for international organization and cooperation.

Infrastructure interdependencies are a particularly important element of the issue, because they are unlikely to be a primary focus of attention of the system operators. Such interdependencies are critical for two of the identified infrastructures: telecommunications and electric power. Not only do they depend on each other—telecommunications equipment requires electric power and electric power system operation depends on distributed control facilities—but most other infrastructures depend on these two. For these reasons the substance of international attention must start with telecommunications and electric power. Of these two, the electric power system interdependencies are usually between adjacent jurisdictions, while those for telecommunications derive from their global extent.

The Need For Collective Action

As the PCCIP stated:

> …protecting our infrastructures at home is not enough. Many aspects of infrastructure operations extend beyond our national borders, and even beyond the control of their owners and operators. The very nature of the cyber dimension renders national borders

almost obsolete, and national laws and policies based on those borders of less and less consequence.

There are other reasons besides the multinational connectivity of what are essentially shared infrastructure systems for addressing protection in terms of collective actions among sovereign countries. Several have been noted earlier: facilitating the exchange of information regarding security measures and threats; and facilitating agreements to provide redundant capacity, to share load, and to assist in reconstitution. These are relatively straightforward and may, in some cases, be implemented under existing international treaties and administrative agreements.

One possible action that is more complex, however, is to construct an international order that will deter cyber attackers. Deterrence rests on the paradigm of detect-locate-identify-punish, and to do so with sufficient certainty that cyber attacks on infrastructure will not escape the prospect of legal action or international sanctions against the attacker. Detection of system attacks requires international cooperation in pooling system "anomaly" data if evidence of coordinated attacks, or their precursor probes, is to be available for analysis and for use in formulating responses. Location requires back-tracking attacks from target to source, recognizing that routing attacks through multiple locations and nations serves to conceal the points of origin. Identification requires the cooperation of local authorities to pursue their citizens, or to impinge on their sovereign authority to investigate and punish. Punishment itself has two faces. One is a law enforcement face, where civil or criminal statutes are violated and this then defines the character of the punishment. The other is a national or international security face, where a relationship between the specific attack and a sponsoring sovereign state must be established.

Finally, the greater the degree of economic development in a country, the more that country stands to lose through cyber attack. The inevitable spread of information technology will have the effect of putting more nations at greater risk over time. Thus the time is appropriate to take international action to reduce the likelihood that cyber attacks will be seen as an effective threat to international development and order. The leading nations of the world need to exercise global leadership in understanding and controlling the adverse consequences of the technologies on which we all depend.

Obstacles to Collective Action

The principle of sovereignty and the diversity of the international system of sovereign states may impede cooperation in enhancing cyber security. A discussion of information attacks from the standpoint of existing concepts of international law is provided in [4], where it is noted that the absence of prohibitions against information warfare is significant because the general rule is that whatever is not prohibited is permitted. This lacuna thus prevents the direct application of much of the body of existing treaties and agreements to support collective international action against cyber attacks.

Nevertheless, we adopt the view that cyber attacks are, or should be, illegal acts subject to investigation and prosecution by national law enforcement agencies acting within a context of international legal agreements. However, it must be recognized that a sovereign state exerts exclusive jurisdiction over actions within its territory, and that governments have no independent obligation to cooperate with one another [5]. Furthermore, even when international or bilateral treaties for mutual legal assistance for cooperation between law enforcement agencies exist, they generally contain exceptions that permit the parties to refuse cooperation under certain circumstances such as to protect sovereignty, security, or similar overriding interests.

At the punishment end of criminal law enforcement, further complication derives from the fact that virtually all extradition treaties contain a "double criminality" requirement that mandates that an extradition request be based on an offense considered illegal under the laws of both the requesting country and the one to which the request is directed. Considering the relatively recent emergence of cyber threats, the varying degrees of appreciation of the threat among the nations of the world, and the absence of common legal structures defining criminal

actions, collective international action against cyber "criminals" is problematic at best. The United States has already faced this difficulty at least twice. During the Persian Gulf War, Dutch hackers who attacked Pentagon computers were beyond the reach of American justice because the Netherlands did not recognize their activities as crimes, and in 1995 an Argentine intruder into sensitive U.S. systems avoided punishment because his country had insufficient computer crime legislation.

The pursuit of infrastructure assurance through liability allocation faces similar obstacles. Liability rules vary between and within countries. Furthermore, a court may not be able to obtain civil jurisdiction over the entity that an injured party may wish to hold liable, particularly as extradition does not apply to civil matters.

Administrative arrangements to achieve infrastructure protection will be complicated by the number and types of organizations involved. At the national level, reaching agreement requires that all parties see the issues with a similar sense of urgency before they will put them on their agendas. Even if some set of nations, most likely the most developed, do agree on the importance of joint action, differing domestic priorities may intervene. Technical standards for system security and safety provide one promising avenue for cooperation, although standards may be seen as an attempt to establish or maintain control of markets as, for example, current debates over the allocation of top-level domain names are seen as attempts by the United States or Europe to exert control over Internet commerce.

The uneven status of privatization and deregulation in telecommunications means that countries have varying mixes of public and private actors in their decision-making processes. Where one country's PTT official may make a decision, another country may rely on executives at several companies, possibly operating under a national regulatory structure.

Differing national concepts of freedom and privacy may also hinder coordinated efforts. National laws and practices differ on such matters as bank secrecy or the necessity to protect personal data. Some governments may be more concerned with regulating the content of communications for political or religious reasons than with protecting the communication networks themselves.

Moving Forward

Obstacles to one are challenges to another, and opportunities to yet another. Thus the preceding is more in the nature of initial and boundary conditions than prohibitions. There seem to be three axes along which progress is needed. The first is to raise the level of consciousness of the issue of infrastructure protection, to place it on the agendas of more developed countries, and to alert developing countries to the possibility that unwise technical and legal "system architectures" can be limiting their potential.

The second is to encourage an understanding of national responsibilities in the matter of infrastructure assurance and protection among international players who share dependencies. To this end, attempts to standardize the criminality of computer intrusions for purposes of investigation and extradition of perpetrators will be helpful.

The third is to start to lay foundations in international law that will be required to achieve effective cooperation between companies, agencies, and nations. Where and how might such efforts be accomplished? There are a number of organizations that could play a role in furthering an international agenda.

For example, the International Telecommunications Union (ITU) sets standards for telecommunications equipment and coordinates national efforts to avoid broadcast interference. A significant characteristic of the ITU is that although its members are nation-states, various companies acting as members of national delegations participate in drafting technical proposals and participate in working groups. It may, therefore, provide a forum for pursuing telecommunications infrastructure protection.

Another institution, the International Civil Aviation Organization, has succeeded in coordinating and harmonizing national aviation policies. This case is particularly interesting because coordinated international action, as illustrated by the Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation, has successfully guided responses to

international terrorism directed against airlines. The signatory nations agreed to recognize attacks against civil aircraft or air navigation facilities as illegal acts and to extradite or try suspected offenders.

Other organizations that can serve as role models or provide direct assistance in enhancing infrastructure protection are Interpol, which promotes international criminal investigation assistance and information sharing; the United Nations; Intelsat; the World Trade Organization; and the Organization for Economic Cooperation and Development, which has already issued guidelines for the security of information systems. The G-8 are trying to address some of these difficulties; last December their justice ministers issued a communiqué calling for improved cooperation in investigations, harmonization of computer crime legislation, and better procedures for sharing information and evidence [1].

Reaching international or bilateral agreements, even when appropriate forums exist, is a lengthy process requiring actions within each potential signatory country and meetings whose only purpose is to agree to meet at some later time to consider the issue, to establish an appropriate process, and to frame the agenda. Such efforts, in turn, require responsible technical communities within each country able to inform debate and assist in analyzing and drafting national positions. It is to one such community that this discussion is addressed.

References

[1] Communiqué, Meeting of Justice and Interior Ministers of The Eight, Washington, D.C., December 10, 1997.

[2] Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washington, October 1997.

[3] Executive Order 13010, "Critical Infrastructure Protection," July 15, 1996, and as amended November 13, 1996. This and other PCCIP-related material can be accessed at <http://www.pccip.gov>.

[4] Greenberg, L.T., Goodman, S.E., and Soo Hoo, K.J., "Old Law for a New World? The Applicability of International Law to Information Warfare," Center for International Security and Arms Control, Institute for International Studies, Stanford University, February 1997.

[5] Greenberg, L.T., "International and Legal Issues of Infrastructure Protection: Is It a Small World After All?" in Soo Hoo, K.J., et al., "Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda," CISAC, IIS, Stanford University, October 1997.

[6] Kyodo Report. Press release by MITI, Tokyo, September 1, 1997.

Readers are encouraged to send comments, suggestions, anecdotes, insightful speculation, raw data, and submissions of articles on subjects relating to international aspects of IT to:

Sy Goodman
CISAC
320 Galvez Street
Stanford University
Stanford, CA 94305-6165

or sgoodman@leland.stanford.edu
fax: (520) 299-4323

Stephen Lukasik (stephen.j.lukasik@cpmx.saic.com), now retired, was director of ARPA, chief scientist of the FCC, and a vice president of Xerox, TRW, and Northrop. Lawrence Greenberg (LawrenceG@fool.com) is general counsel for The Motley Fool, Inc. Seymour

Goodman is director of the Project on Information Technology and International Security, Stanford University.

Appendix B. Program

WORKSHOP ON PROTECTING AND ASSURING
CRITICAL NATIONAL INFRASTRUCTURE:
NEXT STEPS

LAWRENCE LIVERMORE NATIONAL LABORATORY
FEBRUARY 26–27, 1998

THURSDAY, FEBRUARY 26:

WEST GATE BADGE OFFICE

7:30–8:00 Arrival and badging

B132 ROOM 1000

8:00–8:20 Continental breakfast

8:20–8:30 Welcome—*Robert Kuckuck*
Program and logistics—*Stanley Trost*

8:30–8:50 PCCIP Report: Afterward and expectations—*Tom Marsh, David Keyes*

8:50–9:10 Discussion

9:10–9:50 Panel on four "What next?" subject areas—Chair: *David Elliott*
Breakout track co-chairs: *William Crowell, Charles Giancarlo, Elizabeth Banker, Teresa Lunt*

9:50–10:10 Discussion

10:10–10:30 Break and reassembly in breakout rooms

10:30–11:45 Parallel breakout sessions:

The prospective nature of the government-industry partnership needed to deal with the problems of infrastructure assurance and protection.
Track leaders: *Guy Copeland, William Crowell, David Alderson*

Suggesting and rationalizing priorities and timing with regard to the large number of recommendations in the Commission's report.
Track leaders: *Stephen Lukasik, Charles Giancarlo, Kathleen Bailey, Timothy Holliday*

Legal questions relating to the control of networks misuse and government authority for incentives and regulation to obtain more secure infrastructure.
Track leaders: *Elizabeth Banker, Stevan Mitchell, Lawrence Greenberg, Gregory Grove*

Priorities, division of responsibilities, and benefits from near and long term R&D efforts.
Track leaders: *Anita Jones, Teresa Lunt, Steven Rinaldi*

12:00–12:45 Lunch

12:45–2:00 Industry panel: How robust are computer-based infrastructure systems?
Chair: *Edward Feigenbaum*
John Kimmins, Barry Leiner, Donn Parker, Nancy Wong

2:15–3:30 Breakout sessions, continued

3:30–3:45 Break

3:45–5:15 Final breakout session, closure within sessions

5:45–8:00 Reception and dinner
Dinner speakers: *David Keyes* and *Philip Bobbitt*

FRIDAY, FEBRUARY 27:

B123 AUDITORIUM

7:45–8:15 Coffee and tea

8:15–8:30 Welcome—*C. Bruce Tarter*
Program and logistics—*Ronald Lehman*
Introduction to William Perry—*Michael May*

8:30–9:30 Panel on key issues and responsibilities—Chair: *William Perry*
George Spix, Scott Penberthy, Tom Marsh, Philip Bobbitt, David Cooper, Ron Lee, Anita Jones

9:30–9:45 Break

9:45–11:00 Roundtable discussion of key issues and responsibilities—Chair: *William Perry*

11:00–12:00 Lunch

12:00–12:40 Introduction to the keynote speaker—*C. Bruce Tarter*
Keynote address—*Janet Reno, Attorney General of the United States of America*

B170 CONFERENCE ROOM

1:00–2:30 "What next?" panel and discussion—Chair: *Seymour Goodman*
Guy Copeland, Stephen Lukasik, Stevan Mitchell, Anita Jones, Janet Reno

NATIONAL IGNITION FACILITY

3:00 Optional tours of the NOVA/NIF laser facilities

POINTS OF CONTACT:

Seymour Goodman (sgoodman@leland.stanford.edu)
(650)725-2704 or (520)299-5785, for questions regarding the program

Jan Grimm (jgrimm@llnl.gov)
(510)423-5000, for logistical questions

Workshop Organizing Committee: Seymour Goodman, Ronald Lehman II (co-chairs); Janet Abrams, David Elliott, Stephen Lukasik, and Stanley Trost.

Much appreciated staff support was provided by Diane Goodman, Jan Grimm, Timothy Holliday, Karen Kimball, Banani Santra, and Eileen Vergino.

THE PRINCIPAL PARTICIPANTS AND ORGANIZERS:

Janet Abrams is Director of External Affairs and White House Liaison for the PCCIP and for the Transition Team. She joined the Clinton administration as a White House Fellow in 1994, and was with the Office of the Vice President before joining the PCCIP.

Kathleen Bailey is a Senior Fellow on the staff of the Director of LLNL. Previously she served as Assistant Director of the Arms Control and Disarmament Agency (ACDA), and as a Deputy Assistant Secretary of State of the Bureau of Intelligence and Research.

Elizabeth Banker is an associate with Steptoe & Johnson LLP. She is a member of the firm's technology group where her practice focuses on cryptography and electronic commerce. Prior to joining the firm, she served as Assistant General Counsel to the PCCIP.

Philip Bobbitt is Special Assistant to the President for National Security Affairs and Director for Intelligence at the National Security Council. He is on leave from the University of Texas at Austin, where he is a professor of law.

David Cooper is Associate Director for Computation at LLNL. Prior to joining Livermore he was with NASA in several senior positions concerned with high-performance computing. He is on the Presidential Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet.

Guy Copeland is on the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee (NSTAC). He chairs the NSTAC Information Assurance Task Force and co-chairs its National Information Infrastructure Task Force. He also serves with the Information Technologies Association of America and as an executive with the Computer Sciences Corporation.

William Crowell is Vice-President for Product Management and Strategy of Cylink, Inc. Prior to his retirement from government he served as Deputy Director of the National Security Agency, where he acted as the agency's chief operating officer, guiding and directing strategies and policy, and serving as the principal advisor to the Director.

David Elliott was Staff Director for Science and Technology at the National Security Council and then a Vice President at SAIC and SRI. He is now "retired."

Edward Feigenbaum is a Professor of Computer Science at Stanford University. He was Chief Scientist of the U.S. Air Force during the first Clinton administration. Professor Feigenbaum is a recipient of the ACM Turing Award, and is best known for his work in artificial intelligence, most notably in expert systems.

Charles Giancarlo is Vice President for Global Alliances at Cisco Systems, Inc., the major manufacturer of network hardware used for the Internet and other computer-communications networks. His previous position at Cisco was Vice President for Business Development.

Seymour Goodman heads the Information Technology and International Security Program at CISAC at Stanford, and is Professor of MIS at the University of Arizona. He studies the international dimensions of the information technologies and related public policy issues.

Lawrence Greenberg was a counsel with the NSA and Wilson, Sonsini, Goodrich & Rosati, and is now General Counsel for The Motley Fool, Inc. His primary interests are IT-related law and international law.

Anita Jones is University Professor in computer science at the University of Virginia. Previously she served as the DoD Director of Defense Research and Engineering.

David Keyes is the Acting Director of the PCCIP Transition Team, having served earlier as the Commissioner from the Federal Bureau of Investigation. He has held a wide variety of positions with the FBI, including as the Bureau's representative on the Deputy Attorney General's Critical Infrastructure Working Group.

John Kimmins is the Senior Director of the Security and Fraud Solutions organization at Bellcore. His practice is responsible for requirements, standards, incident response, security analysis of services, new technologies and products, and reviews of telecommunications networks. He is a member of the NSTAC.

Robert Kuckuck is Deputy Director for Operations of the Lawrence Livermore National Laboratory. He is a physicist whose prior assignments include heading the laboratory's underground nuclear testing and treaty verification research programs, and creating and leading the University of California Office of Laboratory Administration, which oversees all three of the UC-managed DOE Laboratories.

Ronald Lee is Associate Deputy Attorney General for national security, technology, and cyber matters. He recently joined the Department of Justice from the National Security Agency, where he had been General Counsel.

Ronald Lehman is Director of the Center for Global Security Research at LLNL. Previous positions include Director of the U.S. Arms Control and Disarmament Agency, Assistant Secretary of Defense (International Security Policy), and Deputy Assistant to the President for National Security Affairs.

Barry Leiner is an independent consultant working in distributed system and networking technologies. Previously he had been a Vice President of Microelectronics and Computer Technology Corporation, and before that held several positions with the Defense Advanced Research Projects Agency (DARPA).

Stephen Lukasik is a former Director of DARPA, a former Chief Scientist of the FCC, and has served in various capacities as vice presidents of TRW, Xerox, and Northrop. He is now "retired."

Teresa Lunt is Program Manager for the Information Survivability Program in DARPA. Previously, she was Director of Secure Systems Research at SRI International.

Robert (Tom) Marsh served as Chairman of the Presidential Commission on Critical Infrastructure Protection. He is Chairman of the Board for CAE Electronics, Inc. and for Comverse Government Systems Corp., and serves in various senior capacities for other companies. He is a retired 4-star general whose last assignment was commander of the Air Force Systems Command.

Michael May is Co-Director of CISAC and a Professor of Engineering–Economic Systems and Operations Research at Stanford. He is Director-Emeritus of LLNL. He studies a wide variety of national and international security issues concerned with energy and weapons of mass destruction.

Stevan Mitchell served as the PCCIP Commissioner from the Department of Justice, and continues as a member of the Transition Team. Prior to that, he was a trial attorney with the Criminal Division's Computer Crime Unit.

Donn Parker is one of the "grand old men" of information security, having spent almost thirty years in the field, most of them with SRI. He has written extensively on the subject and is the originator of the I4 service that provides information security due care services to seventy-five of the largest international corporations.

Scott Penberthy is Director of E-Business Technology at IBM.

William Perry is the Michael and Barbara Berberian Professor at Stanford University, with a joint appointment in the School of Engineering and the Institute for International Studies. He was the 19th Secretary of Defense of the United States of America from 1994 to 1997. Previous government service included positions as Deputy Secretary of Defense and as Under Secretary of Defense for Research and Engineering. He was Co-Director of CISAC from 1988 to 1993. Dr. Perry has a long and distinguished history of involvement with American high technology industry.

Janet Reno has been the U.S. Attorney General since March 1993, and is the first woman to hold this office. She served in various legal capacities with both Houses of the Florida State Legislature, was in private practice, and was elected for five terms as State Attorney General for Dade County, Florida. Among the issues of particular interest to her are those relating to alternative forms of punishment for first-time, non-violent offenders; juvenile crime; environmental protection; civil rights; and infrastructure protection.

Steven Rinaldi is military liaison officer to the Office of Science and Technology Policy, Executive Office of the President. He is responsible for a range of military and national security R&D issues, and is the OSTP focal point for critical infrastructure protection R&D.

George Spix is Chief Architect for Consumer Platforms at Microsoft.

C. Bruce Tarter is Director of the Lawrence Livermore National Laboratory. Prior to his selection as Director, he served as Deputy Director and Acting Director. In these roles, he has led the laboratory through the transition to a post–Cold War nuclear weapons world. Dr. Tarter's scientific background is in astrophysics and computational physics.

Stanley Trost is an IEEE Executive Fellow at the FCC. He was formerly a senior staff engineer and head of electronics engineering at LLNL, and chaired the IEEE Committee on Communication and Information Policy.

Nancy Wong served as a PCCIP commissioner from the private sector, where she had been Manager for Information Assets and Risk Management at the Pacific Gas and Electric Company.

Appendix C. List of Participants

Name	Affiliation
Janet Abrams	PCCIP Staff
Dave Alderson	Stanford
Hector Alvarez	California ISO
Massoud Amin	EPRI
Kathleen Bailey	LLNL
Kirk Bailey	Regence Blue Shield
Ken Baker	Office of Nonproliferation and National Security
Elizabeth Banker	Steptoe and Johnson, LLP
James Bean	US Telephone Association
Sharon Belton	Mayor of Minneapolis
Dave Bernstein	Stanford
Tom Berson	Anagram Laboratories
Matt Bishop	University of California, Davis
Philip Bobbitt	National Security Council
Dan Boneh	Stanford
Joseph Bouchard	National Security Council
David Campbell	BBN Systems
Ron Cochran	LLNL
David Cooper	LLNL
Guy Copeland	CSC and NSTAC
William Crowell	Cylink
Kawika Daguio	American Banking Association
Jerome Davis	NoxTech
John Davis	PCCIP
Meiring de Villiers	Stanford
Whit Diffie	Sun Microsystems
Steve Dougherty	California ISO
Jon Eisenberg	NRC
David Elliott	NSC/SAIC/SRI (Retired)
Ed Feigenbaum	Stanford

John Galat	TDEC
Charles Giancarlo	Cisco Systems
Bob Giovagnoni	PCCIP
Dee Goodman	CISAC Staff
Sy Goodman	Stanford and Arizona
Deborah Gordon	Stanford
Lawrence Greenberg	The Motley Fool
Maurice Greenberg	American International Group
Margaret Greene	BellSouth
Jan Grimm	LLNL Staff
Dick Gronet	LLNL
Greg Grove	US Air Force
Bill Harris	PCCIP
Tim Holliday	Stanford
Jeffrey Jaffe	IBM
Anita Jones	University of Virginia
David Jones	PCCIP
David Keyes	PCCIP
Karen Kimball	LLNL
John Kimmins	Bellcore
Fritz Knabe	University of Virginia
Robert Kuckuck	LLNL
Ron Lee	US Department of Justice
Yuet Lee	Bay Networks
Ron Lehman	LLNL
Barry Leiner	ex-DARPA and MCC
Steve Lukasik	retired ARPA, FCC
Teresa Lunt	DARPA
Doug Mansur	LLNL
John Markoff	*New York Times*
Tom Marsh	PCCIP
Michael May	Stanford
Edward McCallum	US Department of Energy
Ann Miller	US Department of Defense
Norman Mineta	IMS Transportation Systems and Services
Stevan Mitchell	PCCIP
Kathryn Moir	BENS
Ernest Moniz	US Department of Energy
Elvin Moon	EW Moon Engineering & Construction Management Industries
John Morgridge	Cisco Systems
Aldo Nevarez	California ISO
Donn Parker	SRI
Scott Penberthy	IBM
William Perry	Stanford
Irv Pikus	PCCIP
Donald Prosnitz	LLNL
Lars Rabbe	Lucent

Victor Reis	US Department of Energy
Janet Reno	US Department of Justice
Steve Rinaldi	OSTP
Paul Rodgers	PCCIP
Ken Rosenblatt	Santa Clara County District Attorney
Howard Schmidt	Microsoft
Larry Schwartz	University of California
Jeannie Seelbach	SRI
Wayne Shotts	LLNL
Kevin Soo Hoo	Stanford
George Spix	Microsoft
Nancy Suski	LLNL
Bruce Tarter	LLNL
Lowell Thomas	US Telephone Association
Mort Topfer	Dell Computer
Stanley Trost	LLNL
Michael Vatis	Associate Deputy Attorney General
Eileen Vergino	LLNL Staff
Elizabeth Verville	PCCIP
Willis Ware	RAND
Floyd Wicks	Southern California Water Company
Larry Wilcher	US Department of Energy
Dean Wilkening	Stanford
Prescott Winter	National Security Agency
Nancy Wong	PCCIP
Joan Woodard	Sandia National Laboratories
Lee Zeichner	PCCIP