CRITICAL INFRASTRUCTURE PROTECTION: THREATS TO PRIVACY AND OTHER CIVIL LIBERTIES AND CONCERNS WITH GOVERNMENT MANDATES ON INDUSTRY

Michael J. O'Neil[*]
James X. Dempsey[**]

TABLE OF CONTENTS

---

[*] Partner, Preston Gates Ellis & Rouvelas Meeds LLP; former General Counsel, CIA.

[**] Senior Staff Counsel, Center for Democracy and Technology, <http://www.cdt.org>.

I. INTRODUCTION

The federal government has identified eight sectors of the economy that it deems critical to the national security and the essential functioning of the United States' economy - telecommunications, transportation, water supply, oil and gas production, banking and finance, electrical generation, emergency services, and essential government functions.[1] These systems have in common their dependence on information systems that are vulnerable to cyber attack.

The vulnerability of critical infrastructures and the unique risks associated with networked computing have been recognized for some time.[2] But the issue was given new urgency by the report of the President's Commission on Critical Infrastructure Protection ("PCCIP") in October 1997, which highlighted the

---

1. REPORT OF THE PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 3-4 (Oct. 1997) [hereinafter "PCCIP Report"] (full text available on the Internet <http://www.pccip.ncr.gov/report_index.html>).

2. *See generally* PETER G. NEUMANN, COMPUTER-RELATED RISKS (1995) (summarizing a diverse range of computer-related risks including many security, safety and reliability problems); NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE (1991) (presenting a comprehensive agenda for developing nationwide policies and practices for computer security). The phrase "electronic Pearl Harbor" was used by Winn Schwartau in Congressional testimony in June 1991. *See* WINN SCHWARTAU, INFORMATION WARFARE 29 (1994) (citing testimony before the House Science Subcommittee on Technology and Competitiveness, June 27, 1991). The General Accounting Office began warning of problems in government computer security at least as early as 1989. *See, e.g.,* U.S. GEN. ACCOUNTING OFFICE, COMPUTER SECURITY: VIRUS HIGHLIGHTS NEED FOR IMPROVED INTERNET MANAGEMENT GAO/IMTEC-89-57 (June 1989). Key GAO recommendations have not been fully implemented. *See, e.g.,* U.S. GEN. ACCOUNTING OFFICE, DOD INFORMATION SECURITY: SERIOUS WEAKNESSES CONTINUE TO PLACE DEFENSE OPERATIONS AT RISK GAO/AIMD-99-107 (Aug. 1999).

topic of critical infrastructures and made a series of specific recommendations for their protection.[3] On May 22, 1998, the President approved a directive, Presidential Decision Directive 63, establishing a national critical infrastructure protection policy and a government framework to develop and implement infrastructure protection measures.[4] Key organizations created in that directive were a National Infrastructure Protection Center ("NIPC"), located within the Federal Bureau of Investigation ("FBI"), with operational responsibilities, [5] and a Critical Infrastructure Assurance Office ("CIAO"), administratively located in the Department of Commerce, which provides planning and coordination support to a National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, who is located in the National Security Council. [6]

---

3. PCCIP Report, *supra* note 1.

4. The PDD itself is classified, but a "White Paper" explaining its key elements is available. *See generally The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Directive 63* (last modified May 22, 1998) <http://www.ciao.ncr.gov/paper598.html>.

5. *National Infrastructure Protection Center: History of NIPC* (visited Nov. 17, 1999) <http://www.fbi.gov/nipc/history.htm >.

6. *Critical Infrastructure Assurance Office: About the CIAO* (visited Nov. 17, 1999) <http://www.ciao.ncr.gov/about.html>.

7. The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection* (2000) (visited Mar. 10, 2000) <http://www.ciao.ncr.gov/National_Plan/national_plan%20_final.pdf> [hereinafter "National Plan"]. Excerpts from an earlier draft of the plan dated June 6, 1999 are available on the Internet. *See* The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection*, June 6, 1999 draft (visited Nov. 17, 1999) <http://www.cdt.org/policy/terrorism/fidnet> [hereinafter "FIDNet draft"]. The earlier draft had generated widespread criticism. *See, e.g., Hearing Before the Subcomm. on Tech., Terrorism and Gov. Info. of the Senate Judiciary Comm.*, 106th Cong. (Oct. 6, 1999) (statement of John S. Tritak, Director, CIAO) [hereinafter "Tritak testimony"]. But the final National Plan was little changed.

On January 7, 2000, the Executive Branch issued its national plan for critical infrastructure protection.[7] The document sets out a ten point program, focused on protection of the federal government's information systems.

The National Plan fails to answer many questions about the relationship between the federal government and industry in protecting privately owned infrastructures. Nonetheless, elements of the government's approach have emerged as the policy has continued to evolve.[8] The various proposals put forward to date reveal a conflict within the Administration between a centralizing tendency that would set uniform standards and link together "intrusion detection" monitoring for all government and private systems versus a more decentralized approach that recognizes the very different standards applicable to government systems and the privately owned and operated networks that comprise most of the critical infrastructures. Support for either approach can be found in the Plan's call for a partnership in which the private sector would share with the government information concerning attacks on private systems and the government would provide the private sector with vulnerability analyses and attack warnings.[9]

Presently, the policy is developing on two tracks: one focused on government systems and one focused on private sector systems. For the former, the government admits that it has much to do to get its own house in order. From the point of view of privacy protection, the policy, as we explain below, has relied to an unwise degree on monitoring government systems rather than on sustained efforts to close the windows of vulnerability known to exist in those systems.

In terms of private sector systems, the program relies, to a large degree, on the voluntary cooperation of the private sector owners and operators of the critical infrastructures with the gov-

---

8. *See* CONGRESSIONAL RESEARCH SERVICE, LIBRARY OF CONGRESS, CRITICAL INFRASTRUCTURES: BACKGROUND AND EARLY IMPLEMENTATION OF PDD-63 10-15 (1999) [hereinafter "CRS Report"].

9. *See* National Plan, *supra* note 7, at 104-18.

ernment agencies tasked to assist in protecting them.[10] The government also intends to increase research and development spending on information assurance, help fund the education of new information security professionals, assist in the development of best practices/security standards, and encourage systems security improvements.[11]

Critical infrastructure protection poses substantial challenges to policymakers because it involves protecting decentralized, privately owned assets. It also risks infringements on individual privacy, especially because it focuses on information and communications systems.

In addressing these issues, we accept two key premises - that the critical infrastructures identified by the government are vital and that they are subject to vulnerabilities because of their reliance on cyber systems. We conclude that an effective infrastructure protection program can be developed while respecting a third premise: that solutions can be developed to protect critical infrastructures that do not erode civil liberties. Furthermore, we recommend that the Administration and the Congress reject monitoring or secrecy measures offered in the name of infrastructure protection that would infringe on civil liberties. Such measures are both unnecessary and unwise.

This article will examine the government's proposals for protecting the U.S. economy's critical infrastructures from potential cyber-attacks. Part II will discuss key elements of the government's policy structure and why clearer explanation of the government's policy is still needed. Part III will discuss threats to individual privacy rights and Part IV will offer recommendations on what should *not* be included in the government's program.

II. THE RELATIONSHIP BETWEEN THE FEDERAL GOVERNMENT AND PRIVATE SECTOR

With the issuance of the National Plan, a number of key elements of the government's infrastructure protection policy have been set forth, but too many others are, as yet, unformed. In

10. PCCIP Report, *supra* note 1, at 19-20.

11. National Plan, *supra* note 7, at 59-72, 104-18.

particular, the relationship between the federal government and the private sector has not been adequately clarified.[12]

A. *The Role of Private Industry*

"Buy in" by the businesses that own and operate critical infrastructures is essential to the success of a policy that depends for its effectiveness on voluntary cooperation by those businesses. If these businesses do not offer their full cooperation, the government is in no position to protect them relying on its own resources alone. A critical step to establishing a sound and acceptable infrastructure protection program is for the government to explain what it expects to bring to the issue that is not already being addressed by private sector security programs.

The infrastructures at issue are largely privately owned.[13] Those private owners have a substantial economic stake in protecting their investments and ensuring the continued operation of their systems against a range of catastrophic threats, both natural and man-made, both intentional and unintentional, from both outsiders and insiders.[14] Those who own and operate these systems are in the best position to understand and prioritize this range of threats and what is necessary to mitigate them.

Industry may benefit from certain information the government possesses regarding threats from hostile foreign nations

---

12. To some extent, this is because the development of the federal government's infrastructure protection program is a work in progress. The National Plan issued in January 2000 promises "subsequent versions" that will address the "specific role industry and state and local governments will play – on their own and in partnership with the Government – in protecting privately owned infrastructures." National Plan, *supra* note 7, at vi. The policy also reflects conflicts apparent within the structure and goals of the program announced to date. For example, instead of the single private sector Information Sharing and Analysis Center (ISAC) called for in PDD-63, plans now call for ISAC's for each infrastructure sector. *See* CRS Report, *supra* note 8, at 8.

13. PCCIP Report, *supra* note 1, at 3-5.

14. *Id.* at 5. The Y2K problem is the most prominent example of an unintentional, man-made threat.

or groups, but it remains unclear what specific information flow from industry to the government would be beneficial to promote industry's protection of its own infrastructures. For the private sector to assess and respond to the government's plan, the government must clearly articulate its priorities and goals and the key means to achieve them.

B. *Private Industry's Cooperation with the Federal Government: The Need for Clear Policy Pronouncements*

1. Information Security Standards

Two examples make the point that the government has not fully clarified its policy. The first concerns the question of standards. There is no lack of information security standards, but there are no good metrics or means of evaluating such standards or devising new and better standards.[15] The U.S. government admits that it does not even have its own house in order; the task of proposing new standards has barely begun and may take several years.[16] For that reason, the government wishes to encourage industry to lead an effort to devise standards.[17] But at the same time, the National Plan indicates that the National Institute for Standards and Technology, the National Security Agency and other federal agencies might work together to initiate such a process, raising the questions of what the government thinks the first step should be and who should take it.[18]

---

15. National Plan, *supra* note 7, at 112-13; Tritak testimony, *supra* note 7.

16. Tritak testimony, *supra* note 7 ("to put our own house in order first"). *See also, Hearing Before the Subcomm. on Tech., Terrorism and Gov't. Info. of the Senate Judiciary Comm.*, 106th Cong. (Oct. 6, 1999) (statement of Jack L. Brock, Jr., Director, Governmentwide and Defense Info. Systems, Accounting and Info. Management Div, GAO, concerning the need for risk-based standards) <http://www.senate.gov/~judiciary/10699jlb.htm>.

17. PCCIP Report, *supra* note 1, at 37-38.

18. National Plan, *supra* note 7, at 30-32, 112-13.

2. Threat Assessments

Second, government officials have stated that the threat of attacks on critical infrastructures is "evolving," such that it is difficult to quantify adequately.[19] This suggests that industry must rely largely on its own assessments of information system vulnerabilities without the benefit of any clear threat assessment from the government. That is, private sector operators of critical infrastructures would be expected to develop defenses without fully understanding what they were defending against. Industry and government assessments may vary on this point, which again suggests the lack of a starting point for discussion or any clear sense of how this is to be accomplished.

---

19. The most complete statement to date on the specific types of threats the government has identified came in October 1999 testimony. *Critical Information Infrastructure Protection: the Threat is Real: Subcommittee on Technology, Terrorism, and Government Information of the Senate Judiciary Committee*, 106th Cong. (Oct. 6, 1999) (testimony of Michael A. Vatis, Director, NIPC) [hereinafter "Vatis testimony"] (visited Nov. 16, 1999) <http:www.senate.gov/~judiciary/10699mav.htm>. *See also, Subcommittee on Technology, Terrorism, and Government Information of the Senate Judiciary Committee*, 105th Cong. (June 10, 1998) (statement of Michael Vatis, Director, NIPC, FBI); *Subcommittee on Technology of the House Science Committee*, 106th Cong. (Oct. 1, 1999) (testimony of Keith Rhodes, Director, Office of Computer and Information Technology Assessment, GAO); *Information Warfare and Critical Information Protection: Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee*, 106th Cong. (Mar. 16, 1999) (testimony of Robert T. Marsh, former Chairman, PCCIP); *Subcommittee on Commerce, Justice, State and the Judiciary of the House Appropriations Committee*, 105th Cong. (Mar. 5, 1998) (testimony of Louis Freeh, Director, FBI).

C. *Role of the FBI*

1. The Protective versus the Criminal Investigative Responsibilities of the FBI

Perhaps one of the most controversial elements of the government's evolving infrastructure protection program is the placement of the National Infrastructure Protection Center at the FBI.[20] This introduces the possibility of conflict between the FBI's new "protective" role in the critical infrastructure program and the FBI's traditional criminal investigative and foreign counterintelligence responsibilities.[21] The FBI obviously has extremely potent investigative and intelligence authorities, which include the authority, pursuant to judicial approval, to wiretap, to conduct searches and seizures, and to serve subpoenas compelling the production of information.[22] These authorities are cited as a key reason for placing the NIPC in the FBI, yet at the same time the government asserts that it will rely on the voluntary cooperation of businesses to obtain much of the information it is seeking in pursuit of its infrastructure protection responsibilities.[23]

2. Defining the Private Sector's Relationship with the FBI

Businesses asked to cooperate in this type of relationship with the FBI will want to have a clear understanding of when the government's focus may shift from voluntary information gathering to a criminal investigative focus, if only because they wish to assess corporate and personal liability. Yet the FBI is not able to provide assurance in such cases, largely because it is wary of

---

20. CRS Report, *supra* note 8, at 11.

21. *Id.*

22. *See* 18 U.S.C. § 2510 et seq., § 3052 (1994).

23. The role of the FBI is discussed in the National Plan, *supra* note 7, at 42-47, 50-51 and 97.

alerting targets of investigation.[24] The resolution of this conflict will require some better explanation. At this point, it appears possible that the intersection of the FBI's two roles may preclude resolution.

One way to minimize potential conflict is to limit strictly the information the FBI collects as part of its protective mission, and indeed the FBI has in some descriptions of its plans emphasized that it presently seeks only points of contact at infrastructure components.[25] However, points of contact can, and likely will, be asked for other information concerning critical infrastructure businesses.[26]

Accordingly, while the FBI should be given a clear lead in investigating attacks on critical infrastructures, both the protection of civil liberties and the need for effectiveness argue that the infrastructure protective mission, and the role of liaison with industry, would best be placed elsewhere.[27]

Even if this conflict of roles could be resolved in a way that promoted cooperative information sharing, it is still likely to heighten industry reluctance to share information. If voluntary private sector sharing of information with government can shift without warning into mandatory cooperation with a criminal investigation, some businesses may prefer to wait until their cooperation is compelled before they proffer assistance. At least at that point they will know where they stand and how the information they provide is likely to be used.

Such caution will be reinforced by the telecommunication industry's experience of working with the FBI to implement the standard-setting process established by the Communications As-

---

24. PCCIP Report, *supra* note 1, at 79. The government's plans emphasize improving information flow to law enforcement, not to the private sector.

25. Vatis testimony, *supra* note 19, at 17.

26. PCCIP Report, *supra* note 1, at 79.

27. In one key area – that of intrusion detection monitoring – this has already occurred, at least as of the end of 1999. The clearinghouse function NIPC was to have performed for government systems has now been transferred to the General Services Administration. *See* Tritak testimony, *supra* note 7.

sistance for Law Enforcement Act ("CALEA").[28] An industry technical standards body spent years developing standards for digital switching equipment to accommodate law enforcement's need for continued ability to perform court ordered wiretaps only to have the FBI reject the effort because it did not contain additional capabilities the FBI had either disavowed or never mentioned at the time the statute was drafted.[29] When the dispute then moved to the Federal Communications Commission ("FCC") for resolution, the FBI attempted a surprise legislative end run to compel industry inclusion of all the additional capabilities, all the while contending before the FCC that the capabilities were already required by the statute.[30] Such surprise maneuvers and the spirit that lies behind them must be opposed. Only a truly cooperative and transparent working relationship between the FBI and the private sector will succeed in advancing the goals of the critical infrastructure policy.

3. Providing Vulnerability Assessments and Warnings of Cyber Attacks to Industry

Another element of the FBI's role in infrastructure protection is to provide vulnerability assessments and warnings of cyber attacks to industry.[31] The NIPC has a complement of cyber warfare specialists and draws on intelligence reporting.[32] Industry would undoubtedly welcome actionable warnings of possible attacks based on intelligence gathered by the government, although the usefulness of its products will be carefully scrutinized. That is because, at this point, it remains unclear what NIPC can bring to

---

28. Pub. L. No. 103-414, 108 Stat. 4279 (Oct. 25, 1994) (codified 47 U.S.C. §§1001 et seq. (1994)).

29. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L. J. SCI. & TECH. 65, 96-99 (1997).

30. John Markoff, *FBI Seeks Access to Mobile Phone Locations*, N.Y. TIMES, July 17, 1998, at A10.

31. Vatis testimony, *supra* note 19, at 17.

32. *Id.*

the table in this regard. The private sector will want to know how NIPC's assistance, provided over time, will differ in quantity and quality from that of established contributors such as the Computer Emergency Response Team at Carnegie Mellon University.[33]

D. *Different Models for Information Sharing*

Two aspects of the information sharing regime government urges upon the private sector require comment. First, the kind of information sought must be well understood. It is hard to determine with specificity exactly what the government wants to know from business. Clearly, the government seeks information about computer attacks on critical infrastructure cyber control systems.[34] Virtually all such attacks are also crimes, and the FBI can be expected to seek a wide range of information necessary to determine damage and assess blame.[35] Both inquiries of this kind and assistance the NIPC might render in improving security after the fact could involve the government's acquisition of information deemed sensitive business secrets by the companies from which they are obtained. If this is so, businesses will expect the FBI to provide clear assurances that the confidentiality of such information can and will be well protected.[36] It is understood that the FBI is developing a security regime to provide such assurances.[37] To be effective, this security regime must be well understood publicly and rigorously applied.

Second, in cases where there is no ongoing investigation, the FBI will seek voluntary provision of information from busi-

---

33. CERT provides a 24-hour service of expert advice on defense and remediation against cyber attacks.

34. National Plan, *supra* note 7, at 113-14.

35. PCCIP Report, *supra* note 1, at 79.

36. *Id.* at 28, 40.

37. *See Protection of Confidential Private Sector Information Within the National Infrastructure Protection Center,* Memorandum from Michael A. Vatis, Chief, NIPC, to Michael J. O'Neil (Sept. 10, 1998) [hereinafter "Vatis letter"] (on file with authors).

ness.[38] The nature of this information has been variously described - from a "mountain of data"[39] to a list of emergency contacts in each critical infrastructure company.[40] There is a need for a better definition of this category of voluntarily provided information and, most importantly, a clear justification for its collection. Here, too, the private sector will wish to know to whom the information it provides will be disseminated, how it may be used and how it will be protected from unauthorized use.[41] Only the government can provide the necessary representations. Without them, its policy will be ineffectual.

For instance, the FBI should provide more public information concerning the operation, and especially the business secrets confidentiality aspects, of INFRAGARD, its rapidly-expanding program in which participating businesses voluntarily share information for critical infrastructure protection directly with the NIPC.[42] Similarly, providing any protocols developed to assure confidentiality would put meat on the bones of the government's proposals for cooperation.

The Financial Services Information Sharing and Analysis Center ("FS/ISAC") seems to offer a much more promising model for sharing of information. Developed by the financial services industry at the prompting of Treasury Department officials, the FS/ISAC is a private sector non-profit corporation formed to facilitate the sharing of information on cyber threats, incidents and vulnerabilities among banks and other financial institutions, without routine involvement of, or forwarding of information to, the government.[43]

---

38. National Plan, *supra* note 7, at 42-46; *see also* Vatis testimony, *supra* note 19.

39. PCCIP Report, *supra* note 1, at 30.

40. Vatis testimony, *supra* note 19.

41. PCCIP Report, *supra* note 1, at 28.

42. National Plan, *supra* note 7, at 44; CRS Report, *supra* note 8, at 9. The NIPC should also explain why INFRAGARD bypasses individual sector ISACs.

43. *See* John Markoff, *New Center Will Combat Computer Security Threats*, N. Y. TIMES, Oct. 1, 1999, at C2.

Under the FS/ISAC, as announced by the Administration in October 1999, information sharing on risks, attacks and responses will be among the private sector members of the financial services industry, not between industry and government.[44] The government is not a direct participant in the system.[45] Information will be shared among member firms, and can be shared in a form that does not even identify the originating institution.[46] No personally identifiable information will be shared, and information will not be forwarded routinely to the government.[47]

E. "*Market Solutions*" *to Infrastructure Protection*

Government descriptions of critical infrastructure plans put some emphasis on the use of indirect, market-based incentives, rather than legislative mandates, to encourage the development of best practices and appropriate information security standards.[48] These mechanisms include the measurement of industry adherence to new information security standards by insurers when writing liability coverage, incorporation of such standards in accounting evaluations, and the influence such standards will exert on the price of corporate financial instruments.[49]

The government's asserted intent to avoid mandates should be applauded, but it remains an open question whether its concepts will bear fruit as anticipated. The key element in all such schemes is information security standards, an area where the private sector may well be ahead of most government agencies. Insurers, accountants, lenders and investors already understand the importance of information security, but until widely accepted standards are established, they cannot play a major role.

This observation only underscores the earlier point concerning how such standards will be developed. The government

---

44. *See* John Markoff, *supra* note 43, at C2.
45. *Id.*
46. National Plan, *supra* note 7, at xxiv.
47. *See* Markoff, *supra* note 43, at C2.
48. PCCIP Report, *supra* note 1, at 40-42.
49. *Id.* at 41-2, 68-9; National Plan, *supra* note 7, at 113.

should both encourage and cooperate with an industry led approach to standards, but must avoid using the standards-setting process as a proxy for government mandates. If such a process is to succeed, it cannot be driven by a government prescription, nor handled from the government end as was the CALEA process, nor can it be required to meet artificial deadlines. Government can best serve such a process by continuing to seek consensus among business, Congress and the public about the need for critical infrastructure protection. The increased research and development spending in fiscal year 2000 can also be directed in ways that aid the standard-setting process, although we are unaware of the extent to which industry associations or groups were consulted in setting priorities for this spending.

III. PRIVACY AND OTHER CIVIL LIBERTIES CONCERNS

Clear explication is also needed to address the privacy and other civil liberties concerns that are legitimately raised whenever the government proposes expanding its role vis-à-vis rapidly evolving information infrastructures that handle an ever-increasing amount of sensitive personal and business information. The burden rests with the government to justify both the purpose for, and the use to which, any expansion of information gathering will be put, particularly in the area of communications protected by statutes.[50]

The effort to protect critical infrastructures will be severely hampered if it becomes – or is perceived to have become – a Trojan horse for civil liberties infringement. Take, for example, the PCCIP's recommendation of the adoption of key recovery encryption, a form of encryption in which the encryption key, or means of rendering enciphered text into plain text, is retained by a third party agent. [51] This recommendation was strenuously opposed by privacy advocates because it diminishes the confidence, and therefore the privacy protection value, users can place in commercial encryption products.

---

50. *See, e.g.*, 18 U.S.C. § 2510 et seq.; 18 U.S. C. § 2703(d)(1994).

51. PCCIP Report, *supra* note 1, at 74-75.

The PCCIP did itself and the infrastructure protection issue a disservice when it endorsed key recovery. This decision could be seen as a cynical effort by the Administration to advance its position on a surveillance issue that has little or nothing to do with infrastructure protection and everything to do with the attempt to preserve wiretapping and computer evidence seizures used in law enforcement investigations unrelated to critical infrastructures. While the Administration has since announced major revisions in its encryption policy,[52] the early introduction of key recovery into the critical infrastructure debate suggests a willingness to exploit the issue for unrelated (even contradictory) purposes. Adding divisive elements to an already complicated discussion of critical infrastructure policy will only add to the difficulty in encouraging acceptance, because it distracts attention from the principal policy issue and siphons off attention and political energy to a different and controversial topic.

. The notion that the government needs greater authority to monitor communications or the Internet should be strongly resisted. The National Plan disavows any intent to seek any greater monitoring authority than is now available under existing statutes.[53] The FBI has stated that it could perform all current and projected NIPC operations under current law.[54] Given concerns raised by the Administration's monitoring proposals, these assurances of adherence to current law say more about the inadequacy of current law than about the wisdom of the Plan's monitoring proposals.

---

52. Jeri Clausing, *In a Reversal, White House Will End Data-Encryption Export Controls*, N. Y. TIMES, Sept. 17, 1999, at C1; Peter S. Goodman and John Schwartz, *U.S. to End Curb of Secrecy Software*, WASH. POST, Sept. 17, 1999, at A1. *See Center for Democracy & Technology: U.S. Encryption Policy* (visited Mar. 3, 2000) <http://www.cdt.org/crypto/admin> (describing the new policy direction in documents released by the Administration).

53. National Plan, *supra* note 7, at 12, 40-41; Tritak testimony, *supra* note 7 ("FIDNet ... will confer no new authorities on any government agency").

54. Vatis letter, *supra* note 37.

A. *Monitoring Proposals*

Although the essence of the government's partnership with private sector infrastructures is voluntary cooperation, significant proposals that are not voluntary and that raise privacy concerns have been a major part of the government's approach from the beginning. For instance, the PCCIP recommended the establishment of an "early warning and response capability" to protect government and private sector telecommunications networks against cyber-attack.[55] The Commission said that such a capability should include: (1) a means for near real-time monitoring of the telecommunications infrastructure; (2) the ability to recognize and profile system anomalies associated with attacks; (3) the capability to trace, re-route, and isolate electronic signals that are determined to be associated with an attack.[56]

In the summer of 1999, the monitoring concept emerged fully conceptualized under the name of the Federal Intrusion Detection Network ("FIDNet").[57] As first proposed, FIDNet was a government-wide system that depended on artificial intelligence "intrusion detection" software to monitor contacts with sensitive government computers in an effort to identify suspicious behavior, feeding "anomalies" to a central analysis unit at the Federal Bureau of Investigation's NIPC.[58] The draft plan indicated that FIDNet would eventually be extended to private sector systems as well.[59]

---

55. PCCIP Report, *supra* note 1, at 91.

56. *Id.* The concept of monitoring communications networks also was approved at the December 1997 meeting of the Justice and Interior ministers of the G8. In their final communiqué, the ministers agreed that, "To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence." Meeting of Justice and Interior Ministers of the Eight, *Communiqué* (Dec. 10, 1997).

57. FIDNet draft, *supra* note 7, at 58; *see* John Markoff, *U.S. Drawing Plan That Will Monitor Computer* Systems, N.Y. TIMES, July 28, 1999, at A1.

58. FIDNet draft, *supra* note 7, at 58-59.

59. *Id.* at 58.

It is noteworthy that the public and the Congress learned of FIDNet not as a result of an open consultative process but as a result of a casual and premature disclosure by a government official.[60] With all due respect to the Executive Branch's prerogative to conduct internal deliberations, this was not the best way to make national policy on such an important issue. Congress, public interest organizations and private industry should have been consulted sooner on the details of the proposal. And their concerns should have been given greater weight. The proposal generated a storm of protest from civil liberties advocates and Members of Congress, as well as skepticism from computer security experts, and it was changed in some respects since the initial draft, but FIDNet continues to occupy a central role in the National Plan.[61]

FIDNet, as described in the National Plan is a government-wide system using artificial intelligence "intrusion detection" software to monitor contact with non-Department of Defense ("DOD") government computers in an effort to identify suspicious behavior.[62] It was modeled on a DOD system.[63] Intrusion detection monitors installed on individual systems or networks are to be "netted" or linked to a central analysis unit so that patterns across systems could be identified and all sites could be warned of an intruder or intrusion technique used at one site.[64] As first proposed, data from the network of sensors would have been provided to the FBI's NIPC, but in the final Plan, the central analysis unit is at the Federal Computer Incident Response Capability in the General Services Administration ("GSA").[65]

FIDNet is to be installed at "critical systems."[66] The Plan does not clearly define what would be considered a critical sys-

---

60. *See* Markoff, *supra* note 57, at A1.

61. National Plan, *supra* note 7, at xix-xxi, 13-14, 37-42.

62. *Id.* at 39.

63. *Id.* at 38.

64. *Id.*

65. *Compare* FIDNet draft, *supra* note 7, at 59, *and* National Plan, *supra* note 7, at 39-40.

66. National Plan, *supra* note 7, at 39.

tem nor does it designate who would determine what were critical systems. The Plan states that FIDNet "focuses on attacks upon Federally owned, non-public networks or domains,"[67] but that covers all Web sites and email addresses ending in ".gov." The Phase One agencies that have been designated as having the highest priority systems include the Departments of Health and Human Services, Commerce, Transportation, and Treasury and the Environmental Protection Agency.[68] A crucial milestone comes in October 2000, when the Plan seeks to have 22 critical Federal sites connected to a pilot FIDNet; the specific nature and identity of those sites will be a crucial signal of how FIDNet is developing.[69]

The Plan clearly recognizes the civil liberties implications of FIDNet, and insists that it will adhere to applicable privacy laws, but at the same time makes clear that such laws do not pose an impediment to FIDNet: "[a] preliminary legal review by the Justice Department has concluded that, subject to certain limitations, the FIDNet concept complies with the Electronic Communications Privacy Act ("ECPA")."[70] Under the Plan's reading of ECPA, the owner of a system is allowed to monitor use of its own system in order to protect itself, and, if sufficient notice is provided, a user is deemed to consent as a condition of use to any monitoring that may occur, including monitoring conducted by another entity (the GSA in the case of FIDNet).[71]

The Administration has gone to some length to assure the public that FIDNet is a limited system. In a "budget amendment" submitted to Congress by the President in September 1999, the Administration sought $8.4 million for the GSA to create "a new centralized capability ... in the area of intrusion detection and response."[72] The funding would have allowed the GSA to pay for

67. National Plan, *supra* note 7, at 13.

68. *Id.* at 25.

69. *Id.* at 42.

70. *Id.* at 14.

71. *See* 18 U.S.C. § 2701-02 (1994).

72. Letter from William J. Clinton, President to the Speaker of the House of Representatives (Sept. 21, 1999). H.R. DOC. NO. 106-129 (1999).

additional technology in the form of intrusion detection systems and personnel to analyze anomaly data to identify and respond to attacks and to prepare alerts on attack warnings.[73] The budget amendment was careful to minimize the role of the FBI and claim respect for privacy:

> Attack and intrusion information would be gathered and analyzed by agency experts. Only data on system anomalies would be forwarded to GSA for further analysis. Law enforcement would receive information about computer attacks and intrusions only under longstanding legal rules, where an agency determines there is sufficient indication of illegal conduct. The private sector is not linked in any automated or other new way to GSA under this program.[74]

FIDNet failed to achieve Congressional support in Fiscal Year 2000. Yet efforts to establish FIDNet are proceeding. Those within the Administration who favor development of a widespread, centralized system of monitoring for government and private sector communications systems continue to push their vision. Short of a complete Congressional ban on use of any funds for intrusion detection, there is a need for continued oversight within the Executive Branch and by Congress and the public. Moreover, this oversight must be institutionalized; it cannot depend on leaks or the occasional flare-up of publicity.

B. *Legal Standards: Fourth Amendment Protections and Technological Developments*

The debate on FIDNet and the accompanying debate on encryption policy have highlighted the need for a broader look at the legal standards governing the monitoring of communications and government access to data stored on networked computers. In

---

73. H.R. DOC. NO. 106-129 (1999).

74. *Id. See also,* Tritak testimony, *supra* note 7 (stating, "FIDNet will be run by the GSA, not the FBI; will not monitor any private networks or email traffic; will confer no new authorities on any government agency; and will be fully consistent with privacy law and practice.").

the National Plan, the Administration emphasized that FIDNet will be "fully consistent with privacy law and practice."[75] Yet, it is becoming increasingly apparent that current law has failed to keep pace with technological developments and therefore that current "privacy law and practice" fall far short of traditional Fourth Amendment standards.

1. Current Privacy Law

Today, if the government wants to search your home to obtain your computer hard drive or a disc containing stored data, it must secure a judicial warrant issued on probable cause and it must provide you with contemporaneous notice of the search by serving you with a copy of the warrant.[76] This is traditional Fourth Amendment law.[77]

Since the 1968 federal wiretapping statute, popularly known as Title III,[78] the government, seeking to intercept telephone conversations as they occur, must also seek a warrant based on probable cause, but the search and seizure proceeds surreptitiously.[79]

If the government seeks to obtain your e-mail communications, the rules are more complicated. E-mail not more than 180 days old may be seized by the government from a service provider without contemporaneous notice with a warrant based on a showing of probable cause.[80] This has been the law since enactment of the 1986 Electronic Communications Privacy Act.[81] However, under ECPA, if the email is older than 180 days, a sub-

---

75. National Plan, *supra* note 7, at 40. *See also* Tritak testimony, *supra* note 7.

76. FED. R. CRIM. P. 41.

77. Richards v. Wisconsin, 520 U.S. 385 (1997); Wilson v. Arkansas, 514 U.S. 927 (1995) ("knock and announce cases").

78. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (codified at 18 U.S.C. §§ 2510 – 2522 (1994)).

79. *Id.*

80. 18 U.S.C. § 2703(a) (1994).

81. Pub. L. No. 99-508, 100 Stat. 1861 (Oct. 21, 1986).

poena or court order will suffice. [82] In the case of a subpoena, which is issued without prior judicial approval, the government must only claim relevance to an administrative or criminal matter.[83] And if the government or a private sector service provider is monitoring its own system, current legal standards offer little reassurance, for the ECPA gives service providers wide latitude in monitoring and intercepting communications on their own systems to protect their rights or property.[84]

2. Privacy Law for the New Technology

i. Networks and the Internet

Meanwhile, a major technological development is underway: the movement of information out of people's homes or offices and onto networks. While most computerized information used to be stored locally on disks and hard-drives, the Internet offers considerable incentives to store information on networks, so that it can be accessed remotely from any location. This trend gives rise to difficult questions under the Fourth Amendment.[85] Information stored on a computer in your home or office is entitled to full Fourth Amendment protection, but the courts have held in a number of situations that when individuals give information to a third party, they lose constitutional privacy rights in

---

82. 18 U.S.C. § 2703(b) (1994). The legislative history says very little about why stored e-mail has full Fourth Amendment protection only for 180 days. *See* H.R. REP. NO. 99-647 (1986); S. REP. NO. 99-541 (1986).

83. 18 U.S.C. § 2703(b)(1)(B)(I) (1986); *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE, § 4.13 (3d ed. 1996).

84. 18 U.S.C. § 2702(b) (1994).

85. The Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

it.[86] With the rise of networking, this problem is exacerbated. Do people have a constitutionally protected privacy interest in their calendars stored on Internet Web sites? In their data on remote servers they do not own or control? In passwords or decryption keys stored with third party recovery agents? At best, the answers are unclear.

ii. The Cyberspace Electronic Security Act (CESA)

The Fourth Amendment privacy issues at the intersection between critical infrastructure protection and Internet privacy came to the fore with the Administration's announcement in September 1999 of its new encryption policy.[87] The White House's announcement spoke of three pillars of its new approach to commercial encryption: greatly lessened export controls, strong emphasis on critical infrastructure protection, and government access to plaintext of encrypted communications and stored data.[88] The means to achieve the latter was draft legislation entitled the Cyberspace Electronic Security Act ("CESA").[89]

CESA would allow the government to obtain encryption "keys" or other decryption information from third parties under a court order issued upon a finding that (1) such keys are necessary to obtain access to the plaintext of encrypted communications or data, and (2) there is no constitutional expectation of privacy in that plaintext, or any privacy interest has been overcome by consent, warrant, order or other authority.[90] In other words, if the government could by any lawful means get access to communi-

86. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976) (holding bank customer has no Constitutional privacy interest in his cancelled checks held by his bank).

87. Clausing, *supra* note 52, at C1.

88. *Id.*

89. *Analysis, The Cyberspace Electronics Security Act of 1999* (last modified Sept. 13, 1999) <http://www.cdt.org/crypto/CESA/CESArevfact sheetanalsys.shtml> [hereinafter CESA] (Department of Justice section-by-section analysis).

90. *Id.*

cations or data, it could obtain a court order compelling production of any decryption information that has been entrusted to a third party. In the section-by-section analysis accompanying the draft bill, the Department of Justice made it clear that it saw no constitutional expectation of privacy in any storage arrangement with a third person absent a confidentiality provision.[91] Even where such a confidentiality agreement existed, the government maintained that it could be overcome, and access to encryption data could be compelled, on a minimal showing in many cases.[92]

iii. Concerns with the CESA

The government's rationale for enacting CESA exposes how little privacy protection the government believes is accorded to information stored with third parties and how little protection encryption could provide if decryption information is in the hands of third parties.[93] The legislation is premised on the assumption that sensitive personal information being stored increasingly in networks and on the Web has no legal expectation of privacy.

Yet this legal theory ignores the reality of the technology involved. It is now possible to purchase a range of inexpensive, user-friendly, and virtually unbreakable encryption products. So, it is *reasonable* to expect that use of such products to protect one's data would prevent unauthorized access. Because possession of an encryption key is tantamount to disclosure of the data itself, it is also reasonable to expect that the legal bar ought to be set rather high in determining when the government should get access to that secret. The legal theory underlying CESA also ignores the technological trends toward hand-held computers with Internet access and other mobile devices that access the data stored on networks, trends that mean that information may come

---

91. *See* CESA, *supra* note 89.

92. *Id*

93. *Id.*

more and more to be stored in configurations not protected by the Fourth Amendment.[94]

The challenge raised by CESA is to draft government access standards that map the privacy protections of the Fourth Amendment onto the emerging networked environment. As a result of technology, personal data is moving out of the desk drawer and off of the desktop computer and out onto the Internet. However, it should not be the end of the privacy debate to say that this technological change takes information outside the protection of the Fourth Amendment. To stop there would leave the Fourth Amendment protections available in the home when increasingly information is not stored there anymore. Rather, it is necessary to adopt legislative protections that give to information on networks the same level of Fourth Amendment privacy protections that it would have in the home.

Perhaps, the best analogy is to a safe deposit box. If the government seeks something stored in a safe deposit box, it must obtain a search warrant to open the box. If, instead, what the government seeks is records stored with a third party but protected with an effective, off-the-shelf encryption program the government cannot break, and the decryption key is entrusted for safety to another third party, the government should have to meet the same warrant requirement to unlock the encryption. Under the Department of Justice's theory, it never has to show probable cause, let alone give notice to the record subject.[95]

iv. Updating ECPA

It is time to ask whether the statutory privacy standards Congress established in 1986 in ECPA remain the right choices for today, given the increased reliance on networking and the

---

94. *Compare* Katz v. United States, 389 U.S. 347, 350 (1967) (stating that the Fourth Amendment "protects people, not places") *and* United States v. Miller, 425 U.S. 435 (1976) (judging whether privacy expectations are "reasonable" based on where, with whom and how information is stored and accessed).

95. *See* CESA, *supra* note 89 at § 203, adding a new 18 U.S.C. § 2712(b).

trend towards storage of data outside the home and office. The government ought to meet the same standard for access to the encryption key as for the underlying information and in both cases the protection ought to be the full protection accorded by the Fourth Amendment to records that remain in the possession of their creator. The application process could be a unitary one, under which the government would go to the well but once to obtain a search warrant for access to specific information and the means by which to decipher it. This would be particularly appropriate in cases where data and the encryption key were held by different parties. It would also serve to underscore the importance that society ought to be placing on privacy enhancements, while at the same time ensuring that government has the appropriate tools for investigating cyber crime.

Law enforcement will argue that tightened privacy protections in the area of encryption will diminish further current access to potentially crucial information held by terrorists, spies, narco-traffickers and money launderers. However, information protected by encryption ought generally to be given the protection of a probable cause warrant requirement if the encryption key is held by a third party under a secrecy agreement, the circumstance covered by CESA. Such arrangements are likely not going to be favored by either terrorists or drug dealers for the very reason that their data would be reachable by search warrant and out of their direct control.

There will be those who say that this proposal exceeds constitutional norms of privacy protection. It will be argued that, if a person's records are held by a trusted third person, the expectation of privacy inherent in those records is diminished by virtue of their being in another's hands.[96] But technology is changing and, unless Congress acts, the constitutional norms of privacy will be increasingly irrelevant because, while the Fourth Amendment will protect the home, little sensitive data will be stored there. There is need for statutory privacy protection of data stored on networks as a technical substitute for storage in the home.

---

96. United States v. Miller, 425 U.S. at 449.

C. *Additional Privacy and Civil Liberties Issues*

In the case of all the infrastructures, personnel security issues raise serious privacy concerns. The Employee Polygraph Protection Act[97] was adopted to address documented limitations of the polygraph and a long record of abuses.[98] It limits most private employers' use of the polygraph. The presidential commission report recommended weakening the Act's protections.[99] Similarly, the report evidenced a general dissatisfaction with the rules on access to and use of criminal history records for personnel background investigations.[100] These rules have been forged and refined over the years to provide protections against misuse of records that are frequently incomplete, inaccurate or otherwise unreliable.[101]

Secrecy is another concern. The Freedom of Information Act[102] ("FOIA") is a vital component of our democratic system of openness and governmental accountability that allows citizens to obtain a wide range of public records. Over the past decade, tremendous effort has been devoted to decreasing the amount of unnecessarily classified information.[103] In many respects, the strength, economic vitality, and innovation in new communications technologies are supported, not hindered, by openness. Therefore, amendments to the FOIA or increased use of the national security information classification system would raise seri-

---

97. 29 U.S.C. §§ 2001 et seq. (1994).

98. *See* SEN. REP. NO. 100-284, U.S. Code Cong. and Admin. News 726 (1998).

99. PCCIP Report, *supra* note 1, at 88.

100. *Id.*

101. STAFF REPORT ON THE DISSEMINATION OF FBI CRIMINAL HISTORY RECORDS FOR EMPLOYMENT AND LICENSING PURPOSES, *reprinted in* DISSEMINATION OF FBI ARREST RECORDS FOR EMPLOYMENT AND LICENSING PURPOSES: HEARINGS BEFORE THE SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS OF THE COMMITTEE ON THE JUDICIARY, HOUSE OF REPRESENTATIVES, 100TH CONGRESS, FIRST SESSION, OCTOBER 14 AND 21, 1987 (1988).

102. 5 U.S.C. § 552 (1994).

103. *See, e.g.*, Exec. Order No. 12,958, 3 C.F.R. 333 (1995 Comp.).

ous concerns by diminishing public access to information in the hands of the government. These concerns are heightened by the risk that statutory changes would be subject to overbroad interpretation.[104]

At the same time, corporations have a right to protect their proprietary information.[105] Corporate information can be protected without increased use of the classification stamp or FOIA amendments. It is especially noteworthy that FBI officials have concluded that existing FOIA law generally suffices to protect confidential private sector information submitted to the NIPC as part of its infrastructure protection work.[106] This places a heavy burden on any federal agency that would propose a change to the law. FBI officials have also said that they seek no expansion of classification authorities.[107] Nonetheless, it remains a concern that the possible use of *existing* authority needs to be clarified by the FBI and other federal agencies.

IV. WHAT CRITICAL INFRASTRUCTURE PROTECTION SHOULD NOT INCLUDE

Privacy concerns and the threat of government regulation pose serious impediments to industry and public acceptance of the government's critical information protection proposals. Government officials, Members of Congress, academics, the private and public interest community, industry associations, and the corporations that operate critical infrastructures share the responsibility of developing sound infrastructure protection policies that can be implemented without compromising privacy and other civil liberties. The following "don'ts" should be incorporated

104. *See* ALLAN R. ADLER, LITIGATION UNDER THE FEDERAL OPEN GOVERNMENT LAWS 8 (20th ed. 1997).

105. The Freedom of Information Act allows protection of trade secrets. 5 U.S.C. § 552(b)(4) (1994). Federal criminal law penalizes the theft of trade secrets. *E.g.*, 18 U.S.C. §1831 *et seq.* (1994 & Supp. III 1997).

106. Vatis letter, *supra* note 37.

107. *Id.*

clearly in the government's official descriptions of its infrastructure protection plan.

First, there should be no government compulsion of information sharing by the private sector. The voluntary nature of industry participation in infrastructure protection schemes is vital to the credibility of the government's approach.[108] Because the private sector built and operates these infrastructures, it understands them best and must lead any effort to improve their security.

Second, there should be no mandated security fixes imposed by government. There are already strong market forces to encourage good security practices and industry already leads in such developments.[109] Unless government also proposes to subsidize corporate budgets, this type of planning must be left to those who must also run the systems to be protected.

Third, the government has never run critical infrastructures and should not try to begin to do so. Thus, the government's protective role should not include directing protection or prevention measures; rather it should be limited to encouraging and advising protection and preventive measures and then only if the government has unique knowledge or expertise.

Fourth, there is neither a practical need nor a legal mechanism for government monitoring of private sector information networks to protect critical infrastructures. Any such proposal would offend both constitutional and legal guarantees of privacy and individual rights. If intrusion detection is the goal, this is a function that must be designed and controlled by infrastructure owners and operators.

Fifth, there is no need for the use of polygraph tests for personnel involved in the operation of critical infrastructure com-

---

108. PCCIP Report, *supra* note 1, at 21.

109. These include the imperative to protect against crippling losses that computer system failures can cause, as well as the fiduciary responsibility each officer of a corporation bears for the prudent protection of the corporation's assets and business operations.

panies. Federal and state laws already regulate the use of this device for personnel security checks.[110]

Sixth, there is no need for the imposition of national security information classification controls or government personnel security rules in private sector companies operating in critical infrastructures. Systematic use of classification does not easily lend itself to private sector commerce and would add unnecessary costs and reduce efficiency, particularly in crises.[111] The FBI, which will be the repository of sensitive business information acquired by the federal government for infrastructure protection, has stated that it sees no need for amendments to the FOIA.[112]

The government has not offered justification of any kind for changes in the protections of the FOIA,[113] the Privacy Act,[114] the ECPA,[115] the Computer Security Act,[116] the Employee Polygraph Protection Act,[117] or the Federal Advisory Committee Act.[118] Were any such proposals for statutory change to emerge, they should be the subject of public hearings by the committees of jurisdiction, just as the underlying laws they would amend were originally subject to extensive examination and debate. Unfortunately, recent significant changes to the federal laws have been accomplished by evading this process and the public debate it fosters. A notable example is the amendment expanding the use of "roving" wiretaps, which was added to the conference report

---

110. *E.g.*, 29 U.S.C. § 2001-2006 (1994).

111. *E.g.*, Federal rules relating to the handling of classified information require thorough background investigations for all cleared personnel, storage only in special approved containers, extensive record keeping, etc. *See, e.g.*, Exec. Order No. 12,958, 3 C.F.R. 333 (1995 Comp.).

112. Vatis letter, *supra* note 37.

113. 5 U.S.C. § 552 (1994).

114. 5 U.S.C. §552a (1994).

115. 18 U.S.C. § 2701 *et seq.* (1994).

116. Pub. L. No. 100-235, 101 Stat. 1724 (1988) (codified at 15 U.S.C. §§ 272, 278g-3 (1994)); 40 U.S.C. § 759 (1994).

117. 29 U.S.C. § 2001 *et seq.* (1994).

118. Pub. L. No. 92-463, 86 Stat. 770 (1972) (codified at 5 U.S.C.App. § 2 (1994)).

on an intelligence authorization act even though it had been approved by neither chamber.[119]

VI. CONCLUSION

Three policy questions dominate the issue of critical infrastructure protection - what should the government's role be; what is adequate infrastructure security and how will appropriate standards be determined; and what data does the government need from business and why. None seems fundamentally settled, if only because policy continues to develop. There are more questions than answers.

Nonetheless, a few basic principles are emerging that should guide infrastructure protection efforts. These principles include:

(1) General or centralized monitoring of communications need not and should not be a chief or central component of the government's response to computer security. There are other activities — notably the identification and closing of existing vulnerabilities — that should be given higher priority.

(2) Authority for increased monitoring of information systems is not required and should be rejected. Rather, the underlying laws for monitoring communications systems and accessing stored data should be strengthened.

(3) The role of the FBI and the National Security Agency in computer security should be carefully limited: it has been demonstrated that their surveillance agendas trump their protective missions, and their activities are often so cloaked in secrecy as to generate understandable suspicion.

(4) Oversight of infrastructure protection should be institutionalized within the Executive Branch and should be accessible to the public. There should be established within the Executive Branch appropriate mechanisms for oversight of computer

119. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2397, 2413 (codified as amended at 18 U.S.C. § 2518(11)(b) (1998)).

security issues, involving both industry representatives and privacy advocates.

(5) Congress must follow this issue carefully, and should insist upon periodic reports on the status, scope, and effectiveness of critical infrastructure activities, with special focus on monitoring and intrusion detection initiatives and the protection of privacy.

(6) While it is acknowledged that there is a need for government participation, especially in educating society about what is at stake, the government's role should be limited and largely advisory. The private sector should set information security standards, and the government should clearly define and limit what information it seeks from businesses and how that information will be used.