ELECTRONIC PRIVACY INFORMATION CENTER

Critical Infrastructure Protection and the Endangerment of Civil Liberties

An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)

Electronic Privacy Information Center
Washington, DC

About the Electronic Privacy Information Center

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a project of the Fund for Constitutional Government. EPIC works in association with Privacy International, an international human rights group based in London, UK and is also a member of the Global Internet Liberty Campaign, the Internet Free Expression Alliance and the Internet Privacy Coalition.

The EPIC Bookstore provides a comprehensive selection of books and reports on computer security, cryptography, the First Amendment and free speech, open government, and privacy. Visit the EPIC Bookstore at http://www.epic.org/bookstore/.

First edition 1998

Printed in the United States of America

ISBN: 1-893044-01-7

EPIC Staff

Marc Rotenberg, Executive Director
David L. Sobel, General Counsel
David Banisar, Policy Director
Shauna Van Dongen, Publications Director
Kathleen Ellis, Administrative Director
Wayne Madsen, Senior Fellow, Principal author of this report

ACKNOWLEDGEMENTS

The Electronic Privacy Information Center gratefully acknowledges the support of the Fund for Constitutional Government, the C.S. Fund, the Scherman Foundation, the Rockefeller Family Fund, and the Stern Family Fund as well as the assistance of members of the EPIC Advisory Board.

Preface

More than ten years have passed since adoption of the Computer Security Act. That law, which was intended to ensure that issues of computer security not be held hostage by government secrecy, has remained more a goal than a result. For more than a decade, administrations of both parties have sought to limit government accountability and to extend government secrecy.

The cost of these efforts to expand government control over computer security have been enormous: a failed encryption proposal, expanded wire surveillance, short-sighted technical standards to facilitate monitoring, and lack of trust and confidence in government's ability to defend proposals in open forums among technical experts.

The most recent dangers to civil liberties comes from the new-found threat to our nation's infrastructure. An elaborate report identified a whole series of attacks that terrorists could wage against our communication lines, power grids, and transportation networks. Not surprisingly, perhaps, the report recommended a dramatic expansion of government authority, new funding to combat the threat, and greater secrecy to conceal potential vulnerabilities as well as the work of the government agencies now tasked with defending us.

Taken on its face, there is a real question of whether the PCCIP report adequately evaluated the dangers to our Nation's security. The PCCIP report largely ignored the Y2K problem, now seen as the greatest threat to our nation's infrastructure by experts, industry, and the general public. The PCCIP also ignored the extraordinary damage that could be caused by natural disasters such as the ice storm that crippled large parts of southern Canada during the winter of 1998.

Natural disasters, computer errors, and network vulnerabilities are very real threats that we must consider in a society that is ever more dependent on advanced technologies. To view all dangers

through the lens of terrorist attack, invariably hides from view many of the practical problems we should consider.

But there is another, perhaps more disturbing aspect of the PCCIP report. Almost every solution proposed by the commission represents some new expansion of government authority and some new encroachment into personal liberty. These recommendations follow from the description of a potential problem with barely a moment to consider the consequences for our form of open government.

In each of the areas touched on by the PCCIP Report - privacy, freedom of information, open government, censorship, security classification, Internet monitoring and surveillance, encryption, and the authority of the FBI - it is necessary to examine carefully the proposals of the PCCIP and consider the potential harm to open government, personal liberty, and agency accountability.

Regarding privacy, our view is that there is no need to expand workplace surveillance or weaken the protections established by the Employee Polygraphy Protection Act. We would further oppose any efforts to limit the application of the Freedom of Information Act or the Federal Advisory Committee Act. Not only do we object to the proposals to expand classification authority as envisaged by the PCCIP report, we believe that there is more than ample evidence to support further declassification of information held in federal agencies.

It is worth emphasizing that it was the Freedom of Information Act that helped identify many of the problems with the government's proposed Clipper encryption scheme - errors in design, management and adoption - that might have remained classified if not for the presumption of government accountability firmly established by the FOIA.

The PCCIP proposes the development of a large-scale monitoring strategy for communications networks. Borrowing techniques that have been applied to hostile governments and foreign agents, the PCCIP brings the Cold War home with an open-ended proposal to conduct ongoing surveillance on the communications of American citizens. We believe that the Electronic Communications Privacy Act of 1986 should be strengthened to prohibit such surveillance.

The PCCIP also continues the failed policies of the past, urging the adoption of key escrow encryption scheme even after technical experts have demonstrated its flaws and foreign governments have rejected this approach. But in the key escrow recommendation, one is given an important insight into the nature of the PCCIP effort. For even proponents of key escrow have acknowledged that it poses a significant risk to network security and creates new sources of vulnerability that could otherwise be avoided.

The PCCIP, which was established to identify measures to protect the Nation's critical infrastructure against attack, seems quite prepared to sacrifice this critical goal when the return is greater surveillance capability.

Here finally we reach the critical thrust of the PCCIP effort - a proposal to extend the reach of law enforcement, to limit the means of government accountability, and to transfer more authority to the world of classification and secrecy. These proposals are more of a threat to our system of ordered liberty than any single attack on our infrastructure could ever be.

Openness, not secrecy, remains the key to a nation's security and its future prosperity.

Marc Rotenberg
Executive Director
EPIC

Washington, DC
October, 1998

Table of Contents

EXECUTIVE SUMMARY

On July 15, 1997, President Clinton signed Executive Order 13010, which established the President's Commission on Critical Infrastructure Protection (PPCIP). The Executive Order listed eight sectors that the PCCIP was to examine for security vulnerabilities. They are: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government.

President Clinton appointed retired Air Force General Robert T. Marsh to chair the PCCIP. Although the commission, its Steering Committee, and its Advisory Committee were composed of members of government and industry, the membership of the three bodies consisted of a majority of military and intelligence representatives. Appendix B lists the military and intelligence affiliated members.

PCCIP's report, issued in October 1997, contained many recommendations that have the potential to curtail a number of important civil liberties, including freedom of speech and freedom of information. Although the report concluded there was no evidence of an "impending cyber attack which could have a debilitating effect on the nation's critical infrastructure," it did recommend a new bureaucratic security establishment with expansive authority. If not properly monitored and controlled, these new national security structures and intelligence-sharing networks, in addition to those that already exist, may, instead of protecting the national infrastructure, be used by the government and private corporations to further erode the privacy of U.S. and foreign citizens.

Duane Andrews, a former top Pentagon official who is an executive Vice President at Science Applications International Corporation (SAIC), a large intelligence and military contractor, sees no practical difference. He stated, "A large international bank has exactly the same problems and challenges as the Defense Department." However, columnist Bill Frezza writes, "Maybe I'm overreacting, but the intentional blurring of civilian and military computer security concerns -- each legitimate in its own right -- smells fishy . . . both United Airlines and the U.S. Air Force employ skilled mechanics to keep their planes in the air. So what? I don't recall the Air Force telling United Airlines that it is insufficiently informed to make rational decisions about flying. And if our government is so worried about commercial security, why has the Clinton administration become the single biggest impediment to the adoption of strong encryption?" Not coincidentally, Andrews served as the chairman of the Pentagon's Defense Science Board Task Force on Information Warfare.

In response to the PCCIP's report, on May 22, 1998, President Clinton signed two Presidential Decision Directives - PDD 62 (*Combating Terrorism*) and PDD 63 (*Critical Infrastructure Protection*) - designed to defend the nation's critical infrastructures from various threats, including "cyber attacks" by computer hackers and terrorists. The White House summary of these two PDDs is contained in Appendix A. PDD 63 carried out most of the recommendations contained in the Report of the President's Commission. These include the establishment of several new boards and agencies, some with Internet surveillance authority. One of the new offices is the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism within the National Security Council. This office is headed by Richard Clarke, a person who has spent a number of years in intelligence-related functions. Clarke reports to the President through the Assistant to the President for National Security Affairs.

PDD-63 also authorized the creation of a National Infrastructure Assurance Council (consisting of private sector and state and local government representatives), a National Plan Coordination (NPC) staff, the Critical Infrastructure Assurance Office (CIAO) (headed by Jeffrey Hunker), the Critical Infrastructure Coordination Group (CICG), and the National Infrastructure Protection Center (NIPC) under the FBI. Of most alarm is the fact that the NIPC may be assisted in its Internet surveillance activities by the Department of Defense and the U.S. Intelligence Community. The NIPC is headed by Associate Deputy Attorney General Michael Vatis.

In addition, PDD-63 encourages private industry to establish an Information Sharing and Analysis Center (ISAC). However, the Federal government is authorized to facilitate the start-up of the ISAC. Many observers believe that the NSA's Information Warfare Technical Center in Fort Meade, Maryland, has the right embryonic structure for the proposed ISAC. Such a facility, located within the structure of one of the world's most intrusive intelligence agencies, would constitute a grave threat to the privacy of not only law-abiding American citizens but citizens of other countries as well.

The Pentagon/NSA Angle

> Congress has a "particular obligation to examine the NSA, in light of its tremendous potential for abuse. ... The danger lies in the ability of NSA to turn its awesome technology against domestic communications."
>
> Sen. Frank Church

The Department of Defense and its secretive component, the NSA, were the driving forces behind critical infrastructure protection. They convinced the administration that it was necessary to defend the infrastructures of the United States in order to further offensive and defensive information warfare contingencies -- notions partly drawn up by think tanks like the RAND Corporation and hyped by Hollywood screen writers. In fact, some computer experts interviewed by Reuters claimed the "threat is more Hollywood than hard fact." They added that some information security companies are using information warfare as a catalyst for more security software and gadgetry by exploiting the fear associated with a cyber-attack. The same phenomenon exists with the feared Year 2000 calamity.

For the Pentagon and the intelligence community, information warfare offered a new vista in an era of post-Cold War diminishing military budgets, paucity of conventional threats, base closures, and reductions in force of both military and civilian employees.

The Backdrop of NSDD-145

The information security component of critical infrastructure protection - namely the withholding of what the government deems is "sensitive" information in the private sector - has roots in the Reagan administration. It is important to examine the policy decisions then in order to understand what is driving the current critical infrastructure and information warfare initiatives.

Responsibility for computer security standards within the civilian government had, until 1984, been assigned to the National Bureau of Standards (NBS). During the 1970s, NBS became a pivotal player in the development of computer security standards, particularly the widely accepted Data Encryption Standard (DES). The result of these developments was that NSA faced unprecedented competition from a civilian agency within the Department of Commerce in the area of encryption technology.

On September 17, 1984, NSA prevailed upon President Reagan to sign National Security Decision Directive 145 (NSDD-145). The directive authorized NSA to develop means to protect "unclassified sensitive" information. For the first time in its thirty-two year history, the NSA was assigned responsibilities outside its traditional foreign eavesdropping and military and diplomatic communications security roles. The agency was granted new powers to curb the use of public cryptography and to develop standards and techniques for automated systems security. In addition, NSDD-145 permitted NSA to control the dissemination of government, government-derived, and even non-government information that might adversely affect the national security. Some argued that such a broad definition included *all* information. NSA quickly began to exercise its new-found authority.

The directive also stated that NSA was to act as the government's focal point for information security and as such was to:

> . . . review and approve *all* standards, techniques, systems and equipment for telecommunications and automated equipment security.

NSA also put pressure on the continued viability of DES when it announced that it would no longer certify DES products used by the government after 1988. Ignoring NBS's role within the civilian government agencies, NSA mandated the use of its own secretly-developed encryption algorithms - as part of a program called the Commercial COMSEC Endorsement Program or CCEP - by all government agencies. On November 5, 1986, National Security Adviser John Poindexter, who was embroiled in controversy stemming from the Iran-Contra scandal, further expanded NSA's information security role when he signed National Telecommunications and Information Systems Security Policy (NTISSP) No. 2. Officially titled "Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated Information Systems", Poindexter's directive extended NSA's mandate to the protection of unclassified sensitive information in the commercial data bases of private corporations. NSA found itself in charge of a program that was at variance with the Constitution and its Bill of Rights.

At about the same time, NSA began lobbying against two bills in Congress that were aimed at

curtailing NSA's influence in the civilian government and commercial sectors. House Resolutions 2889 and 145 reinforced NBS's authority over the security civil government computer systems and networks by enshrining it in public law. National Computer Security Center director Patrick R. Gallagher, Jr., in a December 22, 1986 letter to Donald C. Latham, the Pentagon's Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and the Chairman of the National Telecommunications and Information Systems Security Committee (NTISSC), reported that his staff "provided support for [the] lobbying effort that successfully blocked HR 2889 from passage by the 99th Congress." NBS and certain members of Congress were eyeing NSA's computer security center, hoping to move it from NSA to NBS along with a budget approaching $1 billion. HR 145, also known as the Computer Security Act of 1987, ultimately fared better than HR 2889, but, it too, faced the same antagonistic NSA lobbying effort.

In testimony before the Chairman of the House Government Operations Committee in February 1987, the NSA director, General William Odom, was questioned on NSA congressional lobbying by the committee chairman Jack Brooks of Texas. Brooks asked Odom, "Did NSA officials contact private companies to gather support for NSA's opposition to HR 2889 or HR 145? If so, did you authorize these efforts?" Odom answered in writing that "NSA has no knowledge that any of its employees initiated contact with private companies for the purpose of gathering opposition support against HR 2889 or HR 145." Brooks' line of questioning was prompted by reported Congressional lobbying on NSA's behalf by officials and agents of one of its main computer security evaluation contractors, the MITRE Corporation, and by one of its major computer vendors, Digital Equipment Corporation (DEC). In replying to a question from Representative Gerald Kleczka of Wisconsin on whether NSA staff members lobbied against the bill, Odom was a bit more forthcoming. He responded, "The answer is yes, sir. It's not the sense of the word that you used, ëlobby.' It's a sense of talking to Members of the Congress as we do on all sorts of legislation . . ."

Brooks made it quite clear to General Odom what he thought of NSA's computer security lobbying efforts on the Hill when he asked the NSA chief, "Are you aware that it is illegal, against the law, for Government officials to use appropriated funds to lobby Congress on a piece of legislation? Odom replied, "Yes, sir."

Most irksome for Brooks were official visits made by NSA, FBI, and CIA agents to U.S. companies that provided on-line access to computer databases. NSDD-145, in creating a new information category called "unclassified but sensitive," made commercial providers of such information subject to government security controls. One of the largest database providers visited by the government intelligence agents was Dialog, at the time the largest on-line vendor of data in the world. Dialog controlled around 270 databases that contained both commercial and government information.

Brooks then called Latham to testify. The chairman made known his feelings about NSDD 145:

> . . . one of the most ill-advised and potentially troublesome directives ever issued by a President. First, it was drafted in a manner, which usurps Congress's role in setting national policy.
>
> Second, the directive is in conflict with existing statutes which assign to the Office of Management and Budget, the Department of Commerce, and the General Services Administration the sole responsibility for establishing government-wide standards, guidelines and policies for computer and telecommunications security.

> Finally, I seriously question the wisdom of the President's decision to give DOD the power to classify, hence control, information located in civilian agencies and even the private sector which, in DOD's opinion, may affect national security.

Latham, in his testimony, denied that he or anyone else in the NTISSC group had any plans to impose controls on unclassified information in the private sector. However, on November 11, 1986, six days after Admiral Poindexter issued his directive establishing the "unclassified but sensitive category," Diane Fountaine, Latham's Pentagon assistant, shocked a meeting of the Information Industry Association by confirming that the Reagan administration wanted to restrict access to public databases.

In fact, Latham was enforcing both NSDD-145 and the Poindexter Directive to the letter. In September 1986, this resulted in a visit by an NSA official to the headquarters of Mead Data Central in Columbus, Ohio. Mead operated two well-known repositories of data - NEXIS, a well-spring of news from the U.S. and foreign press, and LEXIS, a source data for court cites and other legal data. Describing computer data bases as threats to national security, Latham said, "I'm very concerned about what people are doing -- and not just the Soviets. If that means putting a monitor on NEXIS type systems, I'm for it. The question is, how do you do that technically without interference?" NSA soon began investigating ways to eavesdrop on computer communications without being detected. The perfect method would be to use a computer program to surreptitiously monitor data base requests for particular categories of information. A user who would conduct a data base search using such keywords as "nuclear weapons", "stealth technology", or "National Security Agency" could activate such monitors, alerting the NSA about the database requests. For the NSA, the agency that had pioneered the development of text and voice keyword recognition systems, the monitoring of data base queries would not be an insurmountable task.

Marc Rotenberg, the former counsel for Senator Patrick Leahy's Subcommittee on Technology and Law Senate (and present director of EPIC), later testified before the House Subcommittee on Legislation and National Security that NSA's visits to private companies "leaves open the possibility that any Federal agency could request that the NSA undertake an assessment of any information system maintained by a Federal contractor." He urged the Congress to limit the authority of the NSA in computer security and to establish adequate means for public accountability. He also recommended in 1989 that Congress begin public hearings on the role of encryption technology in computer security. "Discussions about cryptography must become public discussions, regardless of the agencies involved."

Industry's Refusal to Cooperate

The NSA and Pentagon visitors to Mead Data Central were not only interested in stemming the flow of technical data to the Soviets and others, but also in trying to co-opt Mead to provide information on their Soviet bloc clients. Mead would have nothing to do with such a deal. Company president Jack W. Simpson refused to become a snitch for the intelligence community, declaring, "They would control GI Joe dolls as militarily significant if they could get away with it." Gerald Yung, Mead's general counsel, affirmed that "our clients are confidential."

Lockheed Dialog's General Counsel Robert A. Simons broke with the Pentagon and NSA and questioned the government's activities: "Will we all need a passport to enter a public library?" Simons' boss, Dialog President Roger Summit, said "I don't know under what authority it [control of private data bases] would be implemented." Likewise, Kenneth B. Allen, the vice president for government relations of the Information Industry Association, the trade group of

commercial data base companies, criticized the administration's stance: "We think it is dangerous for the government to censor or restrict the flow of information," adding, "We're just looking at the opening salvos here." In light of the recent critical infrastructure and information warfare initiatives, Allen's words could not have been more prophetic.

The Computer Security Act

Despite the opposition of NSA and the Pentagon, Congress passed the Computer Security Act of 1987. The House Report on the legislation notes that NSDD 145 "raised considerable concern within the private sector and the Congress." One of the principal objections to the directive was that

> it gave NSA the authority to use its considerable foreign intelligence expertise within this country. This is particularly troubling since NSA was not created by Congress, but by a secret presidential directive and it has, on occasion, improperly targeted American citizens for surveillance.

Spurred to passage by Senators Patrick Leahy and Lawton Chiles and by Representatives Jack Brooks and Dan Glickman, Public Law 100-235 firmly established the role of the NBS (later renamed the National Institute of Standards and Technology or NIST) in establishing security standards for computer systems and networks processing unclassified information. But NSA still maintained a hook into the unclassified sector -- one that it would begin to exploit to the maximum extent possible. The Computer Security Act called for NIST to draw on NSA for "technical assistance" in particular areas, especially cryptography.

In 1989, NSA and NIST signed a Memorandum of Understanding (MOU). The memorandum effectively returned to NSA many of the powers rejected by the Computer Security Act. The MOU contained several key goals that were to NSA's benefit, including: NSA providing NIST with "technical security guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data;" NSA "initiating research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods"; and NSA being responsive to NIST "in *all* matters related to cryptographic algorithms and cryptographic techniques including *but not limited to* research, development, evaluation, or endorsement." The MOU was signed in March 1989 by Vice Admiral William O. Studeman, Odom's successor as NSA director, and Raymond G. Kammer, NIST's acting director and a disciple of NSA principles. NSA, once again, re-established its cryptographic hegemony within the government. Cynically, Studeman wrote a letter to Congressman John Conyers in June 1989 stating that it was NSA's "fondest desire . . . to work with NIST to start the momentum toward increased fielding of technology, standards, and guidelines in pursuit of PL 100-235 objectives."

The Clipper Conundrum

By early 1993, NSA was, once more, clearly in the driver's seat in protecting computerized information in the civil government sector. It, along with its allies in the Justice Department and FBI, sold the incoming Clinton administration on the technology of escrowed encryption. Most notable was the "Clipper Chip", a backdoor in digitized telephone scrambling programs that permitted law enforcement and intelligence agencies to listen in. The national firestorm that erupted forced many traditional NSA hidden agendas into public view, a situation which NSA found increasingly uncomfortable.

NSA's escrowed encryption proposals, the FBI's "Digital Telephony" proposals to give it virtual real-time access to the nation's digital telecommunications network, and the Clinton administration's continuation of arcane "munitions" export controls on acceptable strength cryptography, continued into the critical infrastructure protection debate. Within the business community, there is an underlying suspicion of government intentions, particularly in the computer and telecommunications industries. The privacy and civil liberties communities are inherently suspicious of administration intentions after witnessing a panoply of intrusive and anti-privacy measures being introduced in proposed legislation or by administrative fiat.

From Clipper to Information Warfare

Control of cryptography is important to NSA but there is another area in which the agency has always wanted to stake a claim -- computer intelligence. Throughout the late 1980s, a group of computer intruders operating out of Hannover, West Germany were discovered to be breaking into the computer systems of U.S. and foreign government agencies and corporations. Furthermore, the hackers were found to be acting on behalf of the Soviet KGB. This incident gave NSA and other intelligence agencies the opportunity to expand their charters. In the spring of 1991, during Desert Storm operations in the Gulf, computer hackers from The Netherlands accessed U.S. military computers connected to the Internet. In all, some thirty-four DOD sites were penetrated according to the General Accounting Office (GAO). In testimony before the Senate Subcommittee on Government Information and Regulation, GAO official Jack L. Brock, Jr. revealed that "at many of the sites, the hackers had access to unclassified, sensitive information." The use of the term "unclassified, sensitive information" was a windfall for NSA. It could confidently resurrect the tenets of NSDD-145 by arguing that it was necessary to protect such information, even though it was available via the publicly-accessible Internet.

NSA, however, still faced some wary members of Congress who were reluctant to expand NSA's powers in contravention of the Computer Security Act. In November 1991, Senator Herb Kohl, the chairman of the Senate subcommittee on Government Information and Regulation, sent a letter to Commerce Secretary Robert Mosbacher, in which he wrote that he held the Commerce Department, not NSA, responsible for the break-in by Dutch teenage hackers into the DOD computers containing "sensitive" information. Kohl also stated that "if the provisions of the Computer Security Act were followed these break-ins would be much less likely to happen." The senator urged Mosbacher to "make computer security a higher priority at the Department of Commerce."

Regardless of Kohl's stance, NSA was determined to take control of the protection of unclassified but sensitive information. In July 1994, NSA's new director, Vice Admiral Mike McConnell, wrote a letter to Senator Ernest Hollings, a key member of the Senate Appropriations Committee, declaring that "the threat to these [computer] systems is real . . . network/computer protection within DOD is a fundamental readiness issue and the need for security products is immediate."

But NSA was clearly looking for new reasons for existence. With the collapse of the Soviet Union, the Warsaw Pact, and a shrinking U.S. military budget, NSA's huge infrastructure and budget were being eyed by anxious budget-cutters. After the closure of NSA eavesdropping stations from Iceland to Alaska, NSA was clearly in search of an expanded mission that would supplement its signals intelligence and communications security responsibilities. Computer intelligence-gathering and computerized digital countermeasures were the answer. The term "information warfare" was coined and the NSA saw it as a natural area in which to assume responsibility.

By 1994, NSA positioned itself to become the top government information warfare-fighting agency. Because many government officials were not exactly sure what "information warfare" was, since no one had ever actually fought one, the Defense Department decided to come up with a definition. According to DOD, information warfare involves "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information and information systems."

NSA set about to influence the information warfare proposals that were being drawn up by a Defense Science Board information warfare panel that met during the summer of 1994. The panel's findings would have a great deal of influence on President Clinton's emerging information warfare policy doctrine. Fortunately for NSA, the information warfare panel of the study group was chaired by a former Reagan administration official, Donald Latham, who was then working for Loral Federal Systems, a large intelligence community contractor.

To consolidate its position, NSA approved the creation of the Defensive Information Warfare Program within the Defense Information Systems Agency (DISA) - a component of the Pentagon. By doing so, NSA was staking the same claim to "Infowar" that it had already established for "Infosec" within the DOD infrastructure. Information warfare also extended DOD's responsibilities in disseminating disinformation, a technique mastered by the KGB during the Cold War. The significant impact of an information war on the international media is clear. Thomas Czerwinski, a professor at the School of Information Warfare and Strategy at the National Defense University in Washington, prophesied about an information war when he asked, "What would happen if you took Sadaam Hussein's image, altered it, and projected it back to Iraq showing him voicing doubts about his own Baath Party?" But the same technology could also be used to discredit democratically-elected leaders with whom the United States disagreed. DOD's move into the area of disinformation, morphing software, perception management, and censorship potentially pits its "cyber warriors" against the nation's "cyber libertarians."

War on Information

Charles Swett, a Pentagon official in the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, warned in 1995 that "the political process is moving on to the Internet." Swett charged that the Zapatista National Liberation Front was lying in their Internet communiqués in claiming the Mexican army had raped and killed children in Chiapas. Swett also argued that the Pentagon should begin scanning "left-wing" news on Internet sites in order to keep track of political activists operating domestically and abroad. However, the Pentagon has a vested interest in trying to eliminate the Zapatista presence on the Internet. The U.S. Army's Special Forces have been involved in training Mexico's army in counter-insurgency operations against the Zapatistas, a group which has only been deemed terrorist by the Mexican oligarchy, New York banks and securities firms, and U.S. military and intelligence officials. In June 1995, then-CIA director John Deutch accused "terrorists" of using the Internet for their own communications. In addition, the Defense Intelligence Agency (DIA) maintains a list of 70 "rebel" Web sites.

Unfortunately, the DIA is involved in psychological warfare operations with several unsavory governments in helping them quell "rebel" movements. Many of these movements are considered "terrorist" only in the eyes of dictatorial regimes supported by the U.S. military. Freedom movements around the world, like the Zapatistas in Chiapas, the Tibetans, East Turkestanis, Bougainvilleans, Chechnians, West Papuans, Iranian Mojaheddin, Kurdistanis, Chinese democrats, and East Timorese, are using the Internet to communicate information about the

horrific situation in their lands. The Pentagon's information warriors have made a habit of confusing Internet activism by such groups with "cyber-attacks." For example, in May 1998, the U.S. information warfare structure announced that the Liberation Tigers of Tamil Eelam, a group fighting for independence from Sri Lanka, had successfully launched a cyber-terrorist assault on Sri Lankan computer systems. In reality, the attack was nothing more than a counter-propaganda e-mail flooding of Sri Lankan embassy web sites. In an annual survey of terrorist incidents, the State Department charged a Tamil group called the Internet Black Tigers with "suicide e-mail bombings" of Sri Lankan web sites. The Tamil group, far from engaging in anything so dramatic, was merely trying to counter Sri Lankan propaganda directed against the Tamils. Using the Pentagon's and State Department's lexicology, one could equate the posting of anti-government banners and posters on a government building as a form of terrorism.

Many experts scoff at the notion that the Internet is vulnerable to terrorist attack. According to Neil Barrett, a principal consultant of Europe's Groupe Bull, "terrorist groups are not using the Internet for anything more than propaganda and internal communications." Barrett also stated that there is a lot of exaggeration over what constitutes a cyber terrorist attack. He cited one case in which an Internet chess club web site was attacked by hackers -- the intrusion was later described as a terrorist attack. Similarly, when the Pentagon alleged that its computer systems were subjected to 250,000 hacker intrusions, it failed to mention that all but 500 of these were mere Internet "pings", a sort of inquiry that can be generated by a search engine looking for information on "nuclear weapons", "missiles", or "chemical warfare", all subjects that would be contained in the Pentagon's Internet-connected systems. However, such search engine "pings" hardly constitute cyber-terrorist attacks.

The Congress should consider measures aimed at preventing the U.S. military and intelligence community, particularly the CIA, DIA, FBI, and NSA from engaging in activities aimed at disrupting the free flow of human rights information on the Internet. Specifically, Internet intelligence-sharing between the United States and nations that violate human rights should be strictly restricted.

The information warfare proponents also seek to spread disinformation via the Internet. The Pentagon and intelligence community have traditionally used such tactics as "spoofing" the airwaves with false messages and distributing propaganda through television and radio broadcasts, air dropping of leaflets, and planting of false stories in foreign newspapers and magazines. For example, the U.S. Air Force Special Operations Command maintains six EC-130 aircraft (code-named Commando Solo) that are designed to broadcast propaganda to civilians over AM, FM, shortwave, and television frequencies. These aircraft have been used in military operations in Saudi Arabia, Turkey, Bosnia, Haiti, Panama, and Grenada. In addition, U.S. Army psychological operations propaganda specialists publish the weekly *Herald of Peace* newspaper in both Serbian and Croatian, which is distributed throughout Bosnia. The Pentagon planners feel that if another country or group resists U.S. policy they are fair game for a propaganda assault. In a paper written for the U.S. Air University, U.S. Air Force Colonel Richard Szafranski maintains that "Information warfare is hostile activity directed against any part of the knowledge and belief systems of an adversary." The use of the Internet for similar disinformation and propagandizing during peacetime could potentially violate laws and U.S. Information Agency regulations intended to shield American citizens from such manipulation and deception. These laws and regulations should be revisited by Congress in consideration of future critical infrastructure protection appropriations.

The March of the Info-Warriors

NSA has put its service cryptologic elements to work on information warfare. The Army got a head start in 1990 when its Signal Warfare Center at Vint Hill Farms, Virginia began soliciting companies to propose the development of destructive computer viruses, self-reproducing malicious computer instructions contained in computer memory that can, if properly programmed, destroy information stored in a computer. The Army, a pioneer in the development of deadly biological viruses at its Fort Detrick, Maryland germ warfare facility, was interested in developing surreptitious programs to launch at an enemy's computer systems and networks, perhaps transmitting destructive computer codes by radio. Computer security specialists warned that such research could potentially backfire against a computer aggressor. Many reasoned that the United States was more vulnerable to the potential "bounce back" effect of such viruses. Nevertheless, NSA's military components began to ready their computer terminals for information warfare.

For example, the Army created its information warfare center at Fort Belvoir, Virginia. Known as the Land Information Warfare Activity (LIWA), it is co-located with the Army Intelligence and Security Command, the Army component of NSA's Central Security Service (CSS). According to a LIWA spokesperson, the Army is "looking beyond the land battle with information warfare initiatives and new technology."

In 1996, the Air Force established its Information Warfare Center at Kelly Air Force Base, Texas. This activity is co-located with the Air Intelligence Agency, the Air Force component of NSA's CSS, and the NSA's Medina Annex Regional Signals Intelligence (SIGINT) Operations Center (RSOC).

The Naval Information Warfare Activity at Fort Meade, Maryland, is located with the Naval Security Group Command, the Navy component of the NSA's CSS. In addition, the Navy's Fleet Information Warfare at the Navy's Atlantic Fleet headquarters in Norfolk, Virginia, is developing new methods for information warfare.

Armed with a new mission of defending against a cyber-attack, NSA further eroded the provisions of the Computer Security Act by offering its services to numerous federal agencies, including the Department of Interior, National Aeronautics and Space Administration, and the Department of the Treasury. For example, NSA penetration teams tried to access unclassified computer networks at NASA to probe the vulnerabilities of satellite control, launch control and other operations. Even more alarming was the fact that the General Accounting Office (GAO), the congressional watchdog agency that is tasked with ensuring federal agencies are complying with laws like the Computer Security Act, asked NSA to conduct the penetration testing of NASA, an agency which clearly falls under the purview of NIST.

The intelligence community and Pentagon also ensured a body of congressional champions of information warfare advocates and supporters. Chief among them are Senator Jon Kyl, whose Subcommittee on Technology, Terrorism, and Government Information has held numerous hearings featuring "gloom and doom" witnesses complaining that the nation is one the verge of an "electronic Pearl Harbor" and even more distastefully, an "electronic Oklahoma City."

CRITICAL INFRASTRUCTURE PROTECTION IMPACT AREAS & COUNTER-RECOMMENDATIONS

The PCCIP Report contains a number of proposals that could, if implemented, adversely affect the freedom of American citizens. Many of the proposals affecting the ability of Americans to

engage in scientific and other research, as well as political and social discourse, without being subjected to government security controls, are a direct outgrowth of similar proposals advanced by President Reagan's NSDD-145.

Privacy

The PCCIP Report complains that because private sector employers do not have access to criminal history, financial, and employment information and also may incur tort liability for releasing adverse employment information to other employers, the private sector should be granted limited exemptions from these restrictions. The Report recommends that federal and state laws be amended to "balance employers' needs against individual interests in privacy." Such a recommendation is frightening in light of reports that companies are increasingly monitoring the communications of their employees. The degree to which companies may be required or encouraged to hand over the contents of such communications to the FBI's National Infrastructure Threat Center also poses significant civil liberties concerns. Many companies currently possess and use monitoring capabilities. A MacWorld survey revealed that 22 per cent of large companies "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." Only one-third of these companies informed employees that such surveillance was taking place. A 1997 survey by the American Management Association showed that more than 35 per cent of employers use surveillance tactics such as reviewing e-mail, inspecting computer files, or eavesdropping on phone conversations.

The Report also recommends that state legislators amend their privacy laws to require mere implied "consent" as authority for employers to request sensitive background information on employees or prospective employees. In addition, there is a recommendation that Congress amend the Employee Polygraph Protection Act to include information security personnel in the category of professions which can be required to be subjected to polygraph tests.

Freedom of Information, Open Government, and Censorship

The PCCIP Report recommends that the Critical Infrastructure Assurance Office (CIAO) established by PDD-63 require appropriate protection for specified private sector information. It, therefore, proposes to require that the Freedom of Information Act (FOIA) exemptions of paragraph b (3) be broadened to include "sensitive information" from the private sector.

At a partially-open meeting of the Advisory Committee to PCCIP held on December 3, 1997, Steve Mitchell from the Justice Department called for a "cultural change" to take place over the next 15 to 20 years in order to deal with the information warfare threat. He called for FOIA exemptions under both Federal and state law for companies passing on proprietary information to government agencies. He also said state FOIAs, in particular, should be amended because they are often more liberal than the Federal law on opening up government documents and files to the public. Mitchell also called for some form of Federal Advisory Committee Act (FACA) relief for joint government-private sector boards and committees. He said this would permit sensitive but unclassified meetings to be closed to the public.

Another aspect of information warfare involves censorship and disinformation. According to a report written for the Pentagon by SAIC, "widespread dissemination by the U.S. media and its independence vastly complicate military operations. Any information warfare strategy must taken into account the press or *at least* address its potential impact."

Former NSA director and CIA deputy director Studeman stated that there should be a "rapid

media reaction force" charged with disseminating propaganda to various media channels and outlets for "positive purposes". Studeman is currently the Vice President and Deputy General Manager of TRW's Systems and Information Technology Group, another contractor with a vested interest in critical infrastructure protection. Studeman also serves on the Board of Directors of Thiokol Corporation, formerly headed by PCCIP Commission Chairman Marsh.

Congress should ensure that the FOIA and FACA are not amended in any way that would inhibit the public's right to access unclassified information held by the government, regardless of the information's origin.

New Security Classification Category

The PCCIP Report recommends that the CIAO classify new categories of information such as "aggregated" unclassified information. It also recommends that the President use his Executive Order fiat authority to require federal agencies to identify purposes for publishing certain information and "ensure the information is published in a format that minimizes the likelihood it will be used in ways that are incompatible with infrastructure assurance." Creating new classification categories and restricting the dissemination of certain unclassified information to the public was a cornerstone of NSDD-145 and was rejected by the Congress.

In March 1997, the Commission on Protection and Reduction of Government Secrecy, headed by Senator Patrick Moynihan, concluded that there is too much classified information held by the federal government. Instead of calling for an expansion in the ability of federal agencies to classify information, as called for by the Marsh Commission, the Moynihan Commission recommended legislation to establish principles on what information can be classified, determine what information should not be classified, specify how long information should remain classified, and create a national declassification center to provide annual reports on the progress in declassifying government records. In April 1997, after the issuance of the Moynihan Commission report, President Clinton stated, "I think there is too much secrecy in the government and I think too many people have too much unfettered discretion just to declare documents secret."

The actions taken by President Clinton and the PCCIP to facilitate the establishment of new categories of "unclassified sensitive" and "aggregated sensitive" information are clearly at variance with the President's own public comments on limiting government secrecy. The administration should institute policies that are designed to limit the ability of agencies to classify documents, not extend such authority as called for in the PCCIP Report.

Internet Monitoring and Surveillance

In its Information Warfare (Defense) Report to the Undersecretary of Defense, the Defense Science Board (DSB) calls current technology to monitor the National Information Infrastructure (NII) inadequate. The report recommends that an "investment" be made in developing a distributed monitoring and surveillance strategy for large scale networks. Large scale intelligence agency and law enforcement monitoring of the Internet is also suggested in the DSB report. Specifically, the report states "The Internet provides potential for access to rich repositories of open source information." It further states that there are constitutional impediments to using the Internet for espionage: "IC (Intelligence Community) access to the Internet raises difficult questions and serious concerns about conflicts between law enforcement, intelligence activities, and constitutional guarantees." In the debate over the mandatory use of escrowed encryption, the balance between government access to decrypted data and privacy rights - something the Clinton

administration calls "equities" - always appeared to favor access over privacy rights. The DSB report seems to suggest that a similar "equity" situation exists with regard to espionage on the Internet. If past administration balances are considered, it would appear that intelligence and law enforcement espionage on the Internet outweighs the requirement to maintain constitutional guarantees. The Electronic Communications Privacy Act of 1986 should be strengthened to restrict massive government-led or government-inspired Internet surveillance in the name of "infrastructure assurance."

Encryption

The mandatory use of escrowed encryption/key recovery technology is an inherent part of the current critical infrastructure protection proposals. The PCCIP Report states that "establishment of trustworthy key management infrastructures (KMIs) is the only way to enable encryption on a large scale." Arguing for government access to encryption keys, the Report states, "key recovery is needed to provide business access to data when encryption keys are lost or maliciously misplaced, and court-authorized law enforcement access to the plain text of criminal-related communications and data lawfully seized."

The Report also calls on the federal government to encourage efforts by commercial vendors to develop key recovery concepts and techniques. In a speech before several Fortune 500 company officials in late July 1998, Deputy Secretary of Defense John Hamre, a former member of the staff of Sam Nunn's Armed Services Committee, said, "I'd also ask American business not to make a campaign out of just trying to bust through export controls as though somehow there was a God-given, inherent right to send the strongest encryption to anybody in the world, no matter who they are . . . I don't agree with that. I will never agree with that." Linton Wells, Deputy Undersecretary of Defense for Policy Support, quoted Hamre as saying he would "use [the Pentagon's] purchasing power to leverage the use of key recovery cryptography" in the civil agency and private sectors. Wells reaffirmed this when he said that DOD was "putting its money where its mouth is by requiring private vendors to turn over to DOD the encryption key to software programs enabling access to companies' encryption codes in the event of an emergency." By using the DOD officials as the chief proponents for key recovery schemes, the administration seeks to bring the debate under such rubrics as "critical infrastructure protection" and "homeland defense."

One sector of the infrastructure that the PCCIP spent time looking into is the emergency services sector (police, fire, emergency medical services). However, according to a U.S. Department of Commerce memorandum from William A. Reinsch, the Undersecretary of Commerce for Export Administration, because key escrow products have a significant performance flaw, police forces in the United States and abroad are reluctant to use such products. The Reinsch memo points out that "police forces are reluctant to use ëescrowed' encryption products (such as radios in patrol cars). They are more costly and less efficient than non-escrowed products. There can be long gaps in reception due to the escrow features - sometimes as long as a ten-second pause. Our own police do not use recoverable encryption products; they buy the same non-escrowable products used by their counterparts in Europe and Japan. Other government agencies may also reject key recovery -- for example, some U.S. exports were to support Allied government agencies with signals intelligence missions similar to NSA's." Consequently, according to Reinsch, the performance flaws caused by key escrow would place such technology in the category of a threat to the emergency services and intelligence warning sectors of the critical infrastructure and not as a safeguard. Therefore, the administration should reconsider the use of key escrow/recovery technology as a component of critical infrastructure protection.

The Posse Comitatus Act

Congress passed the Posse Comitatus Act of 1878 (20 Stat. 152 [18 USC 1385]) in order to curb the military's role in law enforcement in the South. The act, as amended, states:

> Whosoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined not more than $10,000 or imprisoned not more than two years, or both.

The DSB Report suggests that the Defense Department defend non-military computer systems. Such a suggestion runs afoul of both the Posse Comitatus Act and the Computer Security Act. The Report states:

> The SECDEF/DEPSECDEF should also task the General Counsel to propose legislation, regulation, or executive orders as may be needed to make clear the DOD role in defending non-DOD systems. This should specifically address the need for changes to the Computer Security Act, the capture of information on unidentified intruders (issue of intelligence collection on U.S. persons), the authority to conduct "hot pursuit" of intruders, and the ability to obtain reports from the operators of critical elements of the civil infrastructure.

Congress should revisit the provisions of the Posse Comitatus Act and ensure that the U.S. military is not permitted to engage in unwarranted intrusions into the privacy of U.S. citizens, as it did during the 1970s in monitoring the lawful activities of anti-Vietnam War protesters. Senator Charles Grassley of Iowa, the chairman of Judiciary Subcommittee on Administrative Oversight and the Courts, should be supported in his efforts to enforce the provisions of Posse Comitatus. In early 1997, when Senator Grassley discovered U.S. Army Colonel John Ellis was serving as deputy chief of the FBI's Domestic Terrorism Planning Section, he said, "to the extent we allow a Colonel Ellis incident to succeed, it confirms the militarization of law enforcement." Grassley added, "there should be a clear line of demarcation between the military and law enforcement. And I'm incensed because the people at the FBI and Justice are too stupid to see that."

Expanded Role for the FBI

The FBI played a large role in critical infrastructure protection even before President Clinton signed PDD 62 and 63. It hosted two groups involved in infrastructure protection: the former CIITAC (Computer Investigation and Infrastructure Threat Assessment Center), and the interim Infrastructure Protection Task Force. Both were located at FBI headquarters.

Of particular concern is the role the FBI has played in lobbying the legislative and judicial branches on its surveillance agenda. Such lobbying is reminiscent of that done by the NSA when it was trying to advance the agendas contained in NSDD-145 and stall the passage of the Computer Security Act. This resulted in a sharp rebuke from Representative Brooks who drew attention to the criminal provisions of Title 18, U.S.C. 1913.

FBI Director Freeh's congressional lobbying efforts have been directed towards certain key members of the Senate, including Senators Phil Gramm, Orrin Hatch, Joseph Biden, Arlen Specter, and Patrick Leahy. During 1981, Freeh, while serving as an FBI special agent, helped Senator Sam Nunn's Permanent Subcommittee on Investigations. Not coincidentally, Nunn, both during his time as senator and as co-chair of the PCCIP Advisory Committee, became a strong

proponent of the administration's critical infrastructure proposals. It is also reported that the FBI's Office of Public and Congressional Affairs has grown to 85 full-time positions, becoming "one of the most effective lobbying operations in Washington, public or private."

Also troubling has been the FBI's lobbying directed at members of the federal judiciary. On July 15, 1998, Judge Royce Lamberth of the U.S. District Court for the District of Columbia and the chief judge of the secretive Foreign Intelligence Surveillance Court (FISC) -- the court empowered to grant the NSA and FBI authority to conduct domestic wiretaps in cases involving national security -- revealed that Freeh had been lobbying the judicial branch of the government for an international mandatory key recovery scheme. Freeh's lobbying efforts were conducted through the auspices of the Judicial Conference, the policy-making body for the Administrative Office of the US Courts. In one case, Freeh gave Lamberth and the six other members of the FISC a demonstration of what occurs when the FBI intercepts encrypted communications. Lamberth said he was also convinced of the government's claims that it "takes trillions of years [for the government] to break encryption." According to Lamberth, Freeh was accompanied in his judicial lobbying visit by General John Gordon, representing CIA director George Tenet, and NSA director Lt. Gen. Kenneth Minihan.

The blueprint for the FBI's expanding powers can be found in Vice President Gore's National Performance Review, issued on September 7, 1993. In it, Gore proposed:

> ... to integrate drug enforcement efforts of the DEA [Drug Enforcement Administration] and FBI. This will create savings in administrative and support functions such as laboratories, legal services, training facilities, and administration. Most important, the federal government will get a much more powerful weapon in its fight against crime.
>
> When this has been successfully accomplished, we will move toward combining the enforcement functions of the Bureau of Alcohol, Tobacco and Firearms (BATF) into the FBI . . ..

In granting the FBI widened powers to protect the critical infrastructure, particularly computers and networks, it is important to reflect on a comment by Representative Robert Barr of Georgia, himself a former U.S. attorney. He stated, "Federal law enforcement power far outweighs accountability."

In 1997, the FBI was armed with new guidelines to investigate U.S. citizens suspected of supporting foreign groups deemed by the Secretary of State to be involved in terrorism. One result of this was the FBI's proposed "Bay Area Counterterrorism Task Force," which would combine the resources of the FBI, the Immigration and Naturalization Service, and the San Francisco Police Department to investigate Bay Area organizations, even if there were no grounds to suspect criminal activity. The FBI's political surveillance efforts also conflict with San Francisco Police Department policy, which requires a special review before it can investigate crimes linked to political activity. According to a San Francisco Police Department memo, similar FBI programs exist in Chicago, Los Angeles, Boston, and Washington, D.C.

The anxieties expressed by Senator Grassley and Representative Barr, as well as other legislators, should be transformed into legislation restricting the FBI, other law enforcement agencies, and intelligence agencies from engaging in domestic fishing expeditions aimed against U.S. citizens exercising their First Amendment rights.

Antitrust

The PCCIP Report recommends that the Department of Justice provide antitrust relief to certain private companies to enable them to jointly share information with the government. On July 15, 1998, an official of the NSA told Commerce Undersecretary Reinsch that NSA was trying to engage Microsoft and Intel in its critical infrastructure "solution" but did not want to run afoul of anti-trust laws. Promoting anti-trust relief in the name of protecting against nebulous futuristic information warfare threats appears to be a case of overreaction. Additionally, such anti-trust relief in an era of several mega-mergers between telecommunications giants calls into question the propriety of extending anti-trust exemptions to such a select group of corporations.

Congress should ensure that anti-trust legislation is not weakened to facilitate infrastructure protection or information warfare initiatives.

Liability

The PCCIP Report recommends that the government examine liability relief for private corporations that share sensitive information with the federal government. This could include giving corporations immunity from law suits arising from invasions of employee and customer privacy, workplace-related injuries and sickness, environmental pollution, and internal fraud.

Congress should enact legislation prohibiting the federal government from granting liability relief to companies that share sensitive information, where that sharing results in adverse employment actions being taken against individuals engaged in legal activities.

National Security and Foreign Corporations

The PCCIP Report recommends that the NSC establish standards for sharing critical infrastructure information with foreign corporations and the U.S. subsidiaries of foreign corporations. This places American-owned companies in a strategically better position to compete in the international marketplace and may be in violation of international free trade treaties to which the United States is a party.

State Government Liability and Disclosure

The PCCIP Report bemoans the fact that the number of diverse state laws complicates the maximization of information sharing with the federal government. It recommends that a study group be formed to re-draft state legislation to permit such information sharing. Chief targets of the federal government are the state privacy and freedom of information laws as well as numerous sectoral laws dealing with particular disclosures of confidential information, such as criminal justice records; bank records; credit information; employment records; library records; medical records; privileged communications with psychologists, clergymen, speech pathologists and audiologists, attorneys, accountants, and pharmacists; school records; and tax records.

Federal attempts to curtail state privacy laws should be resisted by federal legislation prohibiting the federal government from pre-empting state privacy laws. In addition, some state laws permit access to documents held by organizations not covered by the Federal FOIA. Federal attempts to limit disclosures at the state level will further erode a citizen's right to access public information. This should also be addressed in new federal legislation.

Government Certification and Deputizing of Information Security Personnel

The PCCIP report recommends that the federal government - namely NSA, NIST, and the Department of Education - work with private industry to develop a training program for information assurance specialists. The DOD's Linton Wells spoke of a Pentagon plan to create a GI-Bill type program to train computer security professionals. The DSB Report suggests loaning DOD personnel to the civil government and private sector to improve infrastructure protections. The DSB also recommends that a "closed community" of experts of information warfare experts be established, and that a warning center be set up that would have the authority to mandate the reporting of all suspected intrusions and computer incidents affecting "DOD systems and networks" (now defined as any which could have an impact on the critical infrastructure).

The PCCIP Report suggests providing monetary reward and payment-for-information programs to encourage on-line users to provide information on suspected computer crimes.

Considering the fact that there already exists a number of professional certification programs in the private sector encompassing such disciplines as information systems security, internal auditing, data processing, computer programming, and network and system administration, proposals to create a virtual "cyber Stasi" of informants and federal deputies is offensive and should be deleted from all federal budget line items. .

Bibliography

Association for Computing Machinery*, Codes, Keys and Conflicts: Issues in U.S. Crypto Policy* (New York: ACM, 1994).

James Bamford, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency* (New York: Houghton Mifflin, 1982).

George Brownell, *The Origin and Development of the National Security Agency (Laguna Hills*, CA: Aegean Park Press, 1981).

David Burnham, *The Rise of the Computer State (New York: Random* Rouse, 1980).

Commission on CIA Activities Within the United States*, Report to the President* (Washington, D.C.: U.S. Government Printing Office, June 1975).

James Kirkatrick Davis*, Spying on America: The FBI's Domestic Counter-Intelligence Program* (New York: Praeger, 1992).

Whitfield Diffie and Susan Landau*, Privacy on the Line: The Politics of Wiretapping and Encryption*, (Cambridge, Mass: MIT Press, 1998).

Steve Dycus et al., *National Security Law* (New York: Little Brown and Company, 1990).

EPIC, *Open Government Archive* [http://www.epic.org/open_gov/]

EPIC, *The 1994 Cryptography and Privacy Sourcebook* (Washington, DC: EPIC 1994)

EPIC, *The 1995 Cryptography and Privacy Sourcebook* (Washington, DC: EPIC 1995)

EPIC, *The 1996 Cryptography and Privacy Sourcebook* (Washington, DC: EPIC 1996)

EPIC, *The 1997 Cryptography and Privacy Sourcebook* (Washington, DC: EPIC 1997)

EPIC, *The 1998 Cryptography and Privacy Sourcebook* (Washington, DC: EPIC 1998)

Mike Frost and Michael Gratton, *Spyworld: Inside the Canadian and American Intelligence Establishments* (Toronto: Doubleday Canada, 1994).

Lance J. Hoffman, ed., *Security and Privacy in Computer Systems* (Los Angeles: Melville Publishing, 1973).

George F. Jelen, *Information Security: An Elusive Goal* (Cambridge, Mass: Harvard University Center for Information Policy Research, 1985).

David Kahn, *The Code-Breakers* (New York, McMillan, 1967).

Wayne Madsen, *Handbook of Personal Data Protection* (New York: MacMillan Publishers, 1992).

National Research Council, *Cryptography's Role in Securing the Information Society* (Washington, D.C.: National Academy Press, 1996).

National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, D.C.: National Academy Press, 1991).

John M. Oseth, *Regulating U.S. Intelligence Operations: A Study in Defining the National Interest* (University of Kentucky Press, 1985).

Harold Relyea, *Evolution and Organization of Intelligence Activities in the United States* (Laguna Hills, CA: Aegean Park Press).

Jeffrey T. Richelson, *The U.S. Intelligence Community*, Cambridge, Mass: Ballinger, 1985).

Marc Rotenberg, "Testimony on the Computer Security Act of 1987 and the Memorandum of Understanding Between the National Institute of Standards (NIST) and the National Security Agency," *Military and Civilian Control of Computer Security Issues* (Washington, DC: Government Printing Office, 1989)

Marc Rotenberg, "The Only Locksmith in Town: The NSA's Efforts to Control the Dissemination of Cryptography," *Index on Censorship* (January 1990)

Bruce Schneier and David Banisar, *The Electronic Privacy Papers* (New York: John Wiley & Sons, 1997).

Stansfield Turner, *Secrecy and Democracy: The CIA in Transition* (New York: Houghton Mifflin, 1985).

Select Committee to Study Government Operations with Respect to Intelligence Activities, U.S. Senate. *Final Reports and Hearings* (Washington, D.C.:U.S. Government Printing Office, 1976). (Church Committee)

Committee on Goverment Operations, U.S. House of Representatives, *The Government's Classification of Private Ideas* (Washington, D.C.: U.S. Goverment Printing Office, 1981).

Committee on Goverment Operations, U.S. House of Representatives, *Computer Security Act of 1987* (Washington, D.C.: U.S. Goverment Printing Office, 1987).

Office of Technology Assessment, U.S. Cong., *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (Washington, D.C.: U.S. Government Printing Office, 1987).

Office of Technology Assessment, U.S. Cong., *Information Privacy and Security in Network Environments* (Washington, D.C.: U.S. Government Printing Office, 1994).

Appendix A: White Paper on PDD-63

WHITE PAPER

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

May 22, 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures,

including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

o the Federal Government to perform essential national security missions and to ensure the general public health and safety;

o state and local governments to maintain order and to deliver minimum essential public services;

o the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

o assessing the vulnerabilities of the sector to cyber or physical attacks;

o recommending a plan to eliminate significant vulnerabilities;

o proposing a system for identifying and preventing attempted major attacks;

o developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

o We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.

o The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.

o Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

o The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

o The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

o Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

o The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

o The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

o We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

o Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components

(elaborated in Annex A).

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical

infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

4. Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the

establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce -- Information and communications

Treasury -- Banking and finance

EPA -- Water supply

Transportation -- Aviation, Highways (including trucking and intelligent transportation systems), Mass transit, Pipelines, Rail, Waterborne commerce

Justice/FBI -- Emergency law enforcement services

FEMA -- Emergency fire service Continuity of government services

HHS -- Public health services, including prevention, surveillance, laboratory services and personal health services

Energy -- Electric power, Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI -- Law enforcement and internal security

CIA -- Foreign intelligence

State -- Foreign affairs

Defense -- National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall

attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal

Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- o Liability issues arising from participation by private sector companies in the information sharing process.
- o Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.
- o The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.
- o The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.

o The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.

o The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

o The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.

o The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.

o The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.

o The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

-

Internal Federal Government Actions

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

o The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.

o The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.

o All federal agencies shall make clear designations regarding who may authorize access to their computer systems.

o The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical

infrastructure.

o The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall:

(1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and

(2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.

o The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

o The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

o GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

o OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.

o The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

Assisting the Private Sector

In order to assist the private sector in achieving and maintaining infrastructure security:

o The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.

o The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.

o The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

APPENDIX B: White House Statement on PDD-62 and

PDD-63

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release May 22, 1998

SUMMARY OF PRESIDENTIAL DECISION

DIRECTIVES 62 and 63

President Clinton today ordered the strengthening of the nation's defenses against emerging unconventional threats to the United States: terrorist acts, use of weapons of mass destruction, assaults on our critical infrastructures and cyber-attacks.

The Combating Terrorism directive (PDD-62) highlights the growing threat of unconventional attacks against the United States. It details a new and more systematic approach to fighting terrorism by bringing a program management approach to U.S. counter-terrorism efforts.

The directive also establishes the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism which will oversee a broad variety of relevant policies and programs including areas such as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction.

The Critical Infrastructure Protection directive (PDD-63) calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. Such infrastructures include telecommunications, banking and finance, energy, transportation, and essential government services. The directive requires immediate federal government action including risk assessment and planning to reduce exposure to attack. It stresses the critical importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives.

APPENDIX C: Members of PCCIP

The government members of the PCCIP clearly represented intelligence and law enforcement interests. They included:

- Peter H. Daly, U.S. Treasury, Senior Advisor in the Office of the Assistant Secretary for Management and Chief Financial Officer. Daly's portfolio includes responsibility for electronic money policy issues as they affect law enforcement.

- John C. Davis, National Security Agency, Director of the National Computer Security Center. Davis served in various positions during a 34-year career at NSA, including Deputy Chief of the INFOSEC Operations and Technical Support Group, Deputy Chief of the Research and Technology Group,

Chief of the Microelectronics Office, and Chief of the Office of Computer and Processing Technology in the Research and Engineering Organization.

- Thomas J. Falvey, Department of Transportation (DOT), Office of the Secretary, Office of Intelligence and Security. Falvey is the DOT's National Security Advisor in the Office of Intelligence and Security and the department's expert on transportation infrastructure protection and assurance and information warfare.

- Brenton C. Greene, Department of Defense (DOD), Office of the Under Secretary of Defense for Policy, Director for Infrastructure Policy. Greene, a former U.S. nuclear submarine commander, led the DOD staff element responsible for developing policy, plans, programs and procedures for infrastructure assurance policy and information warfare.

- David A. Jones, Department of Energy (DOE), Office of Safeguards and Security, Director, Policy, Standards and Analysis Division. At DOE Jones was responsible for developing, promulgating and analyzing DOE-wide safeguards and security policy, procedures and standards, including physical security, information security, personnel security, nuclear materials control and accountability, and the Design Basis Threat.

- William B. Joyce, Central Intelligence Agency (CIA). Joyce joined the Central Intelligence Agency in 1972 and has served in a number of supervisory and management positions overseas and in Washington. He specializes in the collection and processing of foreign open source intelligence.

- Stevan D. Mitchell, Department of Justice. Mitchell is a trial attorney with the Criminal Division's Computer Crime Unit where has litigated cases, conducted investigations, drafted legislative proposals, and participated in international efforts to curb illegal uses of advanced technology, presumably including encryption technology.

- Dr. Irwin M. Pikus, Department of Commerce, Bureau of Export Administration. Dr. Pikus worked in the Bureau of Export Administration where he directed an office that collects and analyzes information dealing with foreign technology comparable to the advanced technologies whose exports are controlled by the United States. This presumably includes encryption technology.

- Dr. John R. Powers, Federal Emergency Management Agency, Senior Policy Advisor for Strategic Planning. Dr. Powers developed a policy framework for an integrated emergency response capability and helped change the approach to both mobilization and civil defense within the civil sector. FEMA is authorized to assume extra-constitutional powers in the event of a national emergency. Therefore, it has often been referred to as "the secret government."

- Susan Simens, Federal Bureau of Investigation (FBI). Simens is a Supervisory Special Agent with the Federal Bureau of Investigations. During her 18 years with the Bureau, she has been assigned to matters involving national security, including management of the FBI's computer espionage program.

Some of the members representing the private sector also had close links with the military and intelligence communities, including the PCCIP chairman. Robert Marsh currently serves as the chairman of the board of CAE Electronics, Inc. and Comverse Government Systems Corporation, two companies with close links to the Pentagon and intelligence agencies. He is also a trustee of the MITRE Corporation, a government think tank that is under contract to the CIA, NSA, and the military services. From 1989-1991, Marsh served as the first chairman of Thiokol Corporation, another Pentagon contractor.

Others having similar links include:

- Merritt Adams, American Telephone & Telegraph (AT&T). Adams is an international telecommunications consultant specializing in electronic surveillance.

- Dr. William J. Harris, Texas Transportation Institute. While Associate Director of the Texas Transportation Institute from 1985 to 1995, Dr. Harris contributed to development of a major program in intelligent transportation systems. He also spent a number of years with the Battelle Memorial Institute, a think tank with contracts with numerous military agencies.

The PCCIP's Steering Committee was composed of a similar cadre of members representing law enforcement, the military, and intelligence. They included General Marsh, along with:

- Attorney General Janet Reno.

- John J. Hamre, Deputy Secretary of Defense (from 1978 to 1984, he served in the Congressional Budget Office, rising to the position of Deputy Assistant Director for National Security and International Affairs).

- General Donald Kerrick, Deputy Assistant to the President for National Security Affairs (he previously served as the Director for Operations for the Defense Intelligence Agency and in 1994 and 1995, he served on the White House National Security Council as Director of European Affairs).

- Don Gips, Representative from the Office of the Vice President (he had previously served a three-year tenure as the FCC's Deputy Chief of the Office of Plans and Policy and later as Chief of the FCC's International Bureau. Before working at the FCC, Mr. Gips held the position of Engagement Manager at McKinsey & Company, an international consulting firm).

The PCCIP Advisory Committee was also packed with a number of members close to the military, law enforcement and intelligence communities. They included the two co-chairs:

- Former Senator Sam Nunn, of Georgia, a senior partner in the Atlanta law firm of King & Spalding. Nunn was elected to the United States Senate from Georgia in 1972 and served for four terms. He served as chairman of the Senate Armed Services Committee and the Permanent Subcommittee on Investigations. Nunn also served on the Senate's Intelligence Committee. He serves on the boards of the Center for Strategic and International Studies (a think tank for the intelligence community and State Department) and General Electric.

- Jamie S. Gorelick, Vice Chair of Fannie Mae. Gorelick previously served as Deputy Attorney General at the Department of Justice where she championed escrowed encryption and wider surveillance capabilities for the FBI. She was also General Counsel for the Department of Defense.

Other Advisory Committee members representing the military-intelligence complex include:

- Robert L. Baxter, Senior Vice President with the Bechtel Group, Inc. and President of the Bechtel Civil Company (BCIV). Bechtel is a privately-owned corporation that has been linked to numerous covert activities abroad, involving U.S. intelligence agencies.

- Joseph Holmes, Corporate Vice President and the group executive for EDS Technology and Engineering Group. Holmes has been with EDS since 1968, when it was under the management of H. Ross Perot. EDS has been associated with the provision of computer services to a number of foreign intelligence and police agencies, including the Shah of Iran's SAVAK. In recent times, EDS is at the forefront of providing advanced technology national identification card systems to various countries.

- Charles R. Lee, Chairman and the Chief Executive Officer of GTE Corporation. Lee also serves on the board of United Technologies Corp., a large defense contractor, and is the chairman of the President's National Security Telecommunications Advisory Committee (NSTAC).

- Norman Mineta, Senior Vice President and Managing Director of Transportation Systems and Services at Lockheed Martin. Lockheed Martin is one of the largest Pentagon contractors. A former

Mayor of San Jose, California, Mineta was elected to the U.S. House of Representatives in 1974, where he served for 21 years.

- Mort Topfer, Vice-Chairman of Dell Computer Corporation. Topfer served as Corporate Executive Vice President of Motorola, Inc., and President of Motorola's Land Mobile Products Sector. Topfer also spent a number of years with RCA Laboratories. Both Motorola and RCA developed systems supporting the signals intelligence (SIGINT) and communications intelligence (COMINT) missions of the NSA.

Full biographies available at: <http://www.pccip.gov/staff_bios.html>.

In addition, the Principals Committee that was established by Section 2 of Executive Order 13010 to review Commission reports or recommendations before submission to the President, also had a preponderance of those involved with law enforcement and intelligence. The Principals Committee includes:

- Secretary of Defense
- Attorney General
- Secretary of the Treasury
- Secretary of Commerce
- Secretary of Transportation
- Secretary of Energy
- Director of Central Intelligence
- Director of the Office of Management and Budget
- Director of the Federal Emergency Management Agency
- Assistant to the President for National Security Affairs
- Assistant to the Vice President for National Security Affairs
- Assistant to the President for Economic Policy and Director of the National Economic Council
- Assistant to the President and Director of the Office of Science and Technology Policy

---

economic and political rational for digital wire tapping and surveillance; The legal claims for government surveillance; Government strategies for soliciting cooperation from telephone companies and equipment manufacturers; and Policies government might pursue in the future. *The Electronic Privacy Papers* includes excerpts from the House Judiciary Committee report on the digital telephony bill, the FBI's wish list for electronic surveillance, U.S. cryptography policy statement from the White House, and many other government documents.

Electronic Privacy Information Center
666 Pennsylvania Avenue S.E.
Suite 301
Washington, D.C. 20003