Testimony and Statement for the Record of

Marc Rotenberg, Executive Director
Electronic Privacy Information Center
Washington, DC

Hearing on
CyberAttack: The National Protection Plan and its Privacy Implications

Before the

Senate Judiciary Committee,
Subcommittee on Technology, Terrorism and Government Information
United States Senate

Dirksen Senate Office Building Room 226
February 1, 2000

Mr. Chairman, members of the Subcommittee, thank you for the opportunity to testify today regarding the privacy implications of the Administration's proposed National Plan for Information Systems Protection. My name is Marc Rotenberg and I am the executive director of the Electronic Privacy Information Center, a research and advocacy organization, located here in Washington, DC. EPIC has a general interest in privacy protection and a particular interest in ensuring that efforts to promote computer security do not undermine basic American liberties. For over a decade we have reviewed proposals for information system security in the federal government, made recommendations for changes, and pursued litigation where appropriate.

I should say at the outset that we are all aware that our nation has become increasingly dependent on the hi-tech infrastructure for everything from power and communications to transportation and national defense. Moreover, it is quite likely that others who intend to do us harm would target this infrastructure in an effort to disable or disrupt essential communications resources.

Nonetheless our fear of attack and our need to protect public safety should not lead us to take actions that are wasteful, misguided, or ultimately undermine the values that we seek to defend. We should be particularly careful that the solutions that are pursued reflect the full range of risks to our nation's communications network. The plan presumes that threats to the nation's infrastructure are from adversaries intent on causing harm to the United States and that therefore steps must be taken to "defend our federal cyber systems." Security standards that treat all risks as simply defending against foreign threats will ultimately not serve us well.[1]

In this spirit, I would like to remind the Committee that the winter storm that hit Washington, DC last week did far more damage to the operation of government, the use of our transportation systems, and our supply networks than the widely touted Y2K bug which has consumed so much attention in the federal government. Defending America's cyberspace may require preparation against winter ice storms as well as malicious hackers in foreign countries.

[1] The developers of the Plan are aware of this as well, but they often obscure the problem. On the very first page of the report, the writers describe several genuine security problems with the nation's computer systems but then say, "All of these events have occurred—not on the same day, and not all the result of deliberate action by America's adversaries—but all within the last 36 months." The message should be stated more clearly: not all threats to the nation's computer systems will be malicious attacks from overseas.

Internet was Built to Withstand Attack

To assess the National Plan for Information System Protection, you must first recall that the Internet, which has emerged from the ARPANet, was designed to continue operation even after an attack from a foreign government. Robustness was key to the design. Protecting the Internet from attack is hardly a new problem; it was the basis of its creation.

The key to the Internet's resilience, and what distinguished it from the channel-switched communications networks that proceeded it, is a decentralized architecture that allows multiple-routings for messages sent between the same two points. If, for example, a person wished to send a message from Pittsburgh to Flagstaff in the old telephone network, an outage at the main switch in Phoenix could prevent a call from ever getting through. But in the packet-switched network, where messages could be broken up into small pieces, sent through different channels and then put back together, the disruption at one node would not prevent communications from going through.

In designing the Internet, the engineers recognized that a traditional top-down command and control structure would be vulnerable to attack and that a different way to move information would be necessary. History has shown that the design was well conceived. Over the last thirty years there have been only two incidents that really took down the Internet – and both resulted from software glitches.

It is important also to understand that the Internet really doesn't care whether a node is down because of a military attack or a winter storm – it is equally resistant to both purposeful assault and natural disaster.

Work on Internet security today continues largely in the open among researchers and experts all around the world. Critical to the future of network security is the open exchange of information among security experts, the opportunity to publish findings in the open literature, and the chance to challenge, even attack, another programmer's work. This process which relies on cooperation and the exchange of ideas is the best way to identify security flaws and encourage trust among users.

This work is not done simply by US citizens or US companies. Computer researchers around the world have all played an important role in developing the protocols and promoting the architecture that secures the Internet in the United States and around the world. Indeed the cryptographic techniques that help protect computers in this country were developed by researchers in Japan, Israel and elsewhere.

Unfortunately, the National Plan ignores much of this history. It draws sharp boundaries based on national interests. It treats threats to network reliability as primarily threats from abroad and downplays the risk of software glitches and winter storms. The plan urges the development of computer security experts charged with defending the nation's infrastructure. This view of computer scientists, as soldiers with keyboards, misses the critical point that computer security is an international enterprise.

Ultimately the Plan views the Internet as a domestic communications structure that must be secured from above from foreign threats. But the original architects of the network knew better. A communications network that can be secured from above can also be taken out from above.

Administration has Created Security Problems

My second point is that the federal government's recent efforts to promote computer security in the private sector have created more problems than they have solved. For the past decade the federal government was largely responsible for preventing the widespread availability of encryption and security tools that would have made the nation's computer systems more secure and less vulnerable to attack.

It is only in the past few months, after heavy lobbying by industry, pressure from Congress, and the continued voice of privacy organizations, that the administration has begun to back off the complex and short-sighted export control regime that has not only prevented the development and sale of good security products but also the implementation of better security systems in our country.

The problem is that the federal government has two very distinct views of computer security: one commonly called COMSEC, refers to Communications Security, the other SIGINT, refers to Signals Intelligence. In the COMSEC view of the world there is general agreement about the need to promote security and to make systems more difficult to attack. But in the SIGINT view of the world, the government seeks to get into computers, to intercept communications and to gather information that may be useful to protect the nation's security.

In no agency are the two notions more at odds than the National Security Agency. The NSA simultaneously attempts to promote strong security standards for the nation's computer systems and at the same time to develop the methods to crack codes, break into networks, and seize valuable intelligence. (And even with the resources at the NSA to promote computer security, problems remain. The newspapers reported last week that there was a significant failure at the NSA that took down key systems for several days.)

The Administration said that with many of its early encryption proposals it was trying to balance these competing interests, but the SIGINT interests were clearly undermining the COMSEC efforts. As a result, deeply flawed technical standards, such as the escrowed encryption standard, were put forward and the nation's computer systems remained vulnerable to attack. Also, tens of millions, possibly hundreds of millions of dollars were wasted trying to make these proposals designed by experts in SIGINT work.

The Administration also claimed that the export controls rules that limited the development of encryption products were only intended to control the availability of strong encryption outside of the United States. But in practice the rules kept strong encryption away from American users. For example, there are encryption protocols in software that protect credit card purchases on the Internet. But because of the government's export policy, US manufacturers were required to provide two versions – a

strong 128-bit version for US citizens, and a weaker 40-bit version for non-US citizens. Because of the additional paperwork required for US citizens to download the 128-bit version, many users simply left the 40-bit version in place. As a result US consumers buying products from US companies in the United States were using a weak version of encryption because of a policy that was intended to prevent strong encryption from being made available overseas. This is exactly the kind of problem that will be replayed under the National Infrastructure Protection Plan unless its proponents take a much broader view of the problems in computer security.

Much will be done in the next few years to improve network security in the private sector and across the federal agencies if the federal government simply stays out of the way. Institutions have a clear interest in safeguarding the security of their systems, but the federal government's interests are more divided. Until trust is reestablished in the security field, it would be better for the federal government to follow rather than lead.

Privacy Safeguards in Plan are Insufficient

Largely in response to concerns raised by privacy organizations and members of Congress about the original plan for Critical Infrastructure Protection, the new Information Systems Security Plan discusses the privacy issue at some length. There is much said about the need to protect privacy and uphold privacy laws. But in the end the recommendations on privacy fall short when compared with the enormous surveillance authority that will be given to the federal government.

The Plan sets out a series of "solutions" to address privacy concerns. It requests input from the privacy community, but establishes no formal process to incorporate recommendations. The plan proposes a legal review of elements of the plan, but most of the plan, including specific mission objectives and milestones, has already been established. The privacy section describes the need to review various privacy issues, but then focuses on such concepts as "consent" and "disclosure" that are clearly intended to facilitate government data collection and monitoring. The Plan's authors propose an annual conference and some consideration of privacy issues by the National Infrastructure Advisory Council, which is also tasked with a wide range of other responsibilities. And if the private sector membership of this Council is required to hold government security clearances, as is so often the case with similar bodies, it will limit the ability of citizens and independent experts to provide meaningful input as the proposal goes forward.

The section on privacy stands in sharp contrast to the other sections of the plan where the drafters outline ambitious, expensive and far-reaching proposals for government agencies. Nowhere does the Plan answer such questions as what formal reporting requirements will be established, what independent review will be conducted, and what mechanisms for public accountability and government oversight will be put in place. The federal wiretap law, for example, contains an annual reporting requirement so that the Congress and the public can review the use of wiretap authority by the federal government. The Computer Security Act established a Computer System Security and Privacy Advisory Board that has held frequent meetings, issued reports and adopted

resolutions on privacy and security matters for almost a decade. Where is the same institutional commitment in the Security Plan to ensure oversight and accountability?

It is also clear that the absence of a privacy agency in the federal government with the staff, expertise and resources to review the Information Protection plan and other similar proposals remains a critical problem. Having announced a commitment to ensure the protection of civil liberties, it seems clear that some institutional balance must be established to ensure that these proposals receive adequate review. Isn't it possible that in this vast budget to erect all of these elaborate surveillance techniques that Congress could set aside 3% to establish a federal privacy agency that could actually help safeguard the rights of Americans? This would be a small investment in what many Americans consider their number one concern about our nation's communications infrastructure – the protection of personal privacy.

Problems with FIDNET

While it remains unclear whether the proposed Plan will in fact promote network security, one point is clear: the plan will dramatically expand the ability of the federal government to monitor the activities of Americans all across the country. The plan recommends the development of a Federal Intrusion Detection Network ("FIDNET"), an open-ended monitoring authority that essentially gives a single federal agency the authority to track communications across all federal computer networks. According to the New York Times, "networks of thousands of software monitoring programs would constantly track computer activities, looking for indications of computer network intrusions and other illegal acts."

This is an extraordinary surveillance authority, unlike any capability that currently exists in the federal government. Last year civil liberties organizations warned that this proposal would create dramatic new government authority to monitor American citizens. The drafters of the Plan are aware of this criticism and believe they have addressed this problem. I tell you today that the problems with FIDNET remain.

I would like to draw your attention to a March 8, 1999 memo from Mr. Ronald D. Lee, Associate Deputy Attorney General, to Mr. Jeffrey Hunker, Director of the Critical Infrastructure Assurance Office. (This memo was obtained by EPIC under a Freedom of Information Act request and is attached to this testimony)

Mr. Lee says at the outset it is important to "precisely identify under what legal authority the FIDNET program is to be conducted. Because monitoring ongoing communications is a wiretap within the meaning of 18 U.S.C. § 2511, it can only be authorized pursuant to a wiretap order, or some relevant exemption to the statute."

Mr. Lee goes on to say that while an individual federal agency would have the right to monitor its own network to "protect against network intrusions, this does not mean that the GSA is a 'service provider' within the meaning of the statute for the entire federal government."

Mr. Lee concludes that the only way that the GSA could conduct the type of monitoring contemplated in the FIDNET proposal would be if the federal government would notify all users of federal computer systems that they would be subject to monitoring. Such a policy would cover not only federal employees but all Americans who make use of a federal computer system.

While Mr. Lee indicates that the Justice Department favors this type of government-wide "no privacy" warning notice, I want to make very clear that privacy organizations across the political spectrum would oppose such a proposal as a violation of the spirit of the federal wiretap statute, the plain language of the federal Privacy Act, and contrary to the Fourth Amendment. US law simply does not give the government the right to conduct such general purpose searches. The history of the Fourth Amendment reveals a clear intent to require the government to set out the specific circumstances for a search to occur. There is no "cyber threat" exception to the Fourth Amendment. The fact that the government announces that a warrantless search may occur is hardly a sufficient legal basis to permit such searches to take place.

There are other indications, contained in materials that we received under the FOIA, that the CIAO intends to make use of credit card records and telephone toll records as part of its intrusions detection system. Access to these records raises specific problem under US law.

The FIDNET proposal, as currently conceived, must simply be withdrawn. It is impermissible in the United States to give a federal agency such extensive surveillance authority.

Recommendations

As the White House plan currently stands, it raises far-reaching privacy problems. The designers of the plan are trying to apply twentieth century notions of national defense to twenty-first century problems of communications security. Such an approach will leave our networks ill-prepared to face the challenges of tomorrow.

In too many places the Plan relies too heavily on monitoring and surveillance and not enough on integrity and redundancy. To give a simple example, there are public telephones all across this country filled with money. One way to implement security would be to install cameras and recording devices inside each phone booth to monitor each person's use of the phone to ensure that it is appropriate and to determine whether any efforts are being made to steal the money stored inside the phone. Another approach would simply be to make the phones more secure and the money more difficult to steal. The phone companies have wisely chosen the second approach. The federal government still seems interested in the first.

Everyone wants to ensure that the computer networks that our country relies on remain secure, safe and free from disruption. On this point there is no disagreement. However, there is disagreement as to whether an intrusive, government-directed initiative

that views computer security as almost solely defending “our cyberspace” from foreign assault is the right way to go.

I urge you to proceed very cautiously. The government is just now digging itself out of the many mistakes that were made over the past decade with computer security policy. This is not the best time to be pushing an outdated approach to network security, fraught with privacy problems, on a fast-moving industry that is itself racing to develop good security solutions.

In 1975, Senator Frank Church, who conducted a Senate investigation of intelligence abuses, said of the NSA technology: "That capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything . . . there will be no place to hide."

This Committee should keep Senator Church’s warning in mind as it reviews this proposal to create a vast new surveillance authority across the federal government.

References

White House "National Plan for Information Systems Protection" (January 7, 2000) http://www.ciao.ncr.gov/National_Plan/national%20plan%20final.pdf

Executive Summary of "National Plan for Information Systems Protection" (January 7, 2000) [http://www.whitehouse.gov/WH/EOP/NSC/html/documents/npisp-execsummary-000105.pdf]

Bruce Schneier and David Banisar, *Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance* (Wiley 1997)

Whitfield Diffie and Susan Landau, *Privacy on the Line* (MIT Press 1998)

Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (Touchstone Books 1998)

National Resource Council, CRISIS Report (1996)

Peter G. Neumann, *Computer-Related Risks* (Addison Wesley 1995)

"Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the Report of the President's Commission on Critical Infrastructure Protection" (EPIC 1998) [http://www.amazon.com/exec/obidos/ISBN=1893044017/electronicprivacA]

EPIC, Critical Infrastructure Protection Resources [http://www.epic.org/security/infowar/resources.html]

Letter from Simon Liu, Acting Director, Information Management and Security Staff, Department of Justice to Mr. Wayne Madsen, Senior Fellow, Electronic Privacy Information Center, January 20, 2000 responding to Freedom of Information Act request of July 20, 1000 for “all agency records, including memorandum, letters, and minutes of meetings, dealing with any liaison between the Department of Justice and the Critical Infrastructure Assurance Office."