S. HRG. 106–889

CYBER ATTACKS: THE NATIONAL PROTECTION PLAN AND ITS PRIVACY IMPLICATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

EXAMINING THE VULNERABILITY OF U.S. SYSTEMS TO CYBER ATTACK, FOCUSING ON THE ADMINISTRATION'S NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION AND ITS IMPLICATIONS REGARDING PRIVACY

FEBRUARY 1, 2000

Serial No. J–106–62

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

68–776 CC WASHINGTON : 2001

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

APPENDIX

QUESTIONS AND ANSWERS

CYBER ATTACK: THE NATIONAL PROTECTION PLAN AND ITS PRIVACY IMPLICATIONS

TUESDAY, FEBRUARY 1, 2000

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,
AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl (chairman of the subcommittee) presiding.

Also present: Senators Feinstein and Bennett [ex officio.]

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. The subcommittee will please come to order.

Let me first welcome everyone to this hearing of the Subcommittee on Technology, Terrorism, and Government Information. Today, we will examine the National Plan for Information Systems Protection, released by the President on January 7, and its implications regarding privacy. This is the fifth public hearing we have held on cyber protection in the last 2 years, and the first where we can finally review the long overdue National Plan mandated by the 1996 Defense Authorization Act.

The United States, of course, is the most technologically sophisticated country in the world. Today, virtually every key service in our society is dependent on computer technology—electric power grids, air traffic control, nuclear warning, banking, just to name a few examples. Highly interdependent information systems control these infrastructures.

With the benefits of technological advances comes a new set of vulnerabilities that can be exploited by individuals, terrorists, and foreign nations. Our enemies don't need to risk confronting our powerful military if they can attack vulnerabilities in our critical information infrastructure. According to the National Security Agency, more than 100 nations are working on information warfare tactics. There have already been a disturbing number of attacks on U.S. information systems, exposing our Achilles heel to any potential adversary.

At our last hearing, Michael Vatis, from the FBI, described how Russia conducted a "series of widespread intrusions into Defense Department, other Federal Government agencies, and private sector computer networks." Additionally, China is reportedly consider-

ing forming an entirely new branch of the military for information warriors.

A recent article in the Chinese Liberation Army Daily assessed that the integration of Web warfare with ground combat will be essential to winning future conflicts. Moreover a recent book titled "Unrestricted Warfare," written by two Chinese Army colonels, proposes tactics for developing countries like China to use to compensate for their military inferiority versus the United States. One scenario described in the book envisions a situation where the attacking country causes panic through cyber attacks on civilian electricity, telecommunications, and financial markets. These examples underscore the severity of the threat facing the United States.

In light of these concerns, I authored an amendment to the 1996 Defense Authorization Act directing the President to submit a report to Congress "setting forth the results of a review of the national policy on protecting the national information infrastructure against strategic attacks." This ultimately culminated in the National Plan before us today, which is more than a year overdue.

I am pleased that the Plan calls for specific milestones with timetables for securing our Nation's information systems, although its goals are modest and merely a first step. I hope the administration considers the Plan a living document that must be reviewed and revised with new technological advances and discovered vulnerabilities. This will be a complicated and expensive process, but it is vital to protect our national security and way of life. To support the effort, I am encouraged that news reports indicate the President's budget will include a $160 million increase in spending on cyber security initiatives.

In securing the critical infrastructures that provide our way of life, we must be careful that it doesn't occur at the expense of civil liberties. We need to update our current legal framework to reflect the revolution in information technology, to strike the right balance between security and civil liberties.

The reality is that doing nothing to enhance our cyber security, in fact, erodes the privacy and civil liberties of Americans by making public information accessible to any hacker with a computer and a modem. Let me repeat that. The reality is that doing nothing to enhance our cyber security, in fact, erodes privacy and civil liberties of Americans by making information accessible to any hacker with a computer and a modem. The National Plan's implementation must consider the reasonable privacy issues that must be discussed and appropriately balance them with security interests.

Our witnesses are well-suited to address these issues. Mr. John Tritak, Director of the Critical Infrastructure Assurance Office, is responsible for the development of the National Plan. He will summarize the Plan and speak to the privacy issues it raises.

Our second panel—Mr. Frank Cilluffo, senior policy analyst at the Center for Strategic and International Studies, and Mr. Rotenberg, Executive Director of the Electronic Privacy Information Center—will testify about the balance between security and civil liberties in implementing the Plan. Please note that Mr. Barry Steinhardt, from the ACLU, was also invited to testify, but respectfully declined.

I also want to acknowledge excellent testimony that I am going to put in the record from the General Accounting Office. Jack Brock, who is the Director of the Governmentwide and Defense Information Systems Accounting and Information Management Division, is here today, and I very much appreciate the fine testimony that he presented on critical information and infrastructure protection which will be put in the record here.

[The prepared statement of Mr. Brock follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate

For Release on Delivery
February 1, 2000

CRITICAL INFRASTRUCTURE PROTECTION

Comments on the National Plan for Information Systems Protection

Statement for the Record
Jack L. Brock, Jr., Director
Governmentwide and Defense Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-72

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the *National Plan for Information Systems Protection*.[1] This plan calls for new initiatives to strengthen the nation's defenses against threats to public and private sector information systems that are critical to the country's economic and social welfare, particularly those supporting public utilities, telecommunications, finance, emergency services, and government operations. As a "preliminary" document, it is intended to begin a dialogue on its proposals and lead to the development of plans for protecting other elements of the nation's infrastructure, including those pertaining to the physical infrastructure and specific roles and responsibilities for state and local governments and the private sector.

Beginning this dialogue is vital. As I stressed at this Subcommittee's October 1999 hearing[2] on critical infrastructure protection, our nation's computer-based infrastructures are at increasing risk of severe disruption. The dramatic increase of computer interconnectivity–while facilitating communications, business processes, and access to information–has increased the risk that problems affecting one system will also affect other interconnected systems. Massive computer networks provide pathways among systems that, if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. While the threats or sources of these problems can include natural disasters, such as earthquakes, and system-induced problems, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

This plan is an important and positive step forward toward building the cyber defense necessary to protect critical information assets and infrastructures.

It identifies risks associated with our nation's dependence on computers and computer networks for critical services.

It recognizes the need for the federal government to take the lead in addressing critical infrastructure risks and to serve as a model for information security.

---

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*. Released January 7, 2000. The White House.

[2] *Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations* (GAO/T-AIMD-00-7, October 6, 1999).

It outlines key concepts and general initiatives to assist in achieving these goals.

In doing this, the plan addresses many of the same points we raised at last October's hearing, including the need for improved standards, strengthened evaluations and oversight of agency performance, increased technical expertise, adequate funding, and improved incident detection and response capabilities.

However, there are opportunities for improvement as the plan is further developed as well as significant challenges that must be addressed to build the public-private partnerships necessary for infrastructure protection. In particular, we believe the plan should place more emphasis on providing agencies the incentives and tools to implement the management controls necessary to assure comprehensive computer security programs, as opposed to its current strong emphasis on implementing intrusion detection capabilities. In addition, the plan relies heavily on legislation and requirements already in place that, as a whole, are outmoded and inadequate as well as poorly implemented by the agencies.

Mr. Chairman, my testimony today will provide a more detailed overview of the plan, identify opportunities for sharpening the plan's proposals for improving the federal government's security programs, and outline the challenges facing the government in building the public-private partnerships necessary for comprehensive infrastructure protections.

Overview of *The National Plan for Information Systems Protection*

The National Plan for Information Systems Protection is intended as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. This preliminary version focuses largely on federal efforts being undertaken to protect the nation's critical cyber-based infrastructures. Subsequent versions are to address a broader range of concerns, including the specific role industry and state and local governments will play in protecting physical and cyber-based infrastructures from deliberate attack as well as international aspects of critical infrastructure protection. The end goal of this process is to develop a comprehensive national strategy for

infrastructure assurance as envisioned by Presidential Decision Directive (PDD) 63.[3]

The plan proposes achieving its twin goals of making the U.S. government as a model of information security and developing a public-private partnership to defend our national infrastructure through the following 10 programs which are intended to serve three cross-cutting infrastructure protection objectives.

Table 1: Infrastructure Protection Objectives and Programs

	Crosscutting Objective	Program
Prepare and Prevent	The steps necessary to minimize the possibility of significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.	Identify critical infrastructure assets and shared interdependencies and address vulnerabilities.
Detect and Respond	The actions required to identify and assess an attack in a timely way, and then to contain the attack, quickly recover from it, and reconstitute affected systems.	Detect attacks and unauthorized intrusions.
		Develop intelligence and law enforcement capabilities to protect critical information systems.
		Share attack warning and information in a timely manner.
		Create capabilities for response, reconstitution, and recovery.
Build Strong Foundations	The steps needed to create and nourish the people, organizations, laws, and traditions that will make us better able to prepare for and prevent, detect, and respond to attacks on our critical information networks.	Enhance research and development.
		Train and employ adequate numbers of information security specialists.
		Outreach to make Americans aware of the need for improved cyber security.
		Adopt legislation and appropriations to support infrastructure protections.
		Ensure the full protection of American citizen's civil liberties, their rights to privacy, and their rights to the protection of proprietary data.

[3] Issued in May 1998, this directive requires that the Executive Branch assess the cyber vulnerabilities of the nation's critical infrastructures—information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsibility for continuity of federal, state, and local governments. The directive places special emphasis on protecting the government's own critical assets from cyber attack and the need to remedy deficiencies in order to become a model of information security.

Making the Federal Government a Model

Making the federal government a model of good information security is essential to the plan's success. However, the gap between expectations and actual agency performance is significant. As we testified last October and in subsequent written responses to your questions,[4] our government is not adequately protecting critical federal operations and assets from computer-based attacks. In particular, recent audits conducted by GAO and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, and nonexistent or weak continuity of service plans.

Importantly, our audits have repeatedly identified serious deficiencies in the most basic controls over access to federal systems. For example, managers often provided overly broad access privileges to very large groups of users, affording far more individuals than necessary the ability to browse, and sometimes, modify or delete sensitive or critical information. In addition, access was often not appropriately authorized or documented; users often shared accounts and passwords or posted passwords in plain view; software access controls were improperly implemented; and user activity was not adequately monitored to deter and identify inappropriate actions.

While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. As we reported in 1996 and, again, in 1998,[5] agencies have not established security management programs to ensure that controls, once implemented properly, are effective on an ongoing basis. This framework of effective access controls and management oversight is fundamental to any good computer security program.[6]

[4] *Responses to Posthearing Questions* (GAO/AIMD-00-46R, November 30, 1999).

[5] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996) and *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

[6] To identify potential solutions to this problem, we studied the security management practices of eight nonfederal organizations known for their superior security programs. We found that these organizations managed their information security risks through a cycle of risk management activities. The basic framework, built on 16 specific practices, allows risk management through an ongoing cycle of activities coordinated by a central focal point. See *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

At last October's hearing, we also observed that other crosscutting actions--ranging from clarifying the roles and responsibilities of the many entities involved in information security, to strengthening oversight, to securing adequate technical expertise and

funding--were needed in seven key areas to provide greater assurance that critical infrastructure objectives can be met. I would like to discuss how the plan addresses each of these areas and what additional actions need to be taken.

Clearly Defined Roles and Responsibilities

It is important that a federal strategy delineate the roles and responsibilities of the numerous federal entities involved in information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security; and the National Institute of Standards and Technology (NIST), with assistance from the National Security Agency (NSA), is responsible for establishing related standards. In addition, interagency bodies, such as the CIO Council and the entities created under PDD 63, are attempting to coordinate agency initiatives. However, the proliferation of organizations with overlapping oversight and assistance responsibilities is a source of potential confusion among agency personnel and may be an inefficient use of scarce technical resources.

The plan takes some positive steps to resolve this problem. For example, it discusses in very general terms how tasks associated with accomplishing the plan's objectives relate to computer security responsibilities outlined in existing laws and related guidance. These include the federal computer security and information resource management responsibilities of OMB, agency Chief Information Officers, Chief Financial Officers as well as the CIO Council. It describes OMB's core responsibility for managing federal computer security and information technology. And it generally defines the roles of the major entities created by PDD 63, including the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, the Critical Infrastructure Assurance Office, and the National Infrastructure Protection Center.

In this regard, the plan makes a start at better defining the critical infrastructure protection responsibilities of the many federal entities involved. The plan also introduces or formalizes a number of new entities, interagency working groups, and projects that will have to be integrated into the existing framework of computer security activities. Examples of these new entities and efforts include an Expert Review Team for evaluating agency infrastructure protection plans, a Federal Intrusion

Detection Network, and an interagency working group on system security practices. Because of the number of entities involved (some established by law, some by executive order, and others with less formal mandates), strong and effective leadership will be essential to ensure that their efforts are coordinated and adequately communicated to individual agency personnel and that critical infrastructure protection efforts are appropriately linked with broader computer security efforts.

Risk-Based Standards

The plan recognizes the need for improved standards and asserts that NSA, NIST, GSA, and OMB will work together to identify or develop recommended practices and standards for critical federal information systems. The plan further states an intent to encourage adoption of a uniform set of standards throughout government and private industry. While on the surface these appear to be commendable goals, they do not recognize that such standards must be tailored to provide for varying levels of protection. As the plan is further developed, its focus needs to be sharpened to provide such recognition.

Currently, agencies have wide discretion in deciding (1) what computer controls to implement and (2) the level of rigor with which to enforce these controls. In theory, this is appropriate since, as OMB and NIST guidance states, the level of protection provided should be commensurate with the related risk to operations and assets. In security, one size does not fit all. The risks associated with different types of data and operations vary, depending on their sensitivity and criticality. For example, for undercover law enforcement operations, data confidentiality must be protected at all cost, while for other types of data, such as current information on financial markets, data integrity is the uppermost concern.

Our audit work has shown that agencies have generally done a very poor job of evaluating their information security risks and implementing appropriate controls. As a result, we believe that more specific guidance on what types of controls are appropriate for specific types of systems and data and the ways in which these controls should be implemented would be helpful. Specifically, a more prescriptive set of control standards, supported by a range of data classifications and related minimum requirements, would help clarify expectations for information protection, provide a framework for assessing information security risk, and help ensure that similar types of data and shared data are provided the same level of protection from one agency to another. In essence, risk-based standards would assist agencies in ensuring that their most critical operations and assets are protected at the highest levels, while providing

agencies the flexibility to apply less rigorous (and often less expensive and less cumbersome) controls to lower-risk operations and assets.

Routine Evaluations of Agency Performance

Agency managers have a responsibility to not only determine the level and type of controls necessary to protect information assets but also to routinely evaluate those controls to assess their effectiveness. This responsibility is not being met. At present, there is no mechanism for routinely testing and evaluating the effectiveness of agency information security programs and presenting the results in a way that is meaningful to agency managers.[7] In addition, there is no standard testing methodology that is applied consistently from year to year and among organizations. Without such mechanisms, there is no reliable and meaningful way to measure agency information security practices and, in turn, to provide OMB and the Congress with the information needed to gauge agency performance and hold agencies accountable for implementing needed improvements.

The plan takes some constructive steps in this regard. Particularly, it calls on federal agencies to put in place programs to carry out several types of vulnerability testing and analysis, including routine automated system configuration/integrity/vulnerability testing using commercial-off-the-shelf tools, regular internal self-assessments, and independent external critical reviews. At an agency's request, NSA and NIST are to perform independent analyses of critical federal information infrastructure and provide independent reports of their results to the agency's CIO. And, as mentioned earlier, the plan anticipates establishing a permanent Expert Review Team at NIST to assist governmentwide agencies in adhering to federal computer security requirements.[8]

Nevertheless, we believe that the plan's provisions for testing agency controls may not be rigorous enough. Tests initiated by agency officials are essential because they provide information needed to fulfill their ongoing responsibility for managing security programs. However, routine in-depth tests and evaluations initiated by independent auditors, such as agency inspectors general, are also critical because they serve as an independent check on management evaluations and provide reliable information on actual control effectiveness for congressional and executive branch oversight.

[7] Some independent testing of systems is done through agency annual financial statement audits.

[8] The Critical Infrastructure Assurance Office first established expert review teams in November 1998 to evaluate agency critical infrastructure assurance plans.

Our audits at individual agencies and our best practices work have shown that a continuous cycle of testing, reassessment of risk, and adjustments to policies and controls is needed to ensure that efforts to protect information remain appropriate and effective on an ongoing basis. Establishing such a cycle of activity will require a significant commitment by agency management, the federal audit community, and federal centers of technical expertise, such as NSA and NIST. It will be important for any new audit requirements, including those associated with the Expert Review Team, to be conducted in this context.

Executive Branch and Congressional Oversight

Having effective oversight over agency performance is the linchpin to maximizing protection over critical infrastructure and assets. The government's recent success in dealing with the Year 2000 issue demonstrated the impact that good oversight–both in the Congress and within the agencies–coupled with performance objectives and performance data can have on effective program management. Those success factors are lacking in cyber protection. There is too little incentive for agencies to adhere to guidance, too little performance data to promote truly effective oversight, and too little effort among those providing oversight to exert corrective action.

The administration's call to action through this plan's development and increased congressional interest indicates a heightened concern over cyber security and provides a basis for increased oversight. As noted in the previous section, initial oversight must provide a heavy focus on agency management's fulfillment of its obligations to set and evaluate meaningful controls over its information environment.

Adequate Technical Expertise

Federal agencies cannot provide needed information security without trained staff. The Computer Security Act authorized NIST to provide assistance to agencies and included provisions for periodic training in computer security awareness and practice. However, the availability of adequate technical expertise has been a continuing concern to agencies. GAO has not specifically analyzed the technical skills of agency personnel involved in computer security across government. But we have observed a number of instances where agency staff did not have the skills needed to carry out their computer security responsibilities and were not adequately overseeing activities conducted by contractors. As technology evolves, the challenge of training and retaining people with the expertise to select, implement, and maintain computer security controls is likely to increase.

The plan does a good job of addressing this issue. It describes a program to develop a cadre of highly skilled computer science and information security personnel. This program, if implemented, would include estimating personnel and training needs; establishing centers for information technology excellence that will provide web-based and classroom information security training to federal employees, college and high school students; initiating a scholarship program under which recipients would agree to a pre-determined commitment to federal government service; and establishing a high school and secondary school outreach program.

Adequate Funding

Federal agencies must have adequate resources to support their information security and infrastructure protection efforts. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks.

In releasing the plan on January 7, the President announced that he was proposing a 16 percent increase in funding for critical infrastructure protection in his fiscal year 2001 budget proposal. To jumpstart fiscal year 01 initiatives, the President also proposed $9 million in supplemental funding for this spring.

We have not had the opportunity to examine this proposal in detail. However, as this plan evolves, it will be important to secure OMB and congressional oversight of spending in order to ensure that expenditures are targeted toward reducing the most significant risks and that controls implemented are effective. Our audits have shown that, in the past, agencies have expended resources on controls that, when tested, proved to be ineffective. In addition, they have often addressed identified weaknesses in an ad hoc, piecemeal fashion that resulted in limited improvement. It will be important for future security budgets to be based primarily on risk-based needs and for expenditures be evaluated, to the extent possible, in terms of actual risk reduction.

Incident Detection and Response

Given the vast scale and variety of federal operations, there is a pressing need to more comprehensively monitor and develop responses to intrusions, viruses, and other incidents that threaten federal systems. Several entities are already providing some central coordination and

guidance in this area—including the FBI, NIST, and the FedCIRC.[9] However, as noted in our previous testimony, the specific roles and responsibilities of these organizations, as well as the balance between governmentwide and individual agency responsibilities, should be clarified and expanded to provide a more comprehensive picture of the security events that are occurring and assistance in dealing with them.

The plan proposes to strengthen incident detection and response by developing mechanisms for regular sharing of federal threats, vulnerability, and warning data; and sponsoring conferences to further the coordination and development of common operating systems. In particular, it calls for a governmentwide system for analyzing and correlating attack data consisting of three elements: one for the Department of Defense and national security communities (the Joint Task Force-Computer Network Defense, which is already deployed), a second for non-Defense federal departments and agencies (the Federal Intrusion Detection Network, or FIDNet which will build on existing DOD and other security technology expertise), and a third that provides information to both systems (the National Security Incident Response Center, or NSIRC, which has already been deployed to provide expert assistance to the national security community in isolating, containing, and resolving incidents threatening national security systems).

We agree that developing improved intrusion detection and response capabilities is important. However, available tools and methods for analyzing network traffic and detecting intrusions are still evolving and cannot yet be relied on to serve as an effective "burglar alarm," as envisioned by the plan. While holding promise for the future, such tools and methods currently raise many questions regarding technical feasibility, cost-effectiveness, and the appropriate extent of centralized federal oversight. Accordingly, these efforts merit close congressional oversight.

Legislative Framework

As noted earlier, one of our major concerns with the plan is that it relies on current law, policies, and practices, which are based largely on the Computer Security Act of 1987, even though the act is outmoded and inadequate, as well as poorly implemented. This is a fundamental problem for several reasons. First, the act focuses too much attention on individual system security, rather than taking an organizationwide perspective. Such a narrow focus is unworkable in a networked environment. Second, the

[9] FedCIRC—the Federal Computer Incident Response Capability—is a reporting center at the General Services Administration.

act oversimplifies risk considerations by implying that there are only two categories of information: sensitive versus nonsensitive or classified versus nonclassified. As a result, it fails to recognize that security must be managed for a range of varying levels of risk to the integrity, availability, and confidentiality of information supporting agency operations and assets. Third, the act treats information security as a technical function, rather than as a management function, which removes security from its integral role in program management. Lastly, the Computer Security Act does not require an evaluation of implemented controls (i.e., no testing). And, while OMB's computer security guidance provides more complete guidance and calls for testing of agency controls, we believe a more rigorous routine audit process is needed as well as a more prescriptive set of risk-based minimum mandatory standards for agencies to follow.

At present, there is legislation pending in both Houses that seeks to correct some of these underlying deficiencies. Among other things, these proposals call for a more comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations and assets; recognize the highly networked nature of the federal computing environment; and provide better oversight mechanisms. Such efforts could play an integral role in further strengthening the plan.

Engaging Public-Private Partnerships

The second facet of the plan focuses on developing a public-private partnership to protect our nation's infrastructure. In doing so, the plan proposes developing mechanisms and improving incentives for the private sector to cooperate voluntarily with the federal government, as well as with state and local governments, to work together to provide for the common defense of the infrastructure.

For instance, the plan seeks to establish a Partnership for Critical Infrastructure Security and a National Infrastructure Assurance Council to increase corporate and government communications about shared threats to critical information systems. It also proposes establishing Information Sharing and Analysis Centers to facilitate public-private sector information sharing about actual threats and vulnerabilities in individual infrastructure sectors. These, as well as other proposals, however, are presented in broad terms, with the intent that future versions of the plan will describe a full spectrum of specific actions and programs that have been jointly agreed upon by industry and all levels of government.

We believe this approach is reasonable given the formidable challenges involved in developing effective partnerships with the private sector. The plan itself recognizes some of these challenges. For example, it acknowledges that critical infrastructure protection is not exclusively, even largely, within the province of the federal government, and, as a result, the federal government is limited in what it can do to protect critical infrastructures. It also recognizes that while the nature of the threat to our national infrastructure has changed, the true extent of that threat, our vulnerability to it, and possible means of defense are not entirely clear. Furthermore, the plan appreciates that solutions to critical infrastructure protection must be tailored sector by sector, through consultation about vulnerabilities, threats, and possible response strategies.

At the same time the plan recognizes such challenges, it proposes several initiatives that may have a significant impact on the private sector and affected interest groups. For example, the plan raises the possibility of reviewing laws for possible amendments to remove barriers that discourage private sector companies from sharing information with government agencies about infrastructure protection issues. Specifically, it raises the idea of more explicit confidentiality protections (so that federal law enforcement or defense agencies could assure private companies that such information would not be accessible through the Freedom of Information Act) as well as changes to antitrust or tort liability laws. Because such changes could involve important tradeoffs among significant policy concerns as well as affected interest groups, it will be important to proceed carefully in addressing the concerns of affected parties while at the same time providing the incentives needed to garner private sector cooperation.

The plan also suggests increasing employer rights to monitor employees. This would provide one means of protecting organizations from the "insiders," who as a practical matter, probably pose a greater threat to organizational security than do external threats. Again, the challenge will lie in balancing individual privacy concerns with the need to protect sensitive assets and the common welfare.

These are just two examples of possible changes that may have the potential of improving the public-private partnership for information protection, but that will require extensive public dialogue before they could or should be implemented.

Mr. Chairman, this concludes my statement. The plan fulfills the commitment made on its title page: it does invite a meaningful dialogue. The plan is an engaging step forward in improving the nation's cyber infrastructure. As noted in the statement, much more needs to be done to strengthen the plan's ambitious goal of making the government a model. And serious consideration of changes in the computer security legislative framework is necessary to better assure agency compliance with good practice and process. Finally, the challenges facing the establishment of a meaningful public-private partnership require a level of continuous, long-term commitment on all sides that will be difficult to sustain but that are certainly achievable.

(511693)

Senator KYL. Senator Feinstein, would you like to make your opening statement?

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thanks very much, Mr. Chairman, and thank you for your leadership. As always, it is a pleasure to work with you.

The subject today we discuss is, I think, one of the most important we face. In my view, the security of information and networks will be the biggest national security issue of the decade and one that I think deserves the close oversight of this committee.

I think the events of the last few weeks alone remind us of the importance of information security. Just a few days ago, the National Security Agency publicly admitted what may be the biggest single intelligence failure in its 48-year history. From Monday until late Thursday of last week, NSA's computers were unable to process the millions of communications intercepts flowing in from around the world from U.S. spy satellites. The system that was down is the same one used to track terrorists such as Osama Bin Laden.

And just a month ago, on New Year's Eve no less, another critical United States spy satellite system crashed. This was the same day that numerous terrorist attacks were planned against American citizens, but fortunately prevented. And this crash occurred after the satellite system had been extensively tested for Y2K bugs.

These recent failures of some of our most important and sensitive computer systems have jeopardized our national security and the safety of our citizens. They remind us that our critical infrastructures are governed by computer networks and systems, and that if these networks and systems are disrupted or disabled, American citizens will be left vulnerable to economic disruption, to possible injury, and to possibly death.

Of course, computers not only process signals intelligence, but are responsible for the delivery to virtually every American of electric power, oil and gas, communications, transportation services, banking and financial services, and other vital needs. These computers present a tempting target to hackers, to terrorists, and hostile nations because, given our military supremacy, few adversaries would wish to fight the United States in a conventional war on a traditional battlefield.

Moreover, because so many of our computers are interconnected often through the open architecture of the Internet, there may be less reason for a hostile party to try to terrorize us with bombs, tanks, or planes. With a few keystrokes on a computer keyboard half a world away, such a party could wreck colossal damage. And every single day, someone tries to cause such damage.

In fact, the computers controlling our critical infrastructure are under practically continuous assault. Everyday, assailants make hundreds of unauthorized attempts to gain access to crucial computers. For example, last year there were some 20,000 reported attacks on Department of Defense networks and systems a almost four-fold increase from the previous year. And

many attacks go undetected, which means that the numbers are almost certainly higher than reported.

I think Americans like to think that the United States has not been invaded since the War of 1812. But, in fact, we are invaded everyday. A foreign army once burned the White House and the Capitol in this very city. But now an intruder could cause even greater damage to our Government without even setting foot in the country.

As U.S. Deputy Secretary of Defense John Hamre has said, "We are at war right now, we are in a cyber war." This war is largely invisible unless, of course, a cyber attack succeeds, and that has meant that every American is not as aware of the threat of cyber attacks as they should be. Indeed, it is hard to visualize a cyber attack.

Moreover, even if an attack is detected, it is difficult to determine who is making it and where it is coming from. Through the magic of the Internet, an attack from next door can seem to come from the other side of the world. It is much easier to think of a person or persons physically attacking sites such as Pearl Harbor, the World Trade Center, the Khubar Towers in Saudi Arabia, or the Murrah Building in Oklahoma City than mounting an electronic assault on a computer.

But it is a great mistake to think that terrorists nowadays will only, or even primarily, target government installations or military bases. In fact, 90 percent of critical infrastructure is owned or operated by the private sector. Thus, the battlefield has shifted to public and private computer networks, and society itself has become more, not less, vulnerable to terrorist threats.

While cyber threats seem invisible, they can have serious effects when they succeed, and in recent years there have been a number of incidents of that. In 1999, hackers in China and Taiwan engaged in a cyber war. One expert suggests that Taiwan computers suffered 72,000 cyber attacks in August 1999 alone, while two Taiwanese attacks on China damaged 360,000 computers and caused $120 million in damage.

In 1998, two California high school kids were among a group suspected of penetrating and compromising at least 11 sensitive computer systems in U.S. military installations and dozens of systems at other government facilities, including Federal laboratories that perform nuclear weapons research.

In 1998, a Swedish man launched a cyber attack on the 911 emergency system in southern Florida, disabling part of it. In 1998, a disgruntled New Jersey man cyber bombed his employer's computers, destroying files and corrupting backup tapes. He caused $10 million in damages. In 1997, a teenager used his computer to cripple an FAA control tower in Massachusetts. And even where assailants do not succeed, cyber attacks raise important issues about information security and information warfare.

In 1999, individuals who may have had ties to Russian intelligence—Senator Kyl just spoke about this—carried out a series of massive cyber attacks, targeting the computer systems of the Department of Defense, the Department of Energy, military contractors, and various universities.

In 1999, just days after NATO began bombing missions over the former Republic of Yugoslavia, hackers began trying to crash NATO's e-mail communications system. Experts suspect a terrorist secret society known as Black Hand.

In 1997, a Joint Chiefs of Staff exercise proved that a 35-man team who were instructed not to use any classified tools or break any U.S. law could, in fact, disable parts of the U.S. electric power grid and cripple portions of our military command and control systems in the Pacific and emergency 911 systems in the United States.

We have just begun to address the threat of cyber attacks. Presidential Decision Directive 63, issued in 1998, makes critical infrastructure protection a national security priority and commits us to protecting effectively our critical infrastructures within 5 years.

PDD–63 calls for a comprehensive National Plan for protection of our critical infrastructure within 6 months of the issuance of the directive. We now have that Plan, albeit 14 months late. I hope and am eager to examine how that Plan will work, what changes should be made to it, and how we can assist the Government in realizing the Plan's promise.

I believe very strongly that we have an obligation to protect this Nation from the threat of cyber terrorism and information warfare in a way that maintains and strengthens America's privacy and civil liberties. They may or may not conflict at certain points. That is what we are here to explore. But I think the point I want to make is the overwhelming importance of the mission. There is no question that that mission is going to grow greater in the days to come.

Thank you, Mr. Chairman.

Senator KYL. Thank you very much for an excellent statement, Senator Feinstein.

Our first witness is Mr. John Tritak, director of the Critical Infrastructure Assurance Office. He is the principal administration official responsible for the formulation of the National Plan.

Mr. Tritak, we will place your full written statement in the record and invite you to make any summary remarks you would like to at this time.

STATEMENT OF JOHN S. TRITAK, DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, WASHINGTON, DC

Mr. TRITAK. Thank you very much, Mr. Chairman, Madam Ranking Member. It is truly an honor to be here and finally to be able to discuss the National Plan. I am going to keep my remarks very brief because I think really the purpose of this hearing and other hearings is to engage in a dialog.

You will notice that the National Plan, the very cover of the National Plan says a number of things which I think bear emphasizing at this point. First and foremost, this is Version 1.0. This is not meant to be a complete document. Final solutions have not been presented.

One of the things that became very clear since taking over the CIAO and bearing responsibility for pulling this effort together is just how complex the undertaking really is. I think the PDD which calls for a plan to be presented within 6 months was overly opti-

mistic. I think it was well-intended at the time, but frankly as we got into it and saw what was entailed, it took much longer than expected.

Putting aside the fact that whenever you have to coordinate the efforts of 22 agencies, that in itself is a time-consuming process, there were really fundamental issues that had to be addressed and wrestled with. And I can say happily that what we are presenting in the Plan is, I think, a good, solid first step toward achieving the goal the President set forth in PDD–63 for developing a capacity to defend the Nation's infrastructures.

As I indicated, the goals are rather ambitious. It is calling for nothing short of an ability for the United States to be able to defend itself against deliberate attacks against its infrastructures. In order to do so, we are talking about actions that not only need to be undertaken by the Federal Government, but also State and local government and private industry.

I have said in previous testimony that this issue of critical infrastructure protection is perhaps the first national security challenge this country has ever had where the Federal Government alone cannot solve the problem. It is not a question of simply allocating resources, procuring equipment, and solving the problem. Since 90 percent of these infrastructures are owned and operated within private industry, it calls for a very new and unprecedented relationship with private industry in order to achieve a national goal.

I want to emphasize, under this goal, one of the things I add here is the importance of upholding civil liberties and privacy. After all, the whole point of this exercise in defending our Nation's infrastructures is to protect our way of life and the values that we cherish. It would do very little to serve that interest if we undermined those civil liberties and privacy rights that we enjoy today.

The challenge is not whether or not to trade off privacy and civil liberties and security, but how we protect civil liberties and privacy in the information age. When this country was formed, it began as an agrarian economy. It then moved to an industrial economy that presented those challenges to civil liberties and privacy, and we dealt with them.

We are now moving into an information age. That, too, presents new challenges. But I am confident that engaging in a dialog, which we hope will begin today and continue, will be to ensure that whatever policies and proposals are set forth by the Federal Government and whatever actions are taken to assure the delivery of critical services over our Nation's infrastructures that we continue to protect and uphold the civil liberties and privacy rights of American citizens.

By now, I hope you have both the executive summary of the National Plan as well as the full report. I will not obviously go into any great detail about the National Plan, but what I would like to do is at least provide an overview of the structure.

In order to meet the ultimate goal of defending the Nation's infrastructures by 2003, the Plan is organized around three objectives. The first is to prevent such attacks from occurring and, should they occur, to minimize the effect those attacks may have on the delivery of critical services.

One of the first and important steps in doing so is to evaluate what the critical assets that perform these critical services and deliver these services are; having done so, identify both the interdependencies with private industry as well as the interdependencies between government agencies, identify those vulnerabilities and develop plans for addressing them.

Second is to develop an ability to detect, analyze, and evaluate intrusions and attacks against our Nation's infrastructures, and develop plans for responding and reconstituting those systems. Under this objective, we have four broad programs.

One is to develop a multitiered detection, intrusion, and warning system that will enable government agencies to determine whether or not an attack is underway and to be able to deal with that information in a way that contains the problem and doesn't spread to other agencies and affect delivery of critical services.

Second is to develop the intelligence and law enforcement capabilities with a view toward focusing on critical infrastructure protection; three, to encourage information-sharing both between government agencies, within private industry, and between government and private industry. Fourth is to build on the lessons of Y2K and to begin to explore ways in which the Government can facilitate response, reconstitution, and recovery.

Finally, objective three, Senators, is really what undergirds the achievement of objectives one and two. It involves coordinating research and development among Federal agencies to ensure that there is not unnecessary duplication. It involves training and employing IT security experts.

Today, there is, in fact, a shortfall in this capability. We need not only to ensure that those who are already responsible for this mission have state-of-the-art training, but also to encourage the recruitment of new expertise into the Federal Government, as well as in private industry.

Three, raise cyber security awareness. I think it is fair to say that one of the biggest challenges to this effort overall is awareness and appreciation of what we are talking about. This need for awareness is not only at the Federal Government level; it also requires raising awareness within private industry about how this is different from the challenges that they faced in the past, and, finally, to raise awareness with the American public itself.

Fourth is to develop and explore legislative and legal reforms that may improve information-sharing. One of the important ways in which this country can defend its infrastructures is to share information within the Government and between government and industry. We need to look at ways in which we can encourage that without those that are sharing the information incurring unnecessary liabilities. And, finally, to repeat yet again, all this has to be done within the context of protecting civil liberties and privacy rights.

In the rollout of the National Plan, President Clinton mentioned briefly his budget overview for critical infrastructure protection. As this chart indicates, the request will be for $2 billion, which will be a 15-percent increase over last year, with 85 percent of that budget being used to actually protect the infrastructures of the re-

spective Federal Government agencies, with the remaining 15 percent being used for outreach programs with private industry.

Seventy-two percent of the total will be requested for the national security agencies. They bear a very special responsibility in this critical infrastructure area, so it is appropriate that they would at this stage get the lion's share of the budget. Also, the national security agencies have the most mature programs, and one of the goals of this Plan is to begin to rectify that balance by bringing up to speed the civilian agencies. And then, finally, a 31-percent increase in research and development in programs designed to address specific challenges of critical infrastructure protection.

Finally, Senators, I would just like to highlight very briefly some of the key initiatives, the goal of which is really two-fold. One is to establish the Federal Government as a model for information security. Recognizing that we are asking private industry to bear an increasing responsibility for the defense of the Nation's infrastructures, it is important that the Federal Government itself be a model of information security and computer protection.

We have laid out a number of initiatives designed to do that. First and foremost is to develop the personnel within the Federal Government to do this. As I have indicated before, there is, in fact, a shortage of information security expertise, not only within the Government but within private industry. The ability of the Federal Government to draw that expertise, given the enormous market pull for people coming right out of college to go to private industry—we are exploring a number of ways in which we can recruit and retain some of these people to build a cadre of information technology expertise within the Federal Government.

One of the principal programs in that regard is a ROTC-like program called the Service for Scholarship Program which is designed to assist undergraduates and graduate students through their education, with the understanding that upon graduation they would serve a certain period of service within the Federal Government.

FIDNet, of course, I have a feeling we are going to be talking about in some detail, so I will come back to that when we have our discussion.

Senator KYL. I wish you would discuss it now, if you would.

Mr. TRITAK. Oh, absolutely. Senator, the Federal Intrusion Detection Network is intended to serve, in essence, like a Federal burglar alarm for civilian government computer systems. It is designed to allow Federal agencies to protect those critical computer systems that the public relies on for delivery of important services. This system is only government civilian systems. It does not connect in any way to private sector computer systems.

The Department of Justice has actually undertaken a preliminary review of the FIDNet concept and has determined that it is compliant with existing Federal laws under ECPA. The key issue here, Senator, is to recognize that daily, as you have indicated in your testimony, and as Senator Feinstein has indicated in her testimony, Federal Government agency computer systems are, in fact, being attacked. Some of the information out of those computer systems is actually vital to the privacy rights of American citizens.

This problem is not going to go away. The question is how we are going to deal with it. The current proposal for the FIDNet is

for a pilot program. The concept as it is right now, we believe, is consistent with all privacy statutes and civil liberties statutes. As it goes on through development, at each stage it is going to have to be reviewed to ensure that compliance is adhered to.

At each stage, we will be discussing with you, the private sector community, and others how this is being implemented so that there is an understanding and there is an acceptance of what we are doing from the get-go. Of course, at this point some of the legalities of this matter actually turn on very technical details and design features. That is why it is impossible at this stage in the concept to say how it will work and what it will do and what will remain compliant. What I can assure you is that whatever architecture is actually developed for the FIDNet program, it will be consistent. If those architectures are not consistent, they will not be adopted.

I would like to now turn, Senators, very quickly to the need for building public-private partnerships. The President announced in his rollout address the establishment of an Institute for Information Infrastructure Protection. The purpose of this institute is not to create a new building, a new establishment to duplicate ongoing efforts in infrastructure protection. The goal here is to really fill gaps in what may exist in critical infrastructure protection.

As you know, with the President announcing CIP as a national priority, agencies do have ongoing efforts to address their own needs in this area. However, since much of what is needed for infrastructure protection lies within private industry itself, it is important to have a mechanism by which government and private industry can work together to identify potential gaps where the market itself does not permit a solution and to ensure that monies from the Federal Government can be inserted back into private industry to develop high-risk, high-payoff technologies which will benefit not only private industry but, by extension, the American people.

Finally, Senator, I would just like to touch briefly on the Partnership for Critical Infrastructure Security. This is an area I am particularly proud of because what it is trying to do is bring together all the communities that are necessary to resolve this issue.

Today, we have lead agencies interacting with their private sector counterparts to address sector-specific concerns of critical infrastructure protection. What we are trying to do in this effort is to draw those efforts together and to include a broader community of business interests, to include the risk management community which is going to be responsible for assessing, creating metrics, and holding accountable companies to first adopt and then enforce security measures on their computer systems. It will also include the broader business community who actually depends on these critical infrastructures in order for them to do their business.

We envision as this partnership evolves that we also will include the privacy community and others who have a stake in this outcome. I can tell you the first meeting was held in December. Over 90 companies attended. It was chaired by Secretary Daley. We are now moving to the first working group session later this month, in which industry is actually taking the lead on identifying those issues of concern with regard to critical infrastructure protection. So what we are really trying to do here is to develop a real partner-

ship where hopefully we will discover market solutions, allow the market to come up with solutions as to how to deal with these problems and not regulation.

Senator I think at this point I will conclude my remarks, and I welcome any questions.

Senator KYL. Thank you very much, and I am sure that overview at least indicates the breadth of the effort that is being undertaken here. While both Senator Feinstein and I have been critical of the administration for not acting with enough speed in this matter, we both recognize, I am sure, that it is a complicated and ongoing challenge that will require, as I said, a continuing evolution in your program. And that is fine, but it is important to start and we are at least appreciative of this report on that effort.

One of the interfaces with this program that the Judiciary Committee will have, of course, is determining whether there are any legal changes that will be necessary in our laws to help implement this or to ensure that as it proceeds it can, A, be effective, and, B, not improperly infringe on any constitutional rights of Americans.

I made the point, and I tried to stress the point in my opening statement that if we do nothing, Americans' privacy will, in fact, suffer. I mean, the whole point of providing protection to our infrastructure is to prevent unauthorized entry into these systems in a way that can compromise people and government and businesses' private information. So the whole point of this is to protect the American public.

There are those, on the other hand, who view the effort in some respects as potentially damaging to civil liberties. And I would like to focus on that because of all the areas in which this subcommittee will be working with this critical infrastructure issue which has ramifications that apply to many other committees here in the Congress—the Government Operations Committee, the Intelligence Committee, the Armed Services Committee, and so on—our committee's jurisdiction will surely impact this privacy issue. And so I wanted to focus in on that and that is why I asked you to talk a little bit more about FIDNet.

Now, what I would like to do as a prelude to asking you some specific questions is to describe with a little bit more particularity the kinds of information that you anticipate will be collected and analyzed on the FIDNet program, and if you could also describe the degree of maturity of the program. As I understand it, you are basically just getting this off the ground right now.

So could you address that briefly and then talk about the kinds of things—in other words, how you envision this working. You might want to even use an example. Let's say we find that there has been a particular kind of incident. How would we be reacting to that, at least hypothetically?

Mr. TRITAK. Certainly, Senator, I would be happy to. First, to underscore the remark that you made in closing your question, and that is that we really are just getting off the ground. What we have done so far——

Senator KYL. By the way, may I interrupt you and acknowledge the presence of Bob Bennett, the Senator from Utah, who chaired the very successful Y2K—we just call it the Y2K Committee. But while Senator Bennett probably would not personally want to brag

about this, I figure that the whole reason we didn't have any problems with Y2K is because of the work of his committee. Of course, I served on the committee.

Senator FEINSTEIN. You are humble.

Senator KYL. That is right.

But since Senator Bennett is not a member of the Judiciary Committee, I wanted to acknowledge his presence here before you gave your answer and indicate we will, of course, offer him an opportunity to make some observations and ask questions here as well, and we appreciate him being here.

I am sorry to have interrupted you.

Mr. TRITAK. Senator Bennett, it is good seeing you again.

On FIDNet, Senator Kyl, first let's step back a little bit and let's clarify what FIDNet is and what it is not. It has been characterized as many things, including being a big brother system, or a slippery slope to it. It is nothing of the kind.

To begin with, as I have indicated, what we are talking about here is a civilian computer intrusion detection system within the Federal Government. Currently, today, an agency can install intrusion detection systems at critical computer sites. It can monitor the flow of traffic coming in, with a view toward identifying potentially anomalous activity going on, a virus, for example. When anomalous activity is done, systems admin. today can review that information to determine what is going on and what needs to be done. That authority exists today.

What FIDNet is proposing—well, let me say one more thing about that. Of course, given the nature of certain types of attacks, what you will generally see are mappings that an attacker will use at different agencies to try to develop an overall plan before they actually attack a specific system. They are not going to telegraph their intentions too clearly.

So what could be happening at one agency may only be a small bit of what, in fact, is going on around, which could actually be amounting to something very serious. No agency alone is going to be able to make that determination or ascertain what is, in fact, going on. So what the FIDNet is proposing to do is in instances where anomalous activity has been detected, the information about that anomalous activity will be provided to the FEDSIRC, which is at GSA, for further analysis, and to correlate other data of anomalous activities occurring around Federal agencies to determine what that anomalous activity means.

In the event that that anomalous activity appears suspicious or even indicative of crime, that information would then be further provided to the NIPC for analysis and if, in fact, they determine that there is evidence of criminal activity under Federal law enforcement.

There are several tiers going on here to ensure the protection of privacy. Right now, if a systems administrator detected anomalous activity and concluded that there was evidence of criminal activity, they are obligated under law to provide that information directly to Federal law enforcement.

Some anomalous activity is, in fact, ambiguous; it is not clear what it means. You wouldn't want to send that to Federal law enforcement, and that is not what is intended here. What is intended

here is to be able to make sense—drawing on activity going around Federal agencies, to make sense of what that anomalous activity means for that agency as well as for the Government writ large, because in some instances that may be our first indication that something is up.

If something is up, as I have said, and it suggests malicious intent or even potential criminal activity, there is a mechanism for providing that information on to the NIPC for Mr. Vatis and his team to evaluate. At this point, Senator, this is where the concept of FIDNet lies. Now, there are a lot of details as to how that information is processed, how it will be moved on to the FEDSIRC. And that is why I said that beyond a threshold assessment, a preliminary assessment, we need to further develop the FIDNet program with specific technical options.

There will be RFP's issued, assuming that there is some seed funding for it, and then those technologies and capabilities will be assessed within the broader architecture to ensure compliance with existing privacy laws. I say ensure continued, as opposed to moving forward in the hopes that it will fit privacy or, in fact, requesting that privacy laws be changed in order to accommodate the system.

Senator KYL. What kind of data will be collected by the FIDNet program?

Mr. TRITAK. The information that is monitored on an intrusion detection system is really looking—basically, it is set up to look for anomalous patterns. That information, if the alarm would go off, would be extracted and that information would then be provided to the FEDSIRC for further analysis.

Now, the details of what is contained in that packet, what would be kept at the agency where it is allowed to be kept and what would be moved on further for further analysis, is something that really is a technical detail that I am not in a position to answer right now because I don't know the answer.

Senator KYL. OK; now, what is the potential then for integrating the private sector—let's say the commercial banking computer system—into this overall program and interfacing with FIDNet to provide the burglar alarm for a private sector computer network as we have with the Government network?

Mr. TRITAK. In short, none.

Senator KYL. So the FIDNet program is designed to detect intrusions into the Government interconnection of computers, detect the nature of the activity, and if it is potentially in violation of law, refer the appropriate information to the FBI?

Mr. TRITAK. That is correct, sir.

Senator KYL. One of the subsequent witnesses, Mr. Rotenberg, says that there are—and I am quoting now—there are other indications contained in materials that they received under the Freedom of Information Act that the CIAO, which you lead, intends to make use of credit card records and telephone toll records as part of its intrusion detection system, and suggests that that raises problems under U.S. law. Is that correct?

Mr. TRITAK. Senator, I have to be honest with you. I don't know where that comes from. I think, in fairness, what it may be referred to is that telephone companies have developed technologies that look for certain patterns to suggest that someone may be

using a credit card that isn't theirs, you know, activities which are beyond the normal patterns of activity that the person who owns that credit card would do.

Under those circumstances, there is an alert and those people are actually contacted to find out is this purchase—did you intend this purchase, is this your purchase, and it is really a service actually to the customers.

Senator KYL. As a matter of fact, I can tell you one of my employees had a cell telephone, got a bill with, I think, $600-and some worth of telephone calls to Mexico. And about a day later, she got a call from the company saying this doesn't look like an expenditure that is consistent with your past use of your telephone. She said, it is not; she said, I didn't make those calls. They said, we didn't think so, don't worry about it.

And this is part of the basis for the bill which came out of this subcommittee a couple of years ago on cell phone cloning to try to make it easier to prosecute people who do that. So this was a use of information to help a consumer, a customer who clearly was being taken advantage of by someone. Is that the kind of information that you are talking about here?

Mr. TRITAK. Actually, I want to be very clear. It is not so much the information. It is the technology that helps identify certain patterns of behavior. First of all, I am not a technologist, so I am doubly handicapped. But one of the problems is that when you actually talk about how you identify certain types of patterns that are suggestive of anomalous behavior, we are talking about levels of detail and technical gradients that are very difficult to communicate in normal language.

What I think was referred to in Mr. Rotenberg's statement—I obviously don't want to speak for him, but my understanding to the extent that that ever came up was the fact is right now there is a capability that can identify anomalous patterns. In this case, it happens to be use of credit cards, or it could be the use of the telephone.

It is the underlying technology that led to the creation of that capability which is what I believe was one thing that was raised as something to explore, not so much because we are looking at collecting that sort of information or information about a person or anything else that would be used in an intrusion detection system.

Senator KYL. And this is one of the reasons why you said that you would be careful as you went on to ensure that any use of that technology would not invade privacy.

Mr. TRITAK. That is correct, sir.

Senator KYL. And I will, of course, give Mr. Rotenberg a full opportunity to explore his views on this later, but he also says that based on a March 1999 memo from the Justice Department to CIAO, FIDNet is a violation of the spirit of the Federal wiretap statute, also the plain language of the Federal Privacy Act and contrary to the fourth amendment.

What is your view on that?

Mr. TRITAK. Well, I have to try to remember law school, but I recall that wiretapping has to do with voice communications, and we are not looking at that there. We are talking about traffic that is coming in mainly e-mail.

Senator FEINSTEIN. Say that again.

Mr. TRITAK. I am sorry. My initial reaction, having not had an opportunity to think through this as fully as perhaps I need to, is that wiretapping refers to voice communications. We are not looking at monitoring voice communications through an intrusion detection system. The intrusion detection system is designed to identify incoming e-mail traffic that may contain anomalous malicious code or something, which may then actually go into a computer system and cause damage. So we are really monitoring different things.

Senator KYL. One thing I would like to ask you to do is to consider carefully the testimony of the second panel and to perhaps respond to any points that you think are worth—I shouldn't say worth responding to, but need response to ensure that there is a complete understanding of the FIDNet program from your point of view. And we would leave the record open for sufficient time for you to respond to any comments that you think require response.

I realize that we are catching you a bit unprepared on these matters today, and perhaps at a subsequent hearing we can have the people who really are the experts either in the law or in the technology to further explore these issues.

Mr. TRITAK. Senator, let me also add that in terms of some of the things that you raise and Mr. Rotenberg will be raising in his testimony, I think we need to take all that seriously. All concerns about privacy should be taken seriously and we ought to address them front-on.

I gave you answer about the wiretap law. I am not even sure if it is correct. What I will do, though, is once it is raised, to the extent I can respond to it today, I will. To the extent I cannot, we will provide written answers specifically to those.

Senator KYL. Great, and I have some additional questions which I will submit to you.

[The questions of Senator Kyl are located in the appendix.]

Senator KYL. I would like to turn to Senator Feinstein now. Senator Bennett, by the way, said he would be able to be back.

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

Mr. Tritak, just a quickie. On page 29 of the report, in the chart it mentions that Federal departments and agencies will submit a multiyear vulnerability remediation plan with their fiscal year 2001 budget submissions to OMB, and then annually afterwards. The ERT will work with the departments on implementation. That is due to be completed in June 2000. Are you going to make that date?

Mr. TRITAK. Yes; let me make sure I—page 29, you said?

Senator FEINSTEIN. Page 29, third one down, Federal Department Initiatives to Strengthen Cyber Security.

Mr. TRITAK. OK, and that would be——

Senator FEINSTEIN. 1.3.

Mr. TRITAK. Yes; well, each of the agencies, in fact, will have contained in their budget plans for dealing with their vulnerabilities and remediating——

Senator FEINSTEIN. So that will be on time and this subcommittee can expect it?

Mr. TRITAK. Yes; that is not to say it is going to be complete, and I will tell you that one of the things we are actually undertaking at the CIAO is to assist agencies in sort of focusing very clearly on what it is that they need to do in order to fulfill the missions of PDD–63, and that is to actually go into their agencies and identify those assets that support national critical services, either in national defense, promoting of economic security, or delivery of vital human services, and having identified those assets to back into it to identify with the nodes and networks that support those and then conduct a vulnerability assessment.

With the institutionalization of the ERT, they will then go in and say, OK, let's take a look at those nodes and determine to what extent they are vulnerable and what do we need to do to address them.

Senator FEINSTEIN. I just view that as an important step.

Mr. TRITAK. Very important, ma'am.

Senator FEINSTEIN. And I just wanted to see if it was going to get done on time.

Now, let me just read you a couple of sentences out of the GAO draft report on critical infrastructure protection.

> In particular, we believe the Plan should place more emphasis on providing agencies the incentives and tools to implement the management controls necessary to assure comprehensive computer security programs, as opposed to its current strong emphasis on implementing intrusion detection capabilities.

Then it says,

> In addition, the Plan relies heavily on legislation and requirements already in place that, as a whole, are outmoded and inadequate, as well as poorly implemented by the agencies.

Could you define for us the outmoded and inadequate legislation so that we might do something about it?

Mr. TRITAK. Well, I believe that what may be referred to may be certain aspects of the Computer Security Act. I have not done, in fact, an analysis or studied closely what GAO has said in this regard. I would rather take that question and get back to you than to simply talk off the top of my head.

Senator FEINSTEIN. Would you, please?

Mr. TRITAK. I would be happy to.

Senator FEINSTEIN. This is directly within our jurisdiction to update whatever legislation is outmoded and inadequate. So if we could get that with specificity in the next week, if possible?

Mr. TRITAK. Yes, ma'am.

Senator FEINSTEIN. Great. Thank you very much.

Just a couple of quick questions on your burglar alarm, FIDNet. What is the legal authority for FIDNet?

Mr. TRITAK. Well, the legal authority for FIDNet—I guess I would sort of address it slightly differently. Is FIDNet consistent with existing legal authority? One of the initial analyses that had to be done was whether it was consistent with ECPA, the Electronic Communications and Privacy Act. I usually only refer to it by its acronym.

That makes very clear and puts very severe restrictions on the monitoring of content in electronic communications. However, it does also have some significant exceptions in order to protect Federal Government information systems.

Senator FEINSTEIN. But you are saying the legal authority is within that Electronic Communications and Privacy Act?

Mr. TRITAK. Right.

Senator FEINSTEIN. OK.

Mr. TRITAK. Now, it also needs to be consistent with other laws, but that is one which we did as an initial matter. And there was a preliminary, and I emphasize preliminary, examination by the Department of Justice which found it to be consistent.

Senator FEINSTEIN. Now, Senator Kyl mentioned the wiretap law. Do you agree with Justice that FIDNet must operate under the Federal wiretap law?

Mr. TRITAK. Senator, I am going to be honest with you. I am going to need to take that question. I am not prepared to answer the specific legal authorities with respect to FIDNet and the wiretap law, and I think they deserve a thorough review and response than what I can give you at this time.

Senator FEINSTEIN. I appreciate it.

Mr. TRITAK. I have a few tasks now to get back to you very quickly on, and that will be one of them.

Senator FEINSTEIN. Thanks. Do you see any legal problems with GSA acting as a centralized authority with regard to protection against network intrusions for the entire Federal Government?

Mr. TRITAK. I do not. I understand that there is the view, although there has not been a formal legal opinion issued at this time on this, that the GSA can serve as sort of a super systems administrator in connection with the FIDNet program, meaning that since it has authority to oversee all government agency information and computer systems——

Senator FEINSTEIN. That includes Defense, of course?

Mr. TRITAK. Yes, although in this case the—yes, but in this case the Defense Department has its own system entirely and the FIDNet is not actually going to be tied into that.

Senator FEINSTEIN. So FIDNet would not relate to——

Mr. TRITAK. No; in fact, I am glad you said that. Right now, there is an intrusion detection system at the Department of Defense and that system has been up for a while. In fact, as we proceed in developing FIDNet, obviously we want to benefit from the experiences and lessons learned that the Department of Defense has made in proceeding there. But this is only for non-DOD Federal civilian government agencies. It is not networked into the Department of Defense.

Senator FEINSTEIN. Under the current version of FIDNet, there would be a large new intrusions operations center at GSA. Does this duplicate the mission of the National Infrastructure Protection Center?

Mr. TRITAK. I do not believe it does. The way FIDNet was designed, first of all, it is very clear in ECPA that the systems administrator cannot be an agent of law enforcement. Now, I am not saying here that the NIPC is, in fact, an agent of law enforcement be-

cause it is not. It is, in fact, an agency designed to deal with indications of warning and analysis.

But the decision was made, in an abundance of caution, to locate the FIDNet analysis center, if you like, or what actually would be located at FEDSIRC—is to provide a place where correlation can be done and an assessment of what anomalous activity means. And only in cases where that anomalous activity rises to the level of suspicion and perhaps indicative of criminal activity would it then further sent to the NIPC for analysis and they would make the final determination of sending it to law enforcement based on their own expertise and experience that they believe it needs to move.

Senator FEINSTEIN. A final question. The GAO report points out that its audits have found repeatedly serious deficiencies in the most basic controls over access to Federal systems. It points out that managers often provided overly broad access privileges to very large groups of users, and that affords more individuals than necessary the ability to browse and modify or delete sensitive or critical information.

What are you going to do about that?

Mr. TRITAK. Well, as you have indicated earlier, and I think it bears repeating here, critical infrastructure protection is not going to be solved by technology alone. It is only as good as the personnel, the technology, and the processes that are put in place to do it. Your best intrusion detection system, your best technology for combating cyber terrorism goes out the window if it is not employed properly.

There is, in fact, an effort underway, and it is contemplated in the National Plan to develop more uniform standards across the Federal Government and to raise awareness with government employees on the importance and need for observing proper practices and standards for information security.

I agree that right now the Government is not the model of that. More works needs to be done. By the way, it is also not wholly observed within private industry, and I think you would find—and I think this is something you would really need to talk to Mr. Vatis about, but probably many instances where there have been problems, only some of them are because of technological flaws. Some of them are because people were not observing common security practices which, had they been observed, they may have avoided the problem.

And this a big issue for the information technology community because to simply say something is vulnerable is suggestive that the vulnerability lies squarely with the technologies, when, in fact, the vulnerability is systemic and it requires dealing with all three.

Senator FEINSTEIN. You mentioned earlier that you are going to begin recruiting students and training students, et cetera, to come into this. In our classified briefing, Senator Kyl and I heard about this, and my concern has been that that is going to take a very long time. And I wondered if, particularly with respect to this security aspect, you had considered recruiting from the private sector for a small period of time, say 6 months to 1 year, the outstanding security experts that we can throughout America to really, in essence, do a kind of audit of our departments, our management and security functions, and make some specific recommendations.

Mr. TRITAK. Well, first of all, Senator, let me say that I think that is an excellent idea.

Senator FEINSTEIN. But will it die an early death?

Mr. TRITAK. Not necessarily. I think the only problem is that industry itself is finding a shortage. I mean, they are desperately trying to fill these positions themselves. That said——

Senator FEINSTEIN. I talked to one company that is in the lead in this direction. I would be happy to tell you afterwards.

Mr. TRITAK. I would love to hear who that is. That would be great. In fact, I would say even when we get the scholarship program going, if all goes well and if we get full funding, we envision that the first graduating class having been trained through these programs would be May 2002. So we are trying to put this on a fast track as much as possible.

But I think even if we did get this program going, there needs to be some kind of ongoing interaction between private industry and the Federal Government in this because, first of all, I think industry actually has an interest in the Federal Government having secure computer systems. They, in fact, depend on some of these systems for their own businesses.

And, second, the experiences that are gained in the Federal Government are likely to be different in some respects from the kinds of experiences they have in private industry. Since government in some cases is one of the front lines of attack against hostile forces, that kind of experience in how to deal with it and respond to it would be extremely valuable to private industry.

So I think that is a very good idea, and I would actually like to speak to you afterwards about the companies who have indicated a willingness to volunteer to support Federal Government programs.

Senator FEINSTEIN. Thank you very much. I appreciate it.

Mr. TRITAK. Thank you, Senator.

Senator KYL. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman. I very much appreciate your indulgence in letting me participate in this way, and I apologize for going in and out. We were in the process of trying to gather a quorum up in the Banking Committee so we could report out Alan Greenspan. We have successfully done that and so I am here now.

I want to express my appreciation to you for your hearings not only now, but previously. I think, as I have said previously, that this issue is one that is going to be with us a long, long time. It is only going to increase in its intensity and its importance and we are just at the threshold of beginning to understand it.

I have brought along a little visual aid this morning, Mr. Chairman, and you can't see it too well from where you are. I wish it were on a white background instead of a black background, but that is a map of the world. Some people think it is an abstract painting. Maybe someone could hold it up and show it to the audience as well.

That is a map of the world, only it is a map of the Internet. The most outstanding thing about that when you look at it as a map of the world is that there are no oceans and there are no continents. And when you start talking about either national security

threats or commerce in a world in which there are no oceans and no continents, you realize that we are not talking about a new tool to use in commerce or a new weapon to use in war. We are talking about a whole new place. We are talking about a whole new universe that is different from any that we have structured our Government to defend or our economy to market in in the past. That is why these hearings are so important and the issues that we are addressing are so important, and they are going to go on and on.

Now, in May 1998 President Clinton signed PDD–63, calling for the development of a detailed Federal Plan, and we are having the hearings now on the first cut of that Plan. It was finally released this month. Unfortunately, it is over a year late from the date that was set in PDD–63. It is an invitation to a dialog, as the Plan itself says, and this hearing is going to be part of that dialog.

Now, in my opinion, Mr. Chairman, there are two main problems with the Plan. I don't mean to start out being critical because I start out being grateful that we have it, that we have something to talk about. But here is my reaction to it.

First, the architecture of the Plan is flawed, the structure is wrong. The FBI is given the coordination function, which immediately raises suspicions on the part of industry and questions about the role of the Department of Defense. The greatest area of expertise in this challenge lies with the Department of Defense and the National Security Agency, and they are under the coordination of the FBI. That is one of the reasons why you are holding this hearing, Mr. Chairman, because the FBI is under the jurisdiction of the Judiciary Committee. But the question about the FBI's expertise as opposed to that contained within the DOD and the NSA is a structural question that immediately comes to mind.

The second part of the first problem—the first problem is the structure and now I am giving subtopics under that. The second subtopic is that the Plan seems to me to focus primarily on the hacker threat. I listened very carefully to the President during the State of the Union message when he raised this, and again I applaud him for raising it, and he too stressed the hacker threat, the threat of irresponsible hackers.

I think the broader threat that we face long term is going to come from terrorist groups and eventually, if not immediately, from hostile nation states that have the staying power both financially and technologically far beyond that of a teenage hacker operating out of his bedroom. And I wish the Plan had focused on the broader threat of information warfare and not the more narrow threat of a rogue hacker.

The third subpart of the flawed architecture is that the Plan does not yet articulate a strategy for reconstitution and recovery if an attack occurs. We had the experience in the Y2K Committee of talking about contingency plans, and one of the reasons that Y2K went so smoothly is that in many areas contingency plans simply took over flawlessly and seamlessly.

And people said, gee, there was no Y2K failure, when, in fact, there was, but there was no suspension of service because the contingency plan was working. That is an analogy for the focus on reconstitution and recovery, and there is nothing in this Plan that focuses on that.

And the final aspect of the architecture that—well, I have already talked about it; that is, that the role of DOD and NSA is unclear, and those are the two agencies that have the most expertise.

The second major problem with the Plan—this is parochial, in a sense, because it looks at it from the standpoint of the Congress. The Plan makes it almost impossible to follow the money. Approximately nine committees in the Congress have some kind of critical infrastructure protection oversight responsibility. There is in the President's budget $2.04 billion spread over 15 agencies, and it becomes very difficult to follow the money, very difficult for Congress to provide its appropriate oversight responsibility when things are fractured that much.

I would note that in the 2001 budget tagged for critical infrastructure protection, $276 million is new funding. That is more than a 10-percent increase, closer to a 12- to 15-percent increase. I don't object to that increase. I think the issue is serious enough that it justifies that increase, but it becomes very hard to focus when the thing is spread so wide.

So, Mr. Chairman, I give the President and the administration high marks for proceeding. I am glad the National Plan is finally before us, even at this late date. I know how devilishly difficult it must have been to put together, and so I don't fault the administration too much for being a year late. But I have to lay down my immediate concerns in these two areas, and very much appreciate the opportunity to share that with you this morning.

Thank you.

Senator KYL. Thank you very much, Senator Bennett. As a matter of fact, Senator Feinstein and I were just talking about the criticisms which you leveled. These were criticisms that were raised in earlier hearings that we had, as a matter of fact, prior to the actual development of the Plan when we asked whether or not it wouldn't be more appropriate to have a larger role for the Defense Department, given the fact that our national security is implicated when there is attack on other government agencies than the Department of Defense. That remains an ongoing concern that we have. We continue to evaluate that and look into it with your assistance, as well.

Senator BENNETT. Mr. Chairman, if I could raise an example that I use sometimes when I give speeches on this subject—and I will be giving another one around noon—we have in Utah a steel mill, a very unusual place to put a steel mill in the middle of Utah, next to Utah Lake. It was put there in 1942 for strategic reasons.

The Government was afraid that a steel mill built in Senator Feinstein's State might be subject to attack from the Japanese. They wanted to put it far enough inland that a Japanese bomber wouldn't be able to get to it. Steel mills, as you know, require a fairly large body of water, and there is a lake in Utah that was big enough. So this mill, which is known as the Geneva Steel Mill, because they thought Utah Lake looked a little like Lake Geneva in Switzerland—U.S. Steel built the Geneva Steel Works on the borders of Utah Lake in 1942 as a defense initiative. We needed more steel for our defense purpose and we wanted to protect it.

Now, if the Japanese were to decide that that steel mill was essential to our war effort and that they had to take it out at almost

any cost and launched a bomber from a carrier off the coast of San Francisco to fly to Provo, UT, to try to destroy the Geneva Steel Works, the responsibility of defending that steel mill would obviously fall to the Department of Defense, or in that case the War Department. We didn't have a Department of Defense in 1942.

The responsibility of shooting down that bomber would lie with the Army Air Corps, very clear lines of jurisdiction. And if something happened to the steel mill, the War Production Board would be responsible for trying to get it rebuilt, or that capability rebuilt.

Today, if a hostile nation were to decide that an installation somewhere in the United States was critical to America's defense effort and they were to decide they were going to take it down by a cyber attack, whose responsibility is it to defend that facility? It is nowhere near as clear-cut as the old paradigm, and that underscores what I am trying to say.

We are in a whole new place now. Does the FBI have to defend that critical segment of our economy against foreign attack? Does the National Security Agency have a defense role or is it strictly informational? Who is responsible for reconstitution?

And I would ask you, Mr. Tritak, if I am allowed, do we need an EFEMA? We have spent a lot of time in Y2K talking about FEMA and reconstitution, as I have said. Do we need an EFEMA? Does that need to be part of the Plan? These are the kinds of issues that are much easier to raise than they are to solve.

But I put in terms of the analogy of the steel mill to indicate how differently the world operates now and how the old compartments of responsibilities no longer apply. And your responsibility down at CIAO is to give us all the answers to these terrible problems.

Senator FEINSTEIN. Mr. Chairman, before Mr. Tritak responds, would you add the example you just gave me on the oil because I think it is relevant?

Senator KYL. Sure. There are so many different examples. The point is that while the defense and related national security groups are in charge of their own security, as Senator Bennett points out, there are innumerable implications to national security from attacks on other agency computers.

We were just talking about, for example, the computers that may keep track of world oil shipments and the like. What if those are infiltrated for purposes designed to harm U.S. national security? You know, the Commerce Department computers may not be under the jurisdiction of the Department of Defense, but does GSA or FBI or Commerce have the ability to do the kinds of things that Senator Bennett talked about? No; the Defense Department is the one that ought to be involved in that.

That is why, as I say, these questions were raised earlier on, and maybe you could provide an answer to some of the questions that Senator Bennett has raised as to why the Department of Defense wasn't more closely integrated into this overall Plan.

Mr. TRITAK. Well, let me say that the issue you have raised about the information age knows no boundaries, whether national, bureaucratic, private, public, is probably one of the most significant implications and is going to require us to really look very closely at what do we even mean by national security anymore.

It was very clear when the threats were from a foreign intruder that had to cross a boundary or our air space what needed to be done. That wasn't the question. It is a lot more difficult now. Obviously, no one wants a solution where we create a veritable police state and the Nation's infrastructure needs to be posted with guards or net force-type capabilities on every computer system that may bear some effect on the national economy. On the other hand, as you have pointed out, the way our bureaucracies are currently organized, there are clear lines of responsibility that don't really reflect the new demands that are being posed by the information age.

I don't want to be in a position to define for the Defense Department what they view their mission is. I believe, however, it is fair to say that one of the missions they do have is to ensure that the infrastructures of this country that are necessary for the projection of power overseas or to mobilize war is, in fact, a concern of theirs and they have, in fact, been working on it.

So it wouldn't be true to say that they don't do infrastructure protection within the United States, but it is with a very clear focus on the Defense Department's missions. And when you go beyond that to talk about the defense of the Nation's infrastructures that are necessary for economic security and delivery of human services, we get into a much more complicated set of circumstances.

I am sad to say I don't have the answer to your question right at the moment. But what I will say, though, is going back to something that you raised actually in my first hearing when I was on the job about 2 weeks, and you raised to me a question that has over time really struck me as really at the core of what we need to be turning to next, having gone through the Y2K experience, and that is we accept the fact that the Nation's infrastructures are mainly privately owned and that the industry itself and the market should bear most of the responsibility for reconstituting those systems should they fail.

That was clearly the goal of Y2K and, in fact, they did a very good job. Owners and operators of infrastructures have had to deal with disruptions, whatever the cause, for at least 100 years. And this new information age is going to complicate that because as more and more of their business operations go online or become part of computer-controlled networks, they may become more susceptible to deliberate disruption.

So we recognize that perhaps the first way to deal with this is to raise the awareness with industry that this is a problem that is emerging and what the threats are. There are programs underway for the NIPC to brief industry on what is actually going on to try to raise that level of awareness. We are also as part of this partnership trying to raise this as basically a case for action, that regardless of the source of the disruption, they can't afford to have their systems go down.

And the hope there is that the market itself will go a long way to dealing with this problem, and then when there is a shortfall between the two, that is really where government and private industry need to work together to solve it.

Senator KYL. If I could just interject and then we do need to turn to our other panel, the problem is that industry is working with cross-tensions here. In a competitive age, in a deregulatory envi-

ronment, it is not very cost-effective for Energy to build in robust backup kinds of systems. And the net result is that a lot of the systems are more fragile than they used to be when you had monopolies and the Government was ensuring that they had the money available to build this robustness into the systems.

And I think particularly of communications and the Defense Department and the national security Agencies and the other parts of our Government relying to a significant extent on literally commercial satellites which are very vulnerable. Our communications, our transportation system, and certainly our energy grid all serve both defense and nondefense needs. And in all three of these areas, there are vulnerabilities that didn't exist before that do exist now that are the business of the United States from a defense point of view, and this is a point that both Senator Bennett and Senator Feinstein have made.

I think there will need to be more analysis of how the Defense Department and the NSA and other agencies can interface with the system that is being developed here. Placing it where it has been placed has been a conscious decision. I am inclined to try to provide some significant oversight over the process, but see how it evolves. And I think we are going to have to have some additional discussion on this point as we go on.

I want to make it clear for those who are here, and perhaps here for the first time that we tended not—except in the very fine brief summary in Senator Feinstein's opening statement, we haven't revisited what brought us here, the significant threat to our way of life and to the national security of the United States. We have gone into that at some length before and we have even talked about some of the assumptions of this basic Plan.

As I said in the beginning, this is the fifth hearing of this subcommittee, and what I wanted to do today was to focus on a specific issue which I will get to in the next panel which has to do with privacy concerns, because I would note that our ability to move forward as a government in this area is dependent upon the approval of the citizens of the United States to allow us to move forward. And if they have concerns about a privacy issue, for example, we need to deal with those up front or we are not going to be able to address these more fundamental questions.

But I think it is good that Senator Bennett has reminded us of one of the critical assumptions underlying the structure that you have set up here and the fact that that assumption may not be necessarily a valid one, that we may need to turn more to the national security side of our Government to help us to protect the critical infrastructure, and we will have to evaluate that as time goes on.

Mr. TRITAK. Senator, if I can make just one quick point in answer actually to what I was actually leading up to, Senator, and that is one of the things that struck me about a question you asked fairly early in the Y2K Committee was when, whether, and under what circumstances may the Federal Government play a role in reconstituting privately-owned infrastructures.

Recognizing that we want the market to lead, what happens if that fails, for whatever reason, and it is beginning to have a deleterious effect on national security, economic security, or delivery of vital services? That, to me, is the fundamental question and, in

fact, that is what we are beginning to turn to now because I think it really is at the core of what you mean by an EFEMA versus other things.

But we have begun to look at authorities. One place you start is actually looking at existing authorities and where are the shortfalls for those, and then developing clear ideas about what contingencies might arise and to assure we can plan against those contingencies. We don't know yet for sure what contingencies would apply, but I think the question and the issue is a valid one and you raised it in the Y2K context. I think it is critical to CIP and part of what the Government's responsibility is to defend the Nation in the event of an attack, particularly if it comes from overseas.

Senator KYL. Thank you very much. Well, obviously we will have more questions for you. We will submit some for the record. What we also I think would appreciate is an ongoing communication from you as things evolve. Don't wait for a hearing to come up and talk to us. Feel free to communicate with us on an ongoing basis as the situation evolves so that we will be up to speed with what you are doing.

Thank you again for being here today. Obviously, we could spend all day on some of these issues.

[The prepared statement of Mr. Tritak follows:]

PREPARED STATEMENT OF JOHN S. TRITAK

Mr. Chairman, it is an honor to appear before you here today to talk with you about the National Plan for Information Systems Protection, Version 1.0. This Subcommittee has shown exceptional leadership on the matter of critical infrastructure assurance. I am grateful for the opportunity to discuss the Administration's efforts to achieve President Clinton's goal of establishing a full operational capability to defend the critical infrastructures of the United States by 2003 against deliberate attacks aimed at significantly disrupting the delivery of services vital to our nation's defense, economic security, and the health and safety of its people. This cannot be done without the support and participation of the Congress.

I. INTRODUCTION

The Information Age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our Government, economy, and society are being connected into an ever expanding and interdependent digital nervous system of computers and information systems. With This interdependence comes new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world can potentially break into sensitive Government files, shut down an airport's air traffic control system, or disrupt 911 services for an entire community.

The threats posed to our critical infrastructures by hackers, terrorists, criminal organizations and foreign Governments are real and growing. The need to assure delivery, of critical services over our infrastructures is not only a concern for the national security and federal law enforcement communities, it is also a growing concern for the business community, since the security of information infrastracture is a vital element of E-commerce. Drawing on the full breadth of expertise of the federal government and the private sector is therefore essential to addressing this matter effectively.

President Clinton has increased funding on critical infrastructure substantially during the past three years, including a 15 percent increase in the fiscal year 2001 budget proposal to $2.0 billion. He has also developed and funded new initiatives to defend the nation's computer systems from cuber attack.

In the 18 months since the President signed Presidential Decision Directive 63, we have made significant progress in protecting our critical infrastructures. In response to the President's call for a national plan to serve as a blueprint for establishing a critical infrastructure protection (CIP) capability, the *National Plan for Information Systems Protection* was released last month. It represents the first attempt by any national Government to design a way to protect those infrastructured

essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled through the use of computers and computer networks.

The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback. that is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a Dialogue*—to indicate that it is still a work in progress and that a broader range of perspective must be taken into account if the Plan is truly to be "national;" in scope and treatment.

THE PLAN: OVERVIEW AND HIGHLIGHTS

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes 10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

Program 1 calls for the Government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks from attacks, and to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

Program 2 will install multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.

Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law. It will assist, transform, and strengthen U.S. law enforcement and intelligence Agencies to be able to deal with a new kind of threat and a new kind of criminal—one that acts against computer networks.

Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner. This includes improving information sharing within the Federal Government and encouraging private industry, as well as state and local Governments, to create Information Sharing and Analysis Centers (ISACs), which would share information from the Federal Government. Program 4 additionally calls for removal of existing legal barriers to information sharing.

Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and Agency continuity and recovery plans the ability to deal with information attacks. The goal for Government and the recommendation for industry is that every critical information system have a recovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation's commitment to Prepare and Prevent and to Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that our information security technology stays abreast with changes in the threat environment.

Program 7 will survey the numbers of people and the skills required for information security specialists within the Federal Government and the private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-based attacks.

Program 9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation within the Federal Government, including Congress, and between the Government and private industry.

Program 10 builds mechanisms to highlight and address privacy issues in the development of each and every program. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties. The Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

I would like to highlight a few of the programs in the remainder of my testimony. In these programs, the Administration seeks to accomplish two broad aims of the Plan—the establishment of the U.S. Government as a model of infrastructure protection, and the development of a public-private partnership to defend our national infrastructures.

A. The Federal Government as a model of information security

We often say that more than 90 percent of our critical infrastructures are neither owned nor operated by the Federal Government. Partnerships with the private sector and state and local governments are therefore not just needed, but are the fundamental aspect of critical infrastructure protection. Yet, The President rightly challenged the Federal Government in PDD–63 to serve as a model for critical infrastructure protection—to put our own house in order first. Given the complexity of this issue, we need to take advantage of the breadth of expertise within the Federal Government to ensure that we enlist those Agencies with special capabilities and relationships with private industry to the fullest measure in pursuit of our common goal.

To this end, the President has developed and provided full or pilot funding for the following key initiatives designed to protect the federal Government's computer systems:

Federal Computer Security Requirements and Government Infrastructure Dependencies. One component of this effort supports aggressive, Government-wide implementation of federal computer security requirements and analysis of vulnerabilities. Thus, in support of the release of the National Plan, the President announced his intent to create a permanent Expert Review Team (ERT) at the Department of Commerce's National Institute of Standards and Technology (NIST). The ERT will be responsible for helping Agencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection Plans. Pursuant to existing Congressional authorities and administrative requirements, the Director of the team would consult with the Office of Management and Budget and the National Security Council on the team's plan to protect and enhance computer security for Federal Agencies. The President's Budget for fiscal year 2001 will propose $5 million for the ERT.

Under PDD–63, the President directed the CIAO to coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. Many of the critical infrastructures that support our nation's defense and security are shared by a number of Agencies. Even within Government, critical infrastructure outages may cascade and unduly impair delivery of critical services. The CIAO is coordinating an interagency effort to develop a more aophisticated identification of critical nodes and syatem, and to understand their impact on national security, national economic security, and public health and safety Government-wide. These efforts support the work of the ERT in identifying vulnerabilities of the Government's information infrastructures, and provide valuable input to Agencies for planning secure computer

systems and implementing computer security plans. This research, when complete, will permit the Federal Government to identify and redress its most significant critical infrastructure vulnerabilities first and provide the necessary framework for well informed critical infrastructure protection policy making and budget decisions.

Federal Intrusion Detection Network (FIDNet). PDD–63 marshals Federal Government resources to improve interagency cooperation in detecting and responding to significant computer intrusions into civilian Government critical infrastructure nodes. The program—much like a centralized burglar alarm system—would operate within long-standing, well-established legal requirements and Government policies covering privacy and civil liberties. FIDNet is intended to protect information on critical, civilian Government computer systems, including that provided by private citizens. It will not monitor or be wired into private sector computers. All aspects of the FIDNet will be fully consistent with all laws protecting the civil liberties and privacy rights of Americans.

To support this effort, the Administration will propose funding in the President's fiscal year 2001 Budget ($10 million) to create a centralized intrusion detection and response capability at the General Services Administration (GSA). This capability will function in consort with GSA's Federal Computer Incident Response Capability, and assist Federal Agencies to:

- detect and analyze computer attacks and unauthorized intrusions;
- share attack warnings and related information across Agencies; and
- respond to attacks in accordance with existing procedures and mechanisms.

FIDNet is intended to promote confidence in users of Federal civilian computer systems. It is important to recognize that FIDNet has a graduated system for response and reporting attack and intrusion information would be gathered and analyzed by home-Agency experts. Only data on system anomalies would be forwarded to GSA for further analysis. Thus, intrusion detection would not become a pass-through for all information to The Federal Bureau of Investigation or other law enforcement entities. Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules—no new authorities are implied or envisioned by the FIDNet program.

One additional benefit of Government-wide intrusion detection is to improve computer intrusion reporting and the sharing of incident information consistent with existing government computer security policy. Various authorities require Agencies to report criminal intrusions to appropriate law enforcement personnel, which include the National Infrastructure Protection Center.

FIDNet will support law enforcement's responsibilities where cyber-attacks are of a criminal nature or threaten national security.

In short, FIDNet will:

- be run by the GSA, not the FBI;
- not monitor any private network traffic;
- confer no new authorities on any Government Agency; and
- be fully consistent with privacy law and practice.

Federal Cyber Services (FCS). One of the nation's strategic shortcomings in protecting our critical infrastructures is a shortage of skilled information technology (IT) personnel. Within IT, the shortage of information systems security personnel is acute, The Federal Government's shortfall of skilled information systems security personnel amounts to a crisis. This shortfall reflects a scarcity of university graduate and undergraduate information security programs and the inability of the Government to provide the salary and benefit packages necessary to compete with the private sector for these highly skilled workers. In attacking this problem through the Federal Cyber Services initiative described below, we are leveraging the initial efforts made by the Defense Department, National Security Agency, and some other Federal Agencies. The President's Budget for fiscal year 2001 will propose $25 million for this effort.

The Federal Cyber Services training and education initiative, highlighted by the President at the Plan's release, introduces five programs to help solve the Federal IT security personnel problem.

- a study by the Office of Personnel Management to identify and develop competencies for federal information technology (IT) security positions, and the associated training and certification requirements.
- the development of Centers of IT Excellence to establish competencies and certify current Federal IT workers and maintain their information security skill levels throughout their careers.

- The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT managers by awarding scholarships for the study of information security, in return for a commitment to work for a specified time for the Federal Government. This program will also support the development of information security faculty.
- The development of a high school outreach and awareness program that will provide a curriculum for computer security awareness classes and encourage careers in IT fields.
- The development and implementation of a Federal Information Security awareness curriculum aimed at ensuring computer security literacy throughout the entire Federal workforce.

Research and Development. A key component to our ability to protect our critical infrastructures now and in the future is a robust research and development plan. As part of the structure established by PDD–63, the interagency Critical Infrastructure Coordination Group (CICG) created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works, with Agencies and the private sector to:

- gain agreement on requirements and priorities for information security research and development;
- coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;
- communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and
- identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, has helped focus efforts on coordinated cross-government critical infrastructure protection research. Among the priorities identified by the process are:

- technology to support large-scale networks of intrusion detection monitors;
- artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;
- methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster,
- technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and
- technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

The President's Budget for fiscal year 2001 will propose $606 million across all Agencies for critical infrastructure related R&D investment.

The need exists, however, to coordinate R&D efforts not just across the federal Government, but between the public and private sectors as well. A fundamentally important initiative that has the ability to pull disparate pieces of the national R&D community into closer relationships is the Institute for Information Infrastructure Protection (I^3P), an organization created to identify and fund research and technology development to protect America's cyberspace from attack or other failures. I will discuss this in detail when I address Public-Private Partnership issues.

Public Key Infrastructure. Protecting critical infrastructures in the Federal Government and private sectors requires development of an interoperable public key infrastructure (PKI). A PKI enables data integrity, user identification and authentication, user non-repudiation, and data confidentiality through public key cryptography by distributing digital certificates (essentially electronic credentials) containing public keys, in a secure, scalable, and reliable manner. The potential of PKI has inspired numerous projects and pilots throughout the Federal Government and private sectors. The Federal Government has actively promoted the development of PKI technology and has developed a strategy to integrate these efforts into a fully functional Federal PKI. The President's Budget for fiscal year 2001 will propose $7 million to ensure development of an interoperable Federal PKI.

To achieve the goal of an integrated Federal PKI, and protect oar critical infrastructures, the Federal Government is working with industry to implement the following program of activities:

- *Connect Agency-wide PKIs into a Federal PKI.* DoD, NASA, and other Government Agencies, are actively implementing Agency-wide PKIs to protect their internal critical infrastructures. While a positive step, these isolated PKIs do not protect infrastructures that cross Agency boundaries. Full protection requires an integrated, fully functional PKI.
- *Connect the Federal PKI with Private Sector PKI:* Private sector groups are actively developing their own PKIs as well. While a positive step, these isolated PKIs do not protect infrastructures that cross Government or industry sector boundaries.
- *Encouraging Development of Interoperable Commercial Off-the-Shelf (COTS) PKI Products:* Limitation to a single vendor's solution can be a Serious impediment, as most organizations have a heterogeneous computing environment. Consumers must be able to choose COTS PKI components that suit their needs.
- *Validating the Security of Critical PKI Components:* Protecting critical infrastructures require sound implementation. The strength of the security services provided to the critical infrastructures depends upon the security of the PKI components. Validation of the security of PKI components is needed to ensure that critical infrastructures are adequately protected. NIST is pursuing a validation program for PKI components.
- *Encouraging Development of PKI-Aware Applications:* To encourage development of PKI-aware applications, the Government is working with vendors in key application areas. One example is the secure electronic mail projects that have been performed jointly with industry.

B. Public-Private partnership

The security of information flowing over the information highway is a critical element of E-commerce, as well as to our national security. It is a necessary part of building trust in the accuracy and integrity of transactions made over the information infrastructure. There is a growing awareness that America's information infrastructure—the basis of E-Commerce—is becoming an increasingly attractive target for deliberate attack or sabotage. A strategy of cooperation and partnership between the private sector and the U.S. Government to protect the Nation's infrastructure is the linchpin of this effort. The President is committed to building partnerships with the private sector to protect our computer networks through the following initiatives:

Institute for Information Infrastructure Protection (I^3P). The Institute would identify and address serious R&D gaps that neither the private sector nor the Government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President announced he would propose initial funding of $50 million for the Institute in his fiscal year 2001 Budget. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this organization. The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and supported by leading corporate Chief Technology Officers.

The Institute will work directly with private sector information technology suppliers and consumers to define research priorities and engage the country's finest technical experts to address the priorities identified. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes. The Institute will also make provisions to accept private sector support for some research activities.

Partnership for Critical Infrastructure Security. Last December, Commerce Secretary Daley met with senior representatives from over 90 major corporations, most fortune 500, representing owners and operators of critical infrastructures, their suppliers, and their customers, to discuss the building a Partnership for Critical Infrastructure Security. Industry has taken the lead on this effort and organized a meeting at the U.S. Chamber of Commerce far later this month to give substance and purpose to the Partnership.

The Partnership will explore ways in which industry and Government can work together to address the risks to the nation's critical infrastructures. Federal Lead Agencies are currently building partnerships with individual infrastructure sectors in private industry, including communications, banking and finance, transportation, and energy. The Partnership will serve as a forum in which to draw these individual

efforts together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness and understanding of, and to serve, when appropriate, as a catalyst for action among, the owners and operators of critical infrastructures, the risk management and investment communities, other members of the business community, and state and local Governments.

National Infrastructure Assurance Council (NIAC). President Clinton established the NIAC by Executive Order 13130 on July 14, 1999. When fully constituted, it will consist of up to 30 leaders in industry, academia? the privacy community, and state and local Government. The NIAC will provide advise and counsel to the President on a range of policy matters relating to critical infrastructure assurance, including the enhancement of public-private partnerships, generally.

III. CONCLUSION

In conclusion, the National Plan is an important step forward. My staff and I are committed to building on this promising beginning, coordinating the Governments efforts into an integrated program for critical infrastructure protection in support of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and the Federal Government, generally. We have much work left to do, and I hope to work with the members of this committee, indeed with the Congress as a whole, as we wrestle with this developing field. I look forward to your questions.

Senator KYL. I would like to bring our next panel forward now to look specifically at the National Plan and privacy issues associated with it. We will have two witnesses. The first witness is Mr. Marc Rotenberg, executive director of the Electronic Privacy Information Center, EPIC. Mr. Rotenberg also teaches on information privacy at Georgetown Law School. He has testified before Congress, advocating strong privacy protection in the Internet age.

He has also followed the work of this subcommittee quite closely, stating in a 1998 study entitled "Critical Infrastructure and the Endangerment of Civil Liberties" that in the fight for diminishing resources—I am going to quote now, Senator Feinstein—

> the intelligence community and the Pentagon also ensured a body of congressional champions of information warfare advocates and supporters. Chief among them are Senator Jon Kyl—

thank you—

> whose Subcommittee on Technology, Terrorism, and Government Information has held numerous hearings featuring doom-and-gloom witnesses complaining that the Nation is on the verge of an electronic Pearl Harbor, and even more distastefully, an electronic Oklahoma City.

In any event, thank you for appearing and following our hearings, Mr. Rotenberg. We will place your full statement in the record and in a moment ask you to provide a summary of that.

The other witness in this panel is Frank Cilluffo, senior policy analyst at the Center for Strategic and International Studies. He directs seven task forces on a range of topics, including information warfare and information assurance, terrorism, and financial crimes. These task forces comprise over 175 senior officials and experts from the academic, defense, intelligence, law enforcement, and corporate communities. We will place your full statement in the record as well and ask both of you to summarize your comments.

So, first, Mr. Rotenberg.

PANEL CONSISTING OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, DC; AND FRANK J. CILLUFFO, SENIOR POLICY ANALYST, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, WASHINGTON, DC

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you, Mr. Chairman and Senator Feinstein. I am grateful to be here with the opportunity to talk about privacy. I should say at the outset that there is really no disagreement about the need to keep the Nation's computer network secure and safe from attack. Outages cause disruption for industry. They cause disruption for users, and certainly they pose questions of public safety and national security.

At the same time, I would like to suggest to you in reviewing the Plan that it is very important to keep in mind the history of the growth of the Internet, as well as our country's recent experience with computer security policy to ensure that the plan that is followed through on actually is the best way to protect this underlying interest. In my testimony, I outline some of this history. I would like to briefly highlight a couple of points and then focus in on the FIDNet proposal.

The first point I would like to make is regarding the nature of the Internet itself. This is a very robust communication infrastructure that was designed with the understanding that a foreign adversary may well cause an attack that could have taken out a traditional channel switch network, like a telephone network, for example. And in this old style of networking, if you take out one of the points along the line, the whole line goes down and you cannot get information through.

The Internet relied on a different architecture. It was decentralized, it used multiple nodes. It used a type of switching technology called packet switching which made it possible to move information from one point to another, even if some of the points in between along the way had been taken out, and this made it very robust. It also interestingly made it equally secure against attack from a foreign adversary, as well as a natural disaster or even a winter storm.

Now, I don't mean to suggest to you that there aren't real risks to the Internet today. There are, and I think the subcommittee has done a good job of documenting these risks. But at the same time, I would like to suggest to you that the architects of this infrastructure, the designers, were very much aware from the outset of the need to create a communications network that could withstand attack and that could continue to operate. And this is important to understand what security is about.

The second point I would like to say is that, frankly, during the past decade the Federal Government's record in the area of promoting computer security has been quite mixed. And as you are no doubt aware, the private sector user organizations, privacy organizations, have expressed a lot of concern that many of these proposals that seek at the outset to promote computer security in the end create a lot of computer surveillance, and that whereas a private organization might try to make a system more robust or more dif-

ficult to attack or take down, the Government invariably comes up with proposals that make it easier to monitor and to spy on.

Nowhere was this problem more clearly demonstrated than in the difficulty of developing an encryption policy that would work for the Government and for the private sector. Now, I am not going to go through all that history, but I do want to provide for you one very simple example of the difficulties that the Federal Government's computer security policy over the last decade created for computer users and for private industry, and it has to do with the online transactions involving credit card purchases.

When people went online last Christmas to buy books or CD's or gifts for their families, many of them were typing in credit card numbers, and what secured those credit card numbers so that they could not be stolen by thieves or anybody else was a little bit of encryption built into the software that they were using. They weren't even aware of it, but it scrambled the credit card number so that it would go from their computer to the Web site where they were buying this product online and protected that information.

Now, you can design that encryption so that it is very strong, so that it is difficult to break. But the Federal Government was very reluctant to make that type of strong encryption widely available because they said if we make that available for American consumers, it could also fall into the wrong hands. So what they tried to do instead is they said we are going to create two levels of encryption, one level the strong kind that will let American consumers use it if they prove that they are U.S. citizens, and another a weak kind that will let U.S. companies market to foreign users because they are going to need some encryption, but it is not going to be as strong.

Well, the result of that policy, as I describe in my testimony, was that this past Christmas season when U.S. consumers were buying products from U.S. businesses in the United States, they were invariably using the weak encryption because of a government policy that was trying to keep strong encryption out of the hands of foreign users. This is a reoccurring problem in the computer security field. I think the Plan as currently described is going to recreate this problem and I want to bring it to your attention today. It is a very real problem.

Now, I am going to focus now on FIDNet. A couple of things were said by Mr. Tritak during the last panel, and I hope you will ask me a couple of questions about this, but I have to say at the outset what disturbed me most about Mr. Tritak's presentation—in some ways it is not surprising—is having said on the one hand that the Government is very much aware of privacy issues and privacy laws, and intends to respond to these concerns because they are widely shared by the American public, Mr. Tritak was unaware that the type of government monitoring that is proposed in the Plan as described in FIDNet would fall under the legal rules set out in our Communications Privacy Act, passed in 1986 with strong bipartisan support.

He seemed to think that because this wasn't voice communication, it wasn't subject to any legal rules. That is simply not correct. But it was even more disturbing, as I described in my testimony, that in a memo that was prepared by the Department of Justice

by Mr. Ron Lee to Mr. Tritak's predecessor, Mr. Hunker, who is the Director of the CIAO, Mr. Lee outlined the problem. He said, you have got a real issue here. The type of network monitoring which one agency like the DOD would be permitted to do on its own computer networks which you are now proposing under the Plan to do across all government computer networks clearly would fall under the Communications Privacy Act. And if you want to do this, advised Mr. Lee, you are going to have to notify all people using government computer networks, not just Federal employees but also U.S. citizens, that they will have no right of privacy using the network.

Now, that is frankly the suggestion that is put forward by Mr. Lee and the Department of Justice that could, in effect, make the privacy issue go away. But it is a solution that I think privacy organizations across the political spectrum would have a great deal of difficulty with. And as I have tried to suggest in the testimony, I think for the Government to say, in effect, you have no legal rights of privacy when you are using the Government computer system would be contrary not only to the Federal wiretap statute, but also our Privacy Act, passed in 1974, and our whole fourth amendment tradition which basically says, yes, the Government has the right to search and protect public safety, but it has to be done in a way that recognizes the balance of power within our Government; that the executive branch, the Federal agencies may conduct these activities, but they have to be reviewed by the judicial branch.

The other point which I would like to briefly say, Mr. Chairman, is that there was in my testimony a reference to the use of credit card information and telephone toll record information. And you asked a question which I certainly thought was very appropriate, and that is what type of information would be collected in trying to assess system anomalies because this, of course, is the basis for the search that the Government agencies will conduct.

Now, I don't know exactly what the plan is, and I think Mr. Tritak is correct to say that this is still a Plan in development. But I do have here and am pleased to provide for the subcommittee a memo from Mr. Hunker outlining the National Plan and, "how we get industry buy-in." And contained in this Plan is one slide titled "Profiling System Anomalies." The first bullet point is "Systematic Identification of Suspicious and Anomalous Behavior Based on Algorithms to Analyze Similarities and Match Behavioral Patterns."

And then there are three lines. The first line, which frankly I don't understand, says "Traditional Psycho-Linguistics." The second line is "Credit Card Profiling," and the third line is "Toll Fraud Profiling." And this is from a memo that was prepared by Mr. Hunker describing how system anomalization might be identified.

And I should say, in fairness, Mr. Chairman, that this is a big, complex area. I wouldn't expect Mr. Tritak to be familiar with all the details, but I think if we are to take seriously the commitment to privacy protection, we need a clear understanding about the application of U.S. privacy laws, and we clearly need more information about what type of information will be collected from U.S. citizens.

You see, when you set up intrusion detection, it is not just the bad guys and the people who are intent on causing us harm that you are going to be tracking and monitoring. You are going to be tracking U.S. employees working for U.S. firms in London and Tokyo, U.S. trade officials in Geneva and Paris, U.S. computer researchers in Dublin and Tel Aviv, and U.S. citizens within the United States. All of these people will become subject to the monitoring scheme that is outlined in the FIDNet proposal.

So I would be pleased to answer your questions and I thank you again for the chance to be here.

Senator KYL. Thank you.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG

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.

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.

[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.

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 psst 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 percent 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/ISBNI=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, 2000 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."

Senator KYL. Mr. Cilluffo.

STATEMENT OF FRANK J. CILLUFFO

Mr. CILLUFFO. Thank you, Mr. Chairman. Mr. Chairman, Senator Feinstein, I appreciate the opportunity to appear before you today with respect to the recently released National Plan and the challenge of simultaneously assuring the security of our Nation's critical infrastructures while preserving personal privacy.

I also commend you for your leadership on these issues and the recognition that they extend far beyond the Nation's Capital. Indeed, they must be brought before the American people. Many of these issues are misunderstood and give rise to skepticism, distrust, and confusion between individuals, organizations, and government, the initial media account of the proposed FIDNet program being one case in example.

One of the advantages of working at a think tank is that I don't have to stand where I sit, so I can be a little more blunt. Another is that we are simply in the ideas business and are not responsible or held accountable for implementing these ideas. With that in mind, I would like to take a few moments and make a few brief observations on, first, the cyber threat in general; second, the need

to strike the appropriate balance between privacy and security; and, third, the National Plan for Information Systems Protection.

The reason we have to understand the threat, I think, is to be able to do the appropriate balance, we need to know exactly what we are dealing with. And we are all aware of the many benefits of information technology, and this revolution's impact on society has been profound and touches everyone, whether we are examining our economy, our national security, or our quality of life.

Unfortunately, as we touched on earlier, there is a dark side, and along with these new rewards come new risks and unintended consequences which need to be better understood and managed by our corporate and government leaders, and I mention corporate first. These risks—and we discussed some of them—range from the national security issues, strategic information warfare and information operations, the vulnerabilities and threats to our infrastructures, to protecting our personal information, such as medical records and the like.

I think that I have a disagreement with Mr. Rotenberg on the robustness of our infrastructures. I think that the ability to network has far outpaced our ability to protect networks. In some cases, systems are being integrated on top of one another, and hence a failsafe on one day becomes a loophole the next, since you can't beta-test all these networks as a whole.

Moreover, many of our highly advanced systems are based on insecure foundations. ARPANet, while it may have been quiet, was not intended to be secure. It was actually intended to share information between and among scientists, and then it expanded to academe and then it expanded to where it is today. It was not intended to be secure.

Yet, many in public life and among our citizenry remain skeptical or even downright dismissive of any potential dangers. And again I look to Senator Feinstein, and I agree with you. It is difficult to visualize these cyber threats. It is not like Nazi forces moving across Europe, it is not like the effects of Pearl Harbor, or even the Soviet missiles on parade in Red Square. This is something that is difficult to see.

Yet, our real assets today are stored electronically and not in Fort Knox, and the target increasingly is not the military at all, but rather our Government and corporate information systems. Information warfare inherently extends the battlefield to incorporate all of society. As you mentioned, the myth persists that the U.S. hasn't been invaded since 1812. Invasion through cyber space is now a daily occurrence.

The threat spectrum ranges from the so-called ankle biters on one end to foreign nations on the other, and one of the greatest challenges of these cyber threats is its anonymity. Who is behind the clickety-clack of the keyboard breaking into my system? Is it a young adult, is it a foreign intelligence service, is it an economic competitor, is it someone doing the bidding for someone else, or perhaps even someone masquerading, cloaking the perpetrator's true identity leading you to go in the wrong direction?

Additionally, smoking keyboards are hard to find, as an assailant can loop and weave from country to country in a matter of nanoseconds, all while law enforcement is forced to stop at jurisdictional

boundaries defined by the physical world, which have little to no meaning in cyber space. In essence, we have created the global village without a police department, and I thought Senator Bennett's slide was excellent along those lines.

According to a recent report by the Department of Defense, the NCS in particular, currently at least 10 countries—an unclassified report—possess offensive information warfare capabilities somewhat akin to our own. As you mentioned earlier, Mr. Chairman, of unique interest are the current Chinese discussions regarding the possible creation of a fourth branch of the armed services within the PLA devoted entirely to information warfare.

Bits and bytes will never replace bullets and bombs. Yet, one area that I think does require some further examination is the synergy of where the physical and the virtual come together. For example, you have detonated a conventional explosive and then you follow that up with an attack on our E 911 systems. As we heard earlier, a young man in Toborg, Sweden, was able to do it many thousands of miles away. And my Swedish colleagues tell me that that young man is now in an insane asylum, and I guess we can call him a crackpot who hit the jackpot. But he still demonstrates these vulnerabilities that can be exploited by those with more nefarious intent.

And we are also aware of our vulnerabilities due to exercises such as Eligible Receiver and subsequent exercises which we can't get into—squirrels taking down major networks, backhoes, NSA systems being down last week. We are well aware of our vulnerabilities. We have seen demonstrated capabilities, whether it is E 911 systems or whether it is air traffic control.

What we haven't seen yet, though, is the marriage of the true, the real hostile, where the intent and the capability come together. In my eyes, though, that is only a matter of time before this convergence occurs, and I call it where the real bad guys exploit the real good stuff and become more techno-savvy.

As we contemplate methods of dealing with these threats, it is important to remember that our national security community and law enforcement institutions were designed and establish to protect our freedoms, our liberties, and our way of life.

With this in mind, I think it is possible to ensure the security of our Nation's critical infrastructures without compromising civil liberties and personal privacy or by locking down the Internet. Throughout history, the first obligation of any State has been to protect its citizens. Today is no exception. Yet, we must be careful and avoid placing our national security community in a position where they could trample on our liberties in order to preserve them.

Moreover, policies in response to threats of any kind, especially in cyber space, must not stifle the engines of innovation that drive our economy and enhance our lives. We cannot afford to overreact and put up too many virtual or physical walls. If we do, the adversary wins by default because our way of life has been lost, and I look back to the weeks before ushering in the new millennium as a number of lessons that should be learned there.

Too often, the debate is framed as if security and privacy are mutually exclusive. This is simply not true. It is wrong to think of

these issues as an either/or. We must rather think of the need to incorporate both, and in order to preserve the twin goals of security and privacy, we must begin with the notion of a true partnership, and I think we are seeing some very good steps in that direction.

For a number of years, many, myself included, have criticized the current administration for being long on nouns and short on verbs, a lot of talk, not a whole lot of action with respect to critical infrastructure protection and policies, a concern I know you share, Mr. Chairman, given your 1996 amendment to the Defense Authorization Act. And I think that the President was required to answer those questions within 120 days. Well, 4 years later, we do have a 200-page document that begins to address some of your concerns.

Overall, I think the Plan does an excellent job of identifying gaps and shortfalls within the Federal Government and charting an initial course of action to address them. My major concern is that it does not do enough. We must be willing to commit real money to tackling the problem. After all, policy without resources is rhetoric.

While the President's proposed budget for fiscal year 2001 is a good start, a vast majority of those resources have already been earmarked and allocated in previous budgets. I also personally believe that more funds should be devoted to governmentwide programs and measures aimed at prevention and protection. Moreover, only through leading by example can the Government realistically hope for the private sector to commit the sort of resources expected of them.

There were also concerns, legitimate ones in my eyes, that the Plan was developed behind closed doors, without public input, including the Congress and many of the owners and operators of these critical infrastructures, and their views were not solicited. Nevertheless, I do think it is encouraging that the administration seems amenable to accept input at this point, a process I encourage be enhanced.

With respect to infrastructure assurance, we must continue to work toward and build on a true National Plan with full representation from industry and all interested parties. We need to forge a genuine partnership between the public and private sector. It can no longer be merely a case of the Government leading and the private sector following. In other words, Silicon Valley and the Beltway, where the so-called wing tip meets the sandal, must stand side by side on equal footing to address these issues.

No offense, Senator Feinstein, to Silicon Valley.

I think that the Partnership for Critical Infrastructure Security referenced earlier by John Tritak is one that is particularly encouraging.

In closing, New York Yankee great Yogi Berra once said the future ain't what it used to be. The best way to predict the future is to help build it. We should not have to choose between security and privacy. With a lot of hard work we can, and arguably must, have both.

Thank you for your time and I would be pleased to try to answer any questions you may have.

[The prepared statement of Mr. Cilluffo follows:]

PREPARED STATEMENT OF FRANK J. CILLUFFO

Mr. Chairman, Senator Feinstein, distinguished Members of the Committee, I appreciate the opportunity to appear before you today to discuss some of the policy implications with respect to the recently released "National Plan for Information Systems Protection." I would also like to address the difficult challenge of simultaneously ensuring the security of our nation's critical infrastructures while preserving personal privacy.

I commend you for your leadership on these issues and the recognition that they extend far beyond the nation's capital. Indeed, they must be brought before the American people—and soon. Many of these issues are misunderstood and give rise to skepticism, distrust and confusion between individuals, industry and the government—the initial media accounts of the proposed Federal Intrusion Detection Network (FIDNET) to cite one example. We must encourage any initiatives aimed at advancing a meaningful dialogue between our citizens, industry, and government.

One of the advantages of working for a think tank is that *we don't have to stand where we sit,* a rare luxury for someone inside the Beltway. Another is that we are simply in the ideas business and are not responsible or held accountable for implementing our ideas.

With that in mind, I would like to make a few brief observations on:

- Cyber threats in general;
- The need to strike an appropriate balance between privacy and security; and
- The "National Plan for Information Systems Protection."

The information technology revolution has given us an unrivalled, perhaps unsurpassable, lead over the rest of the world in virtually every facet of modern life. Information technology's impact on society has been profound and touches everyone, whether we examine our economy, our quality of life, or our national security. Unfortunately there is a "dark side" to this revolution. Along with the clear rewards come new risks and a litany of unintended consequences that need to be better understood and managed by our industry and government leaders. These risks range from the national security considerations involving threats to, and vulnerabilities of, our critical infrastructures from cyber attacks and information operations, to protecting the confidentiality and integrity of our personal information such as medical records, credit histories, or even our identities, from unauthorized use. If we do not understand these potential consequences, widespread cyber threats—once the domain of science fiction—will become a reality for us all.

Our highly complex and inter-networked environment is based on insecure foundations. It is not widely understood that the Internet's predecessor, ARPANET, was never intended to be "secure." In fact its very design schematic was based on openness—to facilitate the sharing of information between scientists and researchers.

It is also problematic that the *ability* to network has far outpaced the *ability to protect* networks. In some cases, new systems are being integrated on top of one another—hence a fail-safe system on one day becomes a loophole the next. The established cliché about the "weakest link in the chain" has never been more acute or applicable. Additionally, according the Final Report of the President's Commission on Critical Infrastructure Protection (PCCIP), it is estimated that by 2002, a worldwide population of approximately 19 million will have the skills to mount a cyber attack.

All of this interconnection leads to the origins of our problem. Modern societies are dependent upon critical infrastructures such as telecommunications, electric power, health services, banking and finance, transportation, and defense systems, to provide us with a comfortable standard of living. These systems are increasingly interdependent on one another and damage to one can potentially cascade and impact others—with single point failures being of greatest concern. To compound the problem, military and law enforcement authorities report that every month assailants make thousands of unauthorized attempts to gain access to these systems, amounting to a nearly continuous assault.

And yet, many in public life and among our citizenry remain skeptical or downright dismissive of any potential dangers. After all, it is difficult to visualize a cyber threat in the same way that we saw film clips of Hitler's legions marching across Europe, the results of Japan's attack on Pearl Harbor, or Soviet missiles on parade in Red Square. There are other problems with getting people to take these threats seriously. For example, how can you "see" a cyber threat developing? While it may be scary in the abstract, it does not easily lend itself to images of fear, making it difficult to personalize for most Americans.

Today our real assets are stored electronically, not in Fort Knox and the targets are increasingly not government and military installations, but rather public and

private computer network systems. Information warfare extends the battlefield to incorporate all of society. The myth persists that the United States has not been invaded since 1812, but invasion through cyberspace is now a daily occurrence. We can no longer afford to rely on the two oceans that have historically protected our country: instead we must develop the means to mitigate risk in an electronic environment that knows no borders.

The threat spectrum ranges from "ankle biters"[1] to nations, with currently no readily available means to discern who is committing the attack. Additionally, "smoking keyboards" are hard to find as an assailant can loop and weave from country to country in a matter of nanoseconds. Thus, an attack initiated a couple of blocks away can be made to appear to come from halfway around the world. All of this happens while law enforcement is forced to stop at jurisdictional boundaries, defined by the physical world which have no meaning in cyberspace. In essence, we have created a global village without a police department.

According to a recent public report by the Department of Defense (the National Communications System), currently at least ten countries possess offensive information warfare capabilities comparable to our own. Moreover, a 1996 Government Accounting Office (GAO) report references that approximately 120 nations have some sort of computer attack capability. The reality of this potential threat was illustrated in an article published this fall in the Liberation Army Daily; the official newspaper of the Chinese People's Liberation Army (PLA) titled "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power." In this article, the authors discuss Chinese preparations to carry out high-technology warfare over the Internet and advocate the creation of a fourth branch of the armed services within the PLA devoted to information warfare.

Bits and bytes will never replace bullets and bombs. Conventional terrorist organizations, for example, will never abandon car bombs or pipe bombs, which have already proven highly effective, relatively low in cost and risk and still generate headline news. As a force multiplier, however, information warfare increases the lethality of the terrorist when used in concert with other more conventional means. For example, one scenario we created at CSIS involved a malcontent first detonating a conventional explosive followed up by denial of service cyber attacks on the same city's emergency communications network, thereby preventing the first responders and authorities from responding. The consequences were two-fold; it led to an increase in the number of potential casualties and sowed further psychological fear.Is this really far-fetched? Two years ago a young man sitting behind his desktop computer thousands of miles away in Toborg, Sweden, disabled portions of the Emergency 911 system in Southern Florida. Another example of a significant infrastructure disruption occurred in 1997, when a Massachusetts teenager was charged with disabling the Federal Airline Aviation control tower for six hours at Worcester Regional Airport.

It is only a matter of time before there is a convergence between those with hostile intent and techno-savvy, where the real bad guys exploit the real good stuff.

As we contemplate methods of dealing with these threats it is important to remember that our national security community and law enforcement institutions were designed and established to protect our freedom, our civil liberties and our way of life. We expect the national law enforcement agencies to protect us from criminal elements within our borders. We expect the Defense Department and the Armed Forces to protect us from external threats. We expect the nation's intelligence agencies to provide insight into the intentions and capabilities of our adversaries and to provide advance early warning of threats to us.

It would be a mistake to place our national security and law enforcement institutions in a position where they would have to compromise our precious hard-won rights or infringe upon our privacy in order to protect us. The worst possible victory granted cyber attackers would be one that destroyed these values whereby we would become less open, less tolerant and less free.

Concomitantly, we must recognize the many benefits of information technology and understand that these benefits far outweigh any risks. Thus, our policies in response to threats of any kind must not stifle the engines of innovation that drive our economy and enhance our lives. We cannot afford to over react or put up too many "virtual" or "physical walls." If we do, the adversary wins by default because our way of life has been lost.

---

[1] As defined by the NSA Glossary of Terms Used in Security and Intrusion Detection, an ankle-biter is "A person who aspires to be a hacker/cracker but has very limited knowledge related to Automated Information Systems. Usually associated with young adults who collect and use malicious programs obtained from the Internet."

It is possible to ensure the security of our nation's critical infrastructures without compromising civil liberties and personal privacy or locking down the Internet. Throughout history, the first obligation of the state has been to protect its citizens. Today is no exception. Information technology, while providing us many comforts and conveniences has also created for us new kinds of vulnerabilities that can be exploited. These vulnerabilities must be addressed and balanced with the civil liberties we have worked so hard to earn as a nation. It makes no sense to trample on civil liberties in order to preserve them.

Too often, the debate is framed as if security and privacy are mutually exclusive. This is simply not true. It is wrong to think of the issue as "either" "or". We must rather think of the need to incorporate both. In order to preserve the twin goals of security and privacy, we must begin with the notion of a true partnership.

For a number of years many, myself included, have criticized the current Administration for being "long on nouns and short on verbs"—a lot of talk, not a lot of action—with respect to critical infrastructure protection and related policies. A concern I know you share Mr. Chairman, especially given your amendment to the 1996 Defense Authorization Act, wherein "the President shall submit to Congress a report setting forth the results of a review of the national policy on protecting the national information infrastructure against strategic attacks." Four years later, we have a 200-page document ("the Plan") that begins to address some of your concerns. To their credit, the President and his team have done some good work with the Critical Infrastructure Working Group (CIWG), Executive Order 13010, the President's Commission on Critical Infrastructure Protection (PCCIP), Presidential Decision Directive 62, and Presidential Decision Directive 63, albeit most of these initiatives do not adequately address high-end national security threats to our information infrastructures, including strategic information warfare.

Overall, I think the Plan does an excellent job identifying gaps and shortfalls within the Federal government, and charting an initial course of action to address them. My major concern is that it does not do enough.

We must be willing to commit real money to tackling the problem—after all policy without resources is rhetoric. While the President's proposed budget for fiscal year 2001 is a good start, a vast majority of the resources have already been earmarked and allocated in previous budgets. I personally believe that more money should be devoted to government-wide programs (i.e. a more robust and complete PKI infrastructure) and measures aimed at prevention and protection. While there are no protective measures that are completely effective, the 80 percent solution will be sufficient to deter most attackers by increasing the risk of detection or failure. In essence, by raising the bar higher, we would then improve our "signal to noise" ratio and be better positioned to address the more significant threats. Moreover, only through leading by example can the government realistically hope for the private sector to commit the sort of resources expected of them.

There have also been concerns that the Plan was developed behind closed doors, and that public input was not solicited through the *Federal Register* and other means. Many individuals and organizations, including the Congress and the owners and operators of many of the critical infrastructures within industry, could have offered valuable counsel and prevented some of the adverse publicity surrounding the Plan last summer. Nevertheless, it is encouraging that the Administration seems amenable to accept input at this point, a process that needs to be enhanced and encouraged.

With respect to infrastructure assurance, we must continue to work toward and build upon a true national plan with full representation from industry and all interested parties. We need to forge a genuine partnership between the public and private sectors. The public actions of the Critical Infrastructure Assurance Office (CIAO) are very encouraging in this respect. Specifically, the recently announced Partnership for Critical Infrastructure Security, which has brought together approximately ninety leading corporations and various federal agencies to address the problems of infrastructure assurance, is a good example of a step in the right direction.

We also need a true national debate on infrastructure assurance and we need to re-think national security strategy accordingly. It can no longer be a case of the government leading and the private sector following. In other words, Silicon Valley and the Beltway, where the sandal meets the wingtip, must stand side by side and on equal footing in addressing these issues and formulating responses.

Philosopher and New York Yankee great, Yogi Berra, once said, "The future ain't what it used to be." The best way to predict the future is to help build it. We should not have to choose between security and privacy. With a lot of hard work, we can and must, have both.

Thank you for your time. I would be pleased to try to answer any questions you may have.

Senator KYL. Thank you, Mr. Cilluffo. I think the last comment you made summarizes my view, and that is that this doesn't have to be a zero-sum game. We have got to be concerned about both issues, both the protection of American interests, which include privacy interests, and on the other hand doing it in a way that doesn't inhibit people's civil liberties. That is an age-old issue. This is merely one of the latest iterations of it. You could write the history of this country and every decade would have a chapter dealing with some iteration of this particular problem. But it has got a new feature now and a more complicated one, and I think a constructive dialog is important.

I think the questions that Mr. Rotenberg raises are important questions and I think the Government needs to pay more attention to those questions. There needs to be more public discussion of them. There needs to be a lot of serious questioning with respect to the protection of privacy.

But I also think that the people who raise those questions would be more credible in doing so if they didn't denigrate the nature of the challenge that we are trying to deal with here, which I think, Mr. Rotenberg, with all due respect, you do. And I think the very legitimate questions you raised would be enhanced by an acknowledgement right up front that this was not some invention of the Defense Department in order to get more money, which is what you have said, but rather a response to a legitimate concern.

Senator Sam Nunn and I had the first hearings on this. I don't think you would criticize him as somebody that is a mouthpiece for getting more money for the Defense Department. As a matter of fact, I think it is arguably true that we had to drag them kicking and screaming to this problem because they saw it coming out of their budget. And I think if you asked the people downtown, they would say one of the reasons why this was so slow in coming is that nobody wanted to put their arm around this baby because they knew that it was going to be hard and it was going to cost a lot of money and they didn't want it to come out of their budget.

So when you say things, Mr. Rotenberg, like the DOD and its secretive component, the NSA, were driving forces behind critical infrastructure protection—"For the Pentagon and the intel community, info 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, both military and civilian"—I think you are just dead wrong. That isn't how this all came about. It came about because a lot of serious people understood there was a significant threat and they wanted to do something about it.

And I really believe that in raising the questions you have raised, which I again acknowledge are legitimate questions and have not, I would add, been adequately answered by Mr. Tritak today, I think that the discussion needs to begin from a different point.

I would ask you this question. Having been critical, can you offer some suggestions as to how we might better balance the concerns for our protection from this cyber terrorism, on the one hand, and the very legitimate concerns you raised about personal privacy pro-

tection on the other? In other words, rather than just saying there is a huge problem here, the Government is trying to get into everybody's lives, how would you deal with the nature of this challenge? What kind of structure would you set up to provide the kind or protection that you are interested in?

Mr. ROTENBERG. Let me just say at the outset, Senator, I take your criticism. I know that you are referring to a report that we published last year. I should say that the words that you are quoting aren't actually my words. I mean, they were written by someone else. I did write the preface to the report, which I suspect you would probably agree with much of it because, as people know, I tend to be fairly balanced in my assessment of these issues, as I was in my statement for the subcommittee today. But I take your criticism and I think it is a fair one. I think these are real problems.

At the same time, I hope you would appreciate that for people who are concerned about privacy issues and civil liberties issues, there is a sense, as there is this morning, that these very elaborate programs are put together that have enormous civil liberties implications and sort of after the fact people say, and now we want to address privacy concerns, so that you will have to decide, for example, about whether to go forward with a FIDNet proposal that I believe, and even the Department of Justice believes, could be contrary to U.S. law. I think we have a good basis for our criticism.

But you asked me how do we resolve these two issues, and I have tried to suggest in my statement this morning that key to a successful answer is a successful and accurate description of the problem. We are not just defending U.S. borders anymore. I mean, the very interesting thing about Senator Bennett's picture is that this is a worldwide network, and the security solutions and the reliability solutions are being developed by researchers all around the world. U.S. firms, U.S. scientists, U.S. Federal agencies are benefiting today from work that is being done across the globe.

And I think we run some serious risk, if we are intent on trying to protect this network, by now erecting national borders in a world and in an environment where those national borders are just harder to control. Now, in saying this I am not trying to diminish the importance of national security or public safety. In fact, I think I am actually underscoring it.

I am simply trying to say that the problems that we face in the 21st century to protect these communication networks on which we depend are very different from the types of problems we confronted in the 20th century when we could follow airplanes moving in our air space, across our borders, destined for an attack.

Senator KYL. Conceded. We all make that point. We all agree. My question was, so how do you then deal with the issue, and I will ask Mr. Cilluffo to answer the same question. Just get specific for a minute, and we really need to specifically direct your answer to the question.

Mr. ROTENBERG. Fair enough. My first answer is I think we need a proposal that complies with U.S. privacy law. I don't think you can put forward a proposal that says we are concerned about privacy and at the same time ignore the relevant law that this Congress has passed which says that when the Government conducts

electronic surveillance, it has to comply with certain fourth amendment standards. That seems to me a fairly reasonable request to make.

I think a second point to make is that when you are creating within government a great surveillance capability, it is appropriate to have some mechanism for oversight and accountability. Now, I think this is an area, in fact, where Mr. Tritak has given a lot of thought. There is obviously an effort to work with the committees and to incorporate public comments, but that has to be done on a much more formal basis.

I mean, the Department of Justice has annual reporting requirements. The Computer Security Act has a formal committee that conducts hearings, issues reports. We need the types of institutional safeguards vested with the responsibility to protect privacy and civil liberties to counterbalance this very great surveillance authority that is going to be created.

And I should say, by the way, this hearing is really focusing on a small part of the Plan. I think there are large parts of the Plan where there is really no dispute. I mean, what we are really talking about today is whether, to protect computer security, the Federal Government should have openended authority to conduct computer surveillance.

Senator KYL. That is not true, that is just fundamentally not true. Nobody argues that the U.S. Government should have that authority, and if you would like to cite anybody that you can think of that comes at it from that point of view, I invite you to do so right now. You see, I think that is an exaggeration and it is the kind of statement that doesn't help us get to a constructive solution.

Senator Feinstein was saying just a moment ago that we start from the premise that the U.S. Constitution governs here. We have got to protect the liberties that are guaranteed in that document. The question is, with a brand new kind of technology here that we have all acknowledged eliminates the kind of formal barriers that used to instruct us on how to deal with these issues, we have got to come up with structures that, while they solve the problem, don't impinge upon constitutional liberties.

Just to give you one little illustration that is by analogy only—it is not directly applicable here—we have a bill that has passed the Senate unanimously dealing with Internet gambling. The 1961 Telephone and Wire Act prohibits sports gambling, but some defendants in a case said, well, wait a minute, to the U.S. attorney, you can't prove that that bet was transmitted over wire; it could have been through fiber optic cable or satellite microwave transmission.

The point is sometimes you have got to bring the law current with even the terminology of new technology, let alone the application of that technology. And it may be that some of these laws need to be brought up to date so that they enable us both to protect our security and protect the rights of the citizens. But don't start from the premise that it is zero-sum game and that the people that want to protect our security do not want to protect our privacy. It is just not true.

Mr. ROTENBERG. That is not my view, and it is not my view that it is a zero-sum game.

Senator KYL. Well, perhaps I misunderstood the comment you made.

Let me ask Mr. Cilluffo if he has some specific, constructive suggestions on how we square this circle, the challenge that Mr. Rotenberg has laid down.

Mr. CILLUFFO. Well, I think clearly the notion of partnerships, genuine partnerships that provide input from all different parties, is absolutely critical here. This is an issue that touches absolutely everyone, the civil liberties issues as well as the national security issues, and corporate issues such as intangible intellectual property rights and economic and industrial espionage.

There are a whole bunch of issues here that need to be brought to the table, and the only way you can begin doing that is by having this dialog. This table is much bigger than most traditional national security tables have been. It requires the input of so many new parties and so many different communities that I actually give the administration a lot of credit for adding that line to the Plan, an invitation to a dialog, because that is what we need; we need a dialog.

And while I agree that there are some very legitimate civil liberty issues that need to be addressed at that table, that is not the only issue that needs to be addressed, and I really don't see it as an either/or. I would accept nothing less than a plan that both protects our privacy and ensures our security. So the dialog, I think, is an important step. There are a number of initiatives within that, such as the information-sharing analysis centers where industry starts getting together doing some of the initiatives. We have parallel programs inside the Government, but the dialog is crucial.

Senator KYL. Well, let me say this and then I will turn to Senator Feinstein. I think before this is actually implemented, we will have additional hearings in which we will ask legal experts as well as technical experts to sit at this table and walk us through precisely how they envision it being done so that, for example, where they see—well, first of all, where they have the legal authority to look for these anomalies, what do they have the legal right to look for? What gives them that legal right? What kind of potential civil rights problems are there in looking for those anomalies?

Then what can they next do with that information? What is the next filter? Mr. Tritak envisions three or four layers or filters of analysis, as he pointed out. So when it gets to that next level, is there any further challenge to the civil liberties issues and what protections pertain there, all the way down to the hand-off to the FBI, the law enforcement agency, when they have reason to believe a crime might be being committed here, and therefore what the FBI must work—what strictures govern the FBI's actions here. I am sure those will be fairly standard law enforcement kinds of strictures.

But it is that initial broad-based analysis of anomalous information or incidents that probably raises the real questions because once you get to the FBI, I don't see a whole lot changing. I mean, they are going to be stuck with what they are stuck with the way we have got it pretty much written now. On the other hand, there

may be some new techniques that they would wish to employ based on new technology, and if that implicates privacy laws, then we will have to view it in that context.

So I think the challenge, Mr. Rotenberg, that you lay out is an appropriate challenge. I think we need to have people come and testify specifically about exactly what they are going to do because unless there is an acceptance of this by the American people, we are not going to be able to protect ourselves. And someday we will wish that we had tried to figure it out better in advance, and I appreciate your approach to that, Mr. Cilluffo.

Mr. CILLUFFO. Mr. Chairman, if I could add one point, too often the debate also focuses entirely on concerns of big brother. Well, the Government also has a responsibility to protect its citizens from little brothers. The thing that makes this threat so unique is that you don't need to be the United States, you don't need a major budget, you don't need to be the former Soviet Union or the People's Republic of China. Anyone can have a rudimentary capability, and we have a responsibility to protect our citizens.

Just imagine if we could not get our Social Security checks next month. I think people would be in the streets, arguably for good reason. Whether it is air traffic control and the like, I think that there are some very legitimate concerns that we need to look at it from the inverse perspective as well, not to mention that we are stuck prosecuting 21st century crimes with 20th century laws. I agree with Mr. Rotenberg's point, but it also has a flip side that needs to be on the table as well.

Senator KYL. Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Mr. Chairman. You know, I think that we are both on the same line here. I think we both believe that this is the frontier of a huge problem. I think we both believe that the technology is advancing so rapidly, so much quicker than our laws, our philosophy, our ability to really deal with it in any way.

At the same time, it is a whole new worldwide phenomenon and those that produce the phenomenon say, leave us alone, we don't want government interference. And it is very difficult to weigh the balance. On the one hand, you have commercially where people find their Social Security numbers being used without their permission, their drivers' licenses used without their permission, their medical information, their financial information. On one level, that sets up a huge level of privacy concern, and I think you and I will address it in a piece of legislation.

On the other level, you have this situation where a plane or planes go down in a cyber attack. Then what right does the Government have to infiltrate an encrypted computer system to try to get at the perpetrator? So it becomes two different sets of things we are looking at. At the same time, you have pointed out, and I think correctly, the technology is advancing so rapidly that by the time we get there, it is at the next stage.

It is a very hard challenge in front of us. I think we believe we have to do everything we can within protection of privacy to also protect our Nation and our people against attacks that we know as sure as the sun is coming up tomorrow morning are going to happen, and it is hard to get equipped to do so.

Now, let me ask a couple of questions, if I could, that are specific. Mr. Cilluffo, you mention that Congress should appropriate money for a governmentwide information security program such as encryption—and we have had a lot of debates over encryption—that is, a national public key infrastructure. Why do you believe that public key infrastructure is a good solution?

Mr. CILLUFFO. Well, it is not necessarily the encryption piece; it is the public key infrastructure writ large. I believe that that would raise the bar throughout our Federal systems to a level where you have the so-called 80-percent solution. Then the additional 20 percent that still could circumvent all these new protective measures that are put in place—we could focus on those specific threats which I think are the most critical to our national security.

From there, we can hone in our indications and warning capabilities and the like to deal with the more significant threats and keep out the 80 percent, the so-called ankle biters, that really are not significant national security issues.

Senator FEINSTEIN. Explain what you mean by public key.

Mr. CILLUFFO. It is heavily based on encryption means, but it goes beyond to incorporate other token key infrastructures. And to me, encryption is an important piece to protecting ourselves, but it doesn't do a whole lot to protect from denial of service attacks. What good is protecting the confidentiality and integrity of the information if you can't get a dial tone? But the PKI infrastructure does incorporate to add in some of the denial of service protection measures.

Senator FEINSTEIN. Thank you.

Mr. Rotenberg, you noted that many people used credit cards over this past holiday over the Internet, and that weaker encryption was freely available, I think you said due indirectly to the administration's old encryption control regulations. You then suggested that the National Plan will replicate the problem. I didn't understand what you meant. Could you explain it as to what exactly you mean?

Mr. ROTENBERG. Yes, Senator. What I was trying to describe was the problem that results from a Plan, you know, well-intended basically to keep these strong security tools away from people which could cause harm to the country, which is what the export control system does in part, had the practical consequence of keeping the same strong tools away from American consumers.

As computer security policies are implemented, there are all sorts of other effects that can be difficult to control, and it is a very good example, particularly with people using the Internet at Christmastime and making themselves vulnerable with credit card purchases. And I agree with you, by the way. I think that is also a very big part of the privacy issue. There are a lot of things happening obviously in the private sector that may require some government legislation to protect privacy and I would certainly support that.

But here you see sometimes a policy even well-intended that says we have got to try to keep good encryption away from the bad guys has the practical problem of keeping those same tools away from the good guys and leaving the good guys more vulnerable, and that is what I think we need to avoid duplicating.

Senator FEINSTEIN. Well, let me go back to the incident of the computer in Manila where the airline information was in it and this individual was going to bring down, if he could, a whole flock of commercial airliners. Fortunately, you could get into his computer and the information was there.

What is wrong with using the same procedure that one would use with a telephone? In other words, a wire tap; you go before a judge, you get a court order. You have to provide information to a judge, an independent third party, a reasonable cause to believe, et cetera. What is wrong with that procedure?

Mr. ROTENBERG. Actually, I think it is the right procedure.

Senator FEINSTEIN. I do, too.

Mr. ROTENBERG. And throughout the debate on encryption, you know, we really never argued about the Government's right to conduct a wiretap, with lawful authority, with a warrant. We said we understand that.

What we are really discussing is what kind of technological design, what kind of architecture for this evolving communication network is best likely to promote security and privacy. I agree with you, Senator Kyl. I think both goals are critical and we should not face a tradeoff where we are giving up one for the other.

And I guess the sense we have today after going through this long debate on encryption is that there really is a risk that if we focus solely on security, then privacy gets pushed off the table. It becomes sort of an after-the-fact consideration. And so we have to think at the very beginning when we are proposing, for example, public key infrastructure which could be very good to promote network security across Federal agencies—people filing tax returns, for example, make sure those aren't misappropriated. But we have to make sure at the beginning that privacy really becomes part of the design requirement so that we don't face the tradeoffs, and I think that is what I am saying.

Senator FEINSTEIN. Well, let me give you a challenge.

Mr. ROTENBERG. Yes.

Senator FEINSTEIN. I used to say when I was mayor to my staff—they would come in the door at the end of the day with a problem and I would say, don't come in with a problem unless you have got the solution, too. So let me give you that challenge. It is one thing to point out the problem, it is another thing to come up with a solution, and so I would like to challenge you to present us with some solutions.

Mr. ROTENBERG. Senator, I would be pleased to do that. In fact, I would offer to the subcommittee that there are groups of security experts. The American Association for Computing Machinery has been working in this area for a long time. I think we could put together a study group and maybe produce a report in a short period of time to try to answer this question for you. How do we do privacy and security so that both interests are protected as we go forward?

Senator FEINSTEIN. If I understood your opening comments, you would agree that there is a problem out there.

Mr. ROTENBERG. Yes.

Senator FEINSTEIN. So then all of us together, the privacy community as well as the governmental and the private sector, really

ought to come together to come up with the solution because we have to do that.

Mr. ROTENBERG. Yes, I agree.

Senator FEINSTEIN. Thanks, Mr. Chairman.

Senator KYL. Thank you very much. Well put. I was just thinking, just to close this off and put it in context, yesterday when I came through the security mechanism at the airport I was reminded again that just a little tiny bit of my civil liberties have been taken from me for a larger cause. Fortunately, I didn't have anything metal in my pockets to set the machine off, but if I had and I couldn't take it out of my pocket, then I get this routine which frequently happens to me. And I am standing there and somebody runs a little wand all over me.

Senator FEINSTEIN. Yes, me, too.

Senator KYL. Well, I don't care. It is a little bit of an inhibition on my freedom to come and go as I please, but the larger good of ensuring that I don't have some kind of terrorist device gives all of the people on the airplane I get on a sense of assurance that it is going to be OK. I think that is the kind of thing we are looking at here.

What kind of legitimate limitations are we willing to impose on ourselves in order to ensure that the entire Nation is not subject to this kind of terrorism or specific attack, and what kind of assurances can our Government provide its citizens that it has done only that which is necessary and no more? I think that is the nature of the challenge before us.

I will take you up on your offer, Mr. Rotenberg, and what I would like to do is ask both of you to come back or to provide testimony to the committee. I think that what this hearing has demonstrated is that in addition to a wide variety of other kinds of questions, we need to ask Mr. Tritak and others from the administration to be prepared to discuss specifics in the area that I think is most relevant to this subcommittee's jurisdiction which we will probably be dealing with in legislative form at a later date.

So I appreciate both of you being here to testify and we will leave the record open for any further comments you would like to make. In addition, we may have some other written questions that we would like to pose to you.

Thank you, Senator Feinstein. If there is nothing further, then we will adjourn this meeting, and I guarantee you we will have another hearing on this subject in the not too distant future.

Thank you very much. This hearing is adjourned.

[Whereupon, at 12:11 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS AND ANSWERS

RESPONSES OF JOHN TRITAK TO QUESTIONS FROM SENATOR JON KYL

Question 1. In his written testimony for the Subcommittee's February 1, 2000 hearing on critical infrastructure protection, Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, noted that, based on a March 1999 memo from the Justice Department to the CIAO, FIDNet is a "violation of the spirit of the federal wiretap statute, the plain language of the federal Privacy Act, and contrary to the Fourth Amendment." During the hearing, questions about legal authority for FIDNet were raised at the hearing, you testified that FIDNet is consistent with all "privacy laws", yet stated you were unfamiliar with whether Federal wiretap statutes applied to FIDNet. For the record, please explain in detail the current laws that apply to FIDNet, and specifically how FIDNet in its current conception is not in violation of each of those laws. Include, at a minimum, the Privacy Act, the Electronic Communications Privacy Act, the Computer Security Act, and wiretap statutes.

Answer 1. At the outset and before we can respond to your question fully, we need to make two observations as a backdrop for the discussion. First, the Federal Intrusion Detection Network (the "FIDNet") proposal was and continues to be a work in progress. Since the release of PDD–63 in May 1998, the Administration has worked carefully to identify the full range of possible security options that incorporate intrusion detection technology. The proposal as described in the earliest drafts of the National Plan has evolved considerably, and continues to evolve.

The second point to be made is that, as underscored in the National Plan, the FIDNet proposal will be implemented in a manner consistent with all relevant laws, including privacy laws. Our legal analysis of the proposal—and our ongoing consultation with the Department of Justice—continues as part of a comprehensive interagency process and in tandem with the evolution of the FIDNet to assure its adherence to the spirit and letter of law.

FIDNet has been carefully tailored to vest authority and control in the Federal civilian agencies, consistent with the Computer Security Act of 1987, Clinger-Cohen Act, and Executive Order 13011, which implement Congressional policies. Under current practices, federal agency computer system administrators (as well as system administrators in most companies in the private sector) already analyze data flowing over their systems, based on strategic placement of intrusion detection technology in accordance with the needs of the organization. Under the FIDNet proposal as currently formulated:

- The agencies will decide what data on system anomalies to forward to the GSA for further review;
- The GSA will use data on anomalies exclusively to warn agencies about system anomalies; and
- Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules (i.e., when there is evidence of a crime). No new authorities are implied or envisioned by the FIDNet program.

FIDNet is intended to be a multi-level system. At the first level, each agency's own security-protection software will scan for harmful traffic entering that agency's system. (The key to understanding intrusion detection is the concept of a "firewall," which by definition and design is meant to scan incoming transmissions for hostile files and programs.) In fact, this is already being done at federal agencies, not to

mention most private companies. The National Plan contemplates that the implementation and operation of such protective measures will continue to be the responsibility of the individual agencies. The objective of FIDNet is not to send the resulting information to law enforcement officials. Instead, the goal is to improve overall federal system security through improved information sharing among systems administrators and information security officials.

Contrary to Mr. Rotenberg's suggestion, the March 1999 Justice Department memorandum does not state at any point that FIDNet—even in the preliminary form then under analysis—would violate federal privacy law. On the contrary, the memorandum identifies the legal bases on which protective monitoring of government computer systems can be lawfully conducted.

In fact, the current FIDNet proposal is structured to comply fully with the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, which incorporates federal wiretap law. Specifically, while ECPA generally prohibits the interception of electronic communications, it contains two relevant exceptions to that general prohibition: (1) consent of a party and (2) system protection monitoring activities. As to the first of these, the federal agencies participating in FIDNet will, in appropriate instances, establish consent to monitoring by using login "banners" displayed to each network's users.

FIDNet will also rely on the separate exception applicable to systems protection. Under this exception, ECPA expressly authorizes a system owner or his agent to monitor network traffic on the system to the extent necessary to protect the "rights or property" of the system owner.

In addition, the FIDNet concept is compatible with the Privacy Act. The Privacy Act, designed to protect personal privacy from unwarranted invasions by federal agencies, regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies. It forbids the disclosure of personal information by federal agencies except under certain circumstances, and, subject to enumerated exceptions, gives individuals access to information maintained on them.

FIDNet will be fully consistent with the Privacy Act's requirement that physical security and information management practices be designed to ensure individual privacy. As properly and legally formulated, FIDNet will increase the level of privacy and security afforded to information about individuals on government computers.

Question 2. Is there a need for legislation to bring any of those laws up to date to reflect the current state of information technology? If so, please make specific suggestions?

Answer 2. No. No new authorities are implied or envisioned by the FIDNet program.

Question 3. If, in your view, any of those laws need to he updated, do your suggested changes erode privacy and civil liberties in any way?

Answer 3. As previously noted, no new authorities are implied or envisioned by the FIDNet program. In addition, our legal analysis of the proposal—and our ongoing consultation with the Department of Justice—continues as part of a comprehensive interagency process and in tandem with the evolution of the FIDNet to assure its adherence to the spirit and letter of law.

Starting from this point of seeking to protect privacy and civil liberties, we additionally remember your admonition that privacy and liberty are also endangered if we do nothing at all and leave the information on the government systems subject to attack and theft. I firmly believe that FIDNet will not erode privacy and civil liberties; indeed, by protecting citizen information communicated to government agencies from theft or improper release, and securing government systems from attacks by hackers, criminals and terrorists, FIDNet will ultimately serve to enhance privacy and liberty.

Question 4. In his written testimony for the Subcommittee's February 1, 2000 hearing on critical infrastructure protection, Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, stated "There are other indications, contained in materials that we received under the Freedom of Information Act, the CIAO intends to make use of credit card records and telephone toll records as part of its intrusions detection system, "and notes this raises problems under U.S. law. Does the CIAO intend to use credit card records and telephone toll records as part of its intrusion detection system?

Answer 4. There is not, nor has there ever been any intent to use credit card records and telephone toll records as part of an intrusion detection system. Mr. Rotenberg may be misconstruing and misinterpreting comments made about the technology used to detect anomalies in the use of telephone and credit cards.

In the early atages of the FIDNet process, the Administration considered, among others, the technology that telephone companies use to find abnormalities in behavior patterns—in their case for use of telephone phone credit cards—to see if that technology could be used to identify abnormal behaviors patterns on government networks. This was an examination of the underlying technology only, and had nothing to do with using actual phone number or credit card records.

Question 5. Mr. Rotenberg submitted the attached memo for the record at the hearing. The memo includes a chart referring to credit card and toll fraud profiling. Please explain the meaning of that slide.

Answer 5. Consistent with the response to the previous question, the only references to credit card and telephone toll records dealt with consideration of the underlying *technology models* and not with any specific credit card and telephone information. Since releaae of PDD–63 in May 1998, the Administration has reviewed carefully the full range of *available technologies* that may be applied to intrusion detection systems. The slide at issue relates to technology options discussed for the FIDNet. That is, the credit card and toll-fraud detection were only offered as an example of a type of detection technology currently in use.

Specifically, what was then being considered was the technology that telephone companies use to find abnormalities in behavior patterns—in their case for telephone of phone credit cards use—to see if it could be used to identify abnormal behaviors patterns on our networks. This was an examination of the underlying technology only, and had nothing to do with using actual phone number or credit card records.

Question 6. Please provide an outline of FIDNet in its current stage of development.

Answer 6. At present, FIDNet remains entirely on the drawing board. The program plan for fiscal year 2000–2001 relies upon the experience and expertise of the vendor community to actually develop the technical architecture(s) for FIDNet.

An initial Request for Proposal (RFP) from the General Services Administration (GSA) will solicit such architectures from the corporate sector. The expectation is that these architectures will come from those companies that already provide intrusion detection products and services both to industry and government. While the RFP will document all known legal constraints upon the Network, the program plan still calls for yet another legal review of each of the vendors' submissions by the Department of Justice. Depending upon the build costs of the remaining vendor proposal's (those proposed architectures which pass legal muster with the Department of Justice) and the amount of available funding, the GSA Program Office will then fund development of between two and five FIDNet prototypes. The prototypes must then prove the technical, operational and practical viability of their architectures while continuing to steer clear of any new legal/privacy constraints that Justice may have identified. The extent to which the prototypes prove they actually meet all system requirements: technical, legal, privacy-related, operational and fiscal (i.e., best value for the Government) will determine the winner in final Source Selection.

Question 6a. Describe which practices of surveillance and monitoring already take place in individual agencies.

Answer 6a. Because the Program Office is just getting under way, GSA has not yet had the opportunity to begin a comprehensive survey of government agency intrusion detection practices, which products they may have purchased from which vendors, and how the agencies actually employ the intrusion detection systems they have already purchased.

We will keep the Subcommittee informed about the development of the FIDNet proposal and about the information that GSA assembles concerning intrusion detection practices in various agencies.

Question 7. Using the model of FIDNet, explain what type of monitoring would apply to a citizen, in his home who logs on to a government web site. What types of activities would that citizen have to do to "set off a typical intrusion detection system (understanding that different government agencies have varying IDSs)?

Answer 7. Merely accessing a public government web site over the Internet would not be the kind of activity that would trigger an intrusion detection system. That activity is not only exceedingly common, but is entirely expected and encouraged. After all, government agencies' web pages are posted so that they may be accessed and read by the general public.

It is safe to assume, however, that sending e-mail infected with a virus or worm to a government office would certainly activate the agency's anti-virus software and thus "set off" the intrusion detection system of a given agency. Participation in distributed Denial of Service (DDOS) attacks, such as those that recently shut down

Yahoo!®, e-Bay® and other popular commercial web pages, would most likely also trigger an alert.

Please be aware that it will be the systems administrators in the individual agencies who will determine for each critical computer system what type of activity sets off their alarm(s), and what data (within legal constraints) will be sent via FIDNet to the Federal Computer Incident Response Capability (FedCIRC) at GSA when unauthorized activity is suspected. Given the sorts of intrusion detection systems on the market today, agencies' traffic monitoring typically notices anomalous activity that may indicate an unlawful intrusion into a significant information system—such as attempts to enter a government computer system at an unusual port of entry or the delivery/execution of certain types of files that are typically used as vehicles for hostile code, *e.g.*, Trojan horses.

Question 8. While much of the national plan deals with protection against cyber attack, milestone 1.7 calls for all agencies to cooperate in the construction of a program to protect critical infrastructures against physical attack, by terrorists or others. This part of the plan is scheduled to be complete by June 2000. Could you please elaborate on what this part of the plan will consist of?

Answer 8. The National Plan for Critical Physical Infrastructure Protection (NPCPIP) will strengthen our economic and national security through the identification and remediation of critical physical infrastructure vulnerabilities. The plan involves asset identification, process and procedure integration, risk mitigation, remediation, incident reports, response, and interdependency understanding.

The Information Technology revolution that has taken place in America during the 1990s, and the dependence on information systems it has created, makes a national level program for information systems security and defense essential. Given the urgent need for an information systems security and defense plan, and because of the breadth of this topic, the *National Plan for Information Systems Protection,* released by the President on January 7, 2000, focuses on protection of critical information infrastructures from both cyber and physical attack. It excludes consideration of other critical physical infrastructures and security issues related to them.

America depends on both the physical and cyber portions of her critical infrastructures for economic and national security. A cyber event can cause a disruption of a physical infrastructure (e.g., power overload leads to a transformer or substation problem); a physical event/incident can disrupt a cyber infrastructure (e.g., a communications substation or electric transformer problem negatively impacts/degrades Secure Supervisory Control and Data Acquisition (SCADA) or communications systems).

A physical infrastructure plan will integrate the cyber and physical aspects of critical infrastructure protection. All infrastructures consist of both cyber and physical elements and it is important not to separate them, specifically when one considers business continuity and target opportunities. However, for purposes of this plan, we must view the physical infrastructures from a national lens, and thus, we will define critical physical infrastructures to be those that would have broad reaching consequences, e.g. those that would impact on major geographical, economical, regional, or national security levels, if their services or operations were disrupted.

Therefore, to address the physical vulnerabilities of non-cyber infrastructures, a new Critical Physical Infrastructure Protection Plan is being developed to identify the necessary initiatives and programs for ensuring protection of these infrastructures. The CIAO will lead this effort and will work with an inter-agency Task Group which will include DoD, FBI, and other agencies. These elements along with reviews of existing critical physical infrastructure security programs will lead to *The National Plan for Critical Physical Infrastructure Protection* (NPCPIP) to be issued in 2000.

Participating Agencies in NPCPIP Task Group.
Chair/Lead: CIAO*
Sector Liaison Agencies:
- Information & Communications—DOC
- Banking & Finance—Treasury*
- Transportation—DOT*
- Energy—DOE*
- Emergency Fire Service/Continuity of Government—FEMA*
- Public Health—HHS
- Water Supply—EPA*

Lead Agencies for Special Functions:
- Intelligence—CIA
- Foreign Affairs—State
- Law Enforcement—DOJ/FBI*

National Defense—DoD*
Federal Government (Non-DoD)—GSA*
Others:
NSC
Local Law Enforcement—Sheriff, Arapaho Co, Colorado
NSTAC (National Security Telecommunications Advisory Council)—(in a consultant status)
OMB
USDA (Agriculture)
DOI (Interior)
HHS (Health & Human Services)

**Mandatory—will form the core-writing contingent for the physical plan, other organizations including the NSTAC will be used in a reviewer/consultant role.*

Question 8a. Do each of the agencies involved have the expertise to accomplish this study, or are some agencies, such as the FBI and Defense Department being called on to assist other agencies?

Answer 8a. As described above, an interagency task force is developing the NPCPIP. No single agency, alone, has the knowledge base to complete the effort. It should be noted that this plan will not take the form of an agency-by-agency plan, but a cross-sectoral approach.

Question 9. The Plan states that "Federal Agencies aad Departments should have assessed information systems vulnerabilities, adopted a multi-year funding plan to remedy them, and created a system for continuously updating. Private sector companies of every critical sector could do the same. 7 (Milestone 1.21). Is there a need for legislation to ensure that private sector owners and operators do this?

Answer 9. We do not envision the need now for new legislation. Individual companies already address security to varying levels. The degree depends on their level of awareness and understanding of how critical information systems are to their business operations and to their ability to assure reliable services and delivery of products to their customers and the communities they serve. An industry awareness initiative will create market forces that will inevitably elevate the level of attention and investment by industry, an example of which we saw with the Year 2000 conversion experience. At some point, we may recognize a gap between what national security needs for critical infrastructure security and what companies believe their customers and communities are willing to pay for. At that time, additional incentives may be needed for industry to step up to additional levels of investment beyond what the market supports.

Information security, unlike the Year 2000 conversion, has no end point. Consequently, it will require an on-going commitment and institutionalization of controls into core business processes. Technology also continues to change very quickly, requiring continuing attention and investment from those who would benefit from it. Obtaining buy-in from industry in their own business interests will more effectively address this issue in a timely and creative manner.

Question 9a. Other than legislation requiring private companies to undertake this sort of planning, are there other incentives we could use to encourage firms in key sectors to be more pro-active in making their computer networks more secure?

Answer 9a. The most effective incentive for corporations to take action is for the government to articulate its concern in business terms. The government's real focus is on predictable delivery of critical services that enable the government to satisfy its national security responsibilities and foster a competitive economy. Private industry succeeds by providing most of these services. If the government is successful in conveying its message, industry will take action based on sound business management practices.

Question 10. What is the status of the development of Information Sharing and Analysis Center (ISACs), which are intended to bring together companies in key sectors like banking and telecommunications to facilitate the sharing of information about cyber threats and best practices for addressing vulnerabilities?

Answer 10. Building the public-private partnership to ensure action is at the core of the National Plan. Without the full participation of the private sector, federal actions to protect critical infrastructures will not be fully effective. PDD–63 suggests that the private sector, in cooperation with the Federal government, establish Information Sharing and Analysis Centers (ISACs) to facilitate public-private information sharing on vulnerabilities, threats intrusions, and anomalies. It should be noted, however, that ISACs are only one of the many information-sharing mechanisms now employed by the private sector.

Last October, Banking and Finance publicly announced the creation of the Financial Services Information and Analysis Center (FS–ISAC). This is the first center that is operational and it is currently recruiting members from the entire financial industry.

The National Coordinating Center (NCC) for Telecommunications, established in 1984, already performs many of the functions of an ISAC for the telecommunications industry.

The electric power industry, through the North American Electric Reliability Council (NERC), has developed a reporting process and specific data elements on incidents to be shared with the National Infrastructure Protection Center (NIPC). This reporting process was built on a reporting structure and process that already exists within the electric industry to support the reliability, availability, and integrity of the nation's electric grid.

There are other information sharing vehicles in private industry, created for paying members. Many of the large consulting and technology firms provide similar or equivalent services to their customers. Many of these share relevant information with the government.

The government is also engaged in a dialogue with the Partnership for Critical Infrastructure Security to explore the value and feasibility of cross-sector information sharing regarding common threats, experiences, and best practices.

Question 11. Pages 24 and 25 of the executive summary of the Plan describe deterrents and obstacles to companies who wish to share information on cyber-threats with the government. How can we remove these obstacles to encourage companies to share such information with the government? Do you need help from Congress to address these impediments?

Answer 11. Many owners and operators of critical infrastructures and industry officials have expressed reluctance to share information about threats and vulnerabilities with the government. The degree of reluctance varies according to infrastructure, but is present in each. Only 17 percent of respondents who experienced an attack during the previous year reported it to law enforcement, according to the President's Commission on Critical Infrastructure Protection, which published its findings in October 1997.

In a recent meeting with industry officials they have suggested that they would be reluctant to share such proprietary information or to participate in information sharing programs for a number of reasons. They fear information provided to the government may be made public and thereby damage their reputations, expose them to liability, or weaken their competitive position. In addition, potential contributors from the private sector are reluctant to share specific threat and vulnerability information because of impediments they perceive to arise from antitrust and unfair-business laws.

With this dilemma in mind, an interagency group was formed in August 1999 to consider a non-disclosure provision that would allow Federal agencies to accept voluntary contributions of certain security-related information outside the operation of the Freedom of Information Act (FOIA). The information in question would not be of the type normally disclosed either to the Federal government or to the public. In the near future, the group plans to address antitrust and liability issues.

In each of these cases, we will need to work closely with Congress and the privacy community in developing effective solutions and removing these obstacles.

Question 12. The Plan refers to the Partnership for Critical Infrastructure Security. Furthermore, milestone 8.2 states that this partnership will be created this month. What is it and how will it be created?

Answer 12. The Partnership for Critical Infrastructure Security was created on February 22, 2000 at an organizational meeting held at the U.S. Chamber of Commerce. Over 120 companies attended (with more on the waiting list that could not be accommodated, but who want to join the partnership).

The Partnership is intended to be a collaborative effort of industry and government to assure the delivery of essential services over the nation's critical infrastructures. These infrastructures, identified in Presidential Decision Directive 63 (PDD–63), include:

- Energy
- Financial Services
- Transportation
- Communications and Information Services
- Vital Human Services, including Health, Safety, and Water

Private sector membership in the Partnership is open to infrastructure owners and operators, providers of infrastructure hardware, software, and services, risk management and investment professionals, and other members of the business community. Government representation will include state and local governments, as well as Federal agencies and departments responsible for working with the critical infrastructure sectors and for providing functional support for the protection of those infrastructures.

The Partnership recognizes that the nation's critical services depend increasingly on commercial information technologies. The new threats and vulnerabilities that come with greater dependency on these technologies, combined with the growing interdependencies among the nation's critical infrastructures, require urgent attention not only in the government but also in the business community.

The Partnership recognizes that in addition to protecting these infrastructures, attention must be given to the range of actions necessary to assure the delivery of critical services—including mitigation, response, and reconstitution.

Since the vast majority of the critical infrastructures of the United States are owned and operated by private industry, the Partnership recognizes and acknowledges that the Federal government alone cannot protect these infrastructures or assure the delivery of services over them. While most of the challenges to assuring critical services are best handled by industry itself, the Partnership is based on the premise that some of these challenges are better handled by industry and government working together.

The Partnership will explore ways in which industry and government can work together to address the risks to the nation's critical infrastructures. Federal Lead Agencies are currently building partnerships with individual infrastructure sectors in private industry, and state and local governments. The Partnership will provide a forum in which to draw these individual efforts together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness and understanding of, and to serve, when appropriate, as a catalyst for action among, the owners and operators of critical infrastructures, the risk management and investment communities, other members of the business community, and state and local governments.

How the Partnership conducts itself—how it is organized, and how it manages its on-going operations—will largely be determined by its industry members. For its part, the Federal Government is prepared to sponsor on behalf of the Partnership a series of conferences, meetings, and working groups with industry and government executives to:

- Exchanges views on issues of mutual interest to the government and members of industry, including, but not limited to:
  - Interdependencies, including cross-sector information sharing arrangements and the appropriate safeguards for protecting the confidentiality of such information;
  - Evolving threats to critical infrastructures;
  - Education, training and workforce development;
  - Standards and Best Practices;
  - Technology and R&D;
  - Risk Management: prevention, mitigation, response, and reconstitution, including incident response management and consequence management; and,
  - Legal and regulatory matters.
- Facilitate the participation of members of industry in the ongoing development of the national plan for critical infrastructure protection; and,
- Facilitate contributions by members of industry to the work of the National Infrastructure Assurance Council.[1]

[1] President Clinton established the National Infrastructure Assurance Council (NIAC) by Executive Order 13130 on July 14, 1999. The Council will consist of up to 30 leaders in industry and state and local government. Its mandate is to advise and counsel the President on a range of policy matters relating to critical infrastructure assurance, including the enhancement of public-private partnerships, generally. The Partnership for Critical Infrastructure Security could serve as one important channel of communication to the NIAC, ensuring that Council members have the full benefit of a wide cross-section of industry views.

RESPONSES OF JOHN TRITAK TO QUESTIONS FROM SENATOR JOSEPH R. BIDEN, JR.

Question 1. Mr. Tritak in light of privacy advocates' criticism of the Federal Intrusion Detection Network (FIDNet) program, how can you guarantee that civil liberties are protected and that FIDNet will not violate current privacy protection, wiretap and 4th amendment law?

At the outset and before we can respond to your question fully, we need to make two observations as a backdrop for the discussion. First, the Federal Intrusion Detection Network (the "FIDNet") proposal was and continues to be a work in progress. Since the release of PDD–63 in May 1998, the Administration has worked carefully to identify the full range of possible security options that incorporate intrusion detection technology. The proposal as described in the earliest drafts of the National Plan has evolved considerably, and continues to evolve.

The second point to be made is that, as underscored in the National Plan, the FIDNet proposal will be implemented in a manner consistent with all relevant laws, including privacy laws. Our legal analysis of the proposal—and our ongoing consultation with the Department of Justice—continues as part of a comprehensive interagency process and in tandem with the evolution of the FIDNet to assure its adherence to the spirit and letter of law.

FIDNet has been carefully tailored to vest authority and control in the Federal civilian agencies, consistent with the Computer Security Act of 1987, Clinger-Cohen Act, and Executive Order 13011, which implement Congressional policies. Under current practices, federal agency computer system administrators (as well as system administrators in most companies in the private sector) already analyze data flowing over their systems, based on strategic placement of intrusion detection technology in accordance with the needs of the organization. Under the FIDNet proposal as currently formulated:

- The agencies will decide what data on system anomalies to forward to the GSA for further review;
- The GSA will use data on anomalies exclusively to warn agencies about system anomalies; and
- Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules (i.e., when there is evidence of a crime). No new authorities are implied or envisioned by the FIDNet program.

FIDNet is intended to be a multi-level system. At the first level, each agency's own security-protection software will scan for harmful traffic entering that agency's system. (The key to understanding intrusion detection is the concept of a "firewall," which by definition and design is meant to scan incoming transmissions for hostile files and programs.) In fact, this is already being done at federal agencies, not to mention most private companies. The National Plan contemplates that the implementation and operation of such protective measures will continue to be the responsibility of the individual agencies. The objective of FIDNet is not to send the resulting information to law enforcement officials. Instead, the goal is to improve overall federal system security through improved information sharing among systems administrators and information security officials.

Contrary to Mr. Rotenberg's suggestion, the March 1999 Justice Department memorandum does not state at any point that FIDNet—even in the preliminary form then under analysis—would violate federal privacy law. On the contrary, the memorandum identifies the legal bases on which protective monitoring of government computer systems can be lawfully conducted.

In fact, the current FIDNet proposal is structured to comply fully with the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, which incorporates federal wiretap law. Specifically, while ECPA generally prohibits the interception of electronic communications, it contains two relevant exceptions to that general prohibition: (1) consent of a party and (2) system protection monitoring activities. As to the first of these, the federal agencies participating in FIDNet will, in appropriate instances, establish consent to monitoring by using login "banners" displayed to each network's users.

FIDNet will also rely on the separate exception applicable to systems protection. Under this exception, ECPA expressly authorizes a system owner or his agent to monitor network traffic on the system to the extent necessary to protect the "rights or property" of the system owner.

In addition, the FIDNet concept is compatible with the Privacy Act. The Privacy Act, designed to protect personal privacy from unwarranted invasions by federal agencies, regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies. It forbids the disclosure of personal in-

formation by federal agencies except under certain circumstances, and, subject to enumerated exceptions, gives individuals access to information maintained on them.

FIDNet will be fully consistent with the Privacy Act's requirement that physical security and information management practices be designed to ensure individual privacy. As properly and legally formulated, FIDNet will increase the level of privacy and security afforded to information about individuals on government computers.

Question 2. What type of data will be collected by FIDNet and how long will the Government Services Administration retain the data?

Answer 2. FIDNet will not deploy collectors or sensors on any government agencies or other entity network. This is the job of the agency systems administrators and their intrusion detection systems. Instead, the FIDNet will receive from the agencies, under processes established by the agency systems administrators, only those alarm indications that the agency internal intrusion detection systems identify as anomalous and that the agency systems administrators forward to FIDNet.

Intrusion detection system alarm data typically have a short shelf-life and GSA does not envision a need to retain this data. However, legal requirements relating to government records may mandate that certain records be retained or archived in accordance with schedules established in accordance with law. This issue is currently being reviewed. Of course, GSA will continue to adhere to existing laws with respect to records involving law enforcement matters.

RESPONSES OF JOHN TRITAK TO QUESTIONS FROM SENATOR DIANNE FEINSTEIN

Question 1. Does FIDNet comply with the Wire Tap Laws?

Answer 1. Yes, FIDNet complies with the wiretap laws.

At the outset and before we can respond to your question fully, we need to make two observations as a backdrop for the discussion. first, the Federal Intrusion Detection Network (the "FIDNet") proposal was and continues to be a work in progress. Since the release of PDD–63 in May 1998, the Administration has worked carefully to identify the full range of possible security options that incorporate intrusion detection technology. The proposal as described in the earliest drafts of the National Plan has evolved considerably, and continues to evolve.

The second point to be made is that, as underscored in the National Plan, the FIDNet proposal will be implemented in a manner consistent with all relevant laws, including privacy laws. Our legal analysis of the proposal—and our ongoing consultation with the Department of Justice—continues as part of a comprehensive interagency process and in tandem with the evolution of the FIDNet to assure its adherence to the spirit and letter of law.

FIDNet has been carefully tailored to vest authority and control in the Federal civilian agencies, consistent with the Computer Security Act of 1987, Clinger-Cohen Act, and Executive Order 13011, which implement Congressional policies. Under current practices, federal agency computer system administrators (as well as system administrators in most companies in the private sector) already analyze data flowing over their systems, based on strategic placement of intrusion detection technology in accordance with the needs of the organization. Under the FIDNet proposal as currently formulated:

- The agencies will decide what data on system anomalies to forward to the GSA for further review;
- The GSA will use data on anomalies exclusively to warn agencies about system anomalies; and
- Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules (i.e., when there is evidence of a crime). No new authorities are implied or envisioned by the FIDNet program.

FIDNet is intended to be a multi-level system. At the first level, each agency's own security-protection software will scan for harmful traffic entering that agency's system. (The key to understanding intrusion detection is the concept of a "firewall," which by definition and design is meant to scan incoming transmissions for hostile files and programs.) In fact, this is already being done at federal agencies, not to mention most private companies. The National Plan contemplates that the implementation and operation of such protective measures will continue to be the responsibility of the individual agencies. The objective of FIDNet is not to send the resulting information to law enforcement officials. Instead, the goal is to improve overall federal system security through improved information sharing among systems administrators and information security officials.

Contrary to Mr. Rotenberg's suggestion, the March 1999 Justice Department memorandum does not state at any point that FIDNet—even in the preliminary form then under analysis—would violate federal privacy law. On the contrary, the memorandum identifies the legal bases on which protective monitoring of government computer systems can be lawfully conducted.

In fact, the current FIDNet proposal is structured to comply fully with the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq., which incorporates federal wiretap law. Specifically, while ECPA generally prohibits the interception of electronic communications, it contains two relevant exceptions to that general prohibition: (1) consent of a party and (2) system protection monitoring activities. As to the first of these, the federal agencies participating in FIDNet will, in appropriate instances, establish consent to monitoring by using login "banners" displayed to each network's users.

FIDNet will also rely on the separate exception applicable to systems protection. Under this exception, ECPA expressly authorizes a system owner or his agent to monitor network traffic on the system to the extent necessary to protect the "rights or property" of the system owner.

In addition, the FIDNet concept is compatible with the Privacy Act. The Privacy Act, designed to protect personal privacy from unwarranted invasions by federal agencies, regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies. It forbids the disclosure of personal information by federal agencies except under certain circumstances, and, subject to enumerated exceptions, gives individuals access to information maintained on them.

FIDNet will be fully consistent with the Privacy Act's requirement that physical security and information management practices be designed to ensure individual privacy. As properly and legally formulated, FIDNet will increase the level of privacy and security afforded to information about individuals on government computers.

Question 2. Under what legal authority does FIDNet function?

Answer 2. The Administration is committed to structuring the FIDNet concept in strict adherence to exiting protections under the law, including ECPA (Wiretap Statutes), the Privacy Act, and other laws. Please refer to Question 1 above for more details.

Question 3. How are FIDNet and the NIPC redundant?

Answer 3. They are not. FIDNet, when operational, will be a service offered by the GSA to the civilian departments and agencies to help them improve information sharing within the Federal civilian government amongst systems administrators. This information sharing covers the efficiency and reliability of intrusion detection systems which some agencies already employ in accordance with OMB Circular A–130. In short, the FIDNet is a centrally managed operational structure that permits GSA to look at and draw conclusions about anomalous cyber activity across the federal civilian government in a way that no single agency could do for itself.

In contrast, the NIPC serves as the national focal point for threat assessment, warning, investigation, and response to attacks on the critical infrastructures. A significant part of its mission involves establishing mechanisms to increase the sharing of vulnerability and threat information between the government and private industry. It also provides invaluable input and capabilities to federal law enforcement and defense cyber operations.

Question 4. Give your opinion on the GAO's assertion that the current laws governing IT Security are outdated.

Answer 4. The management of information security in the Federal government is an issue that is currently being debated in the Congress and the Administration, including in legislation such as S. 1993. Accordingly, the only observation I would make at this time is that we should rely on the existing legal framework, to the extent we can continue to assure ourselves that the system is working, is effective, and is providing the appropriate level of protection for the full range of proprietary, personal, and other sensitive information.

Question 5. Is there a need to tailor infosec standards to certain types of information, and if so how?

Answer 5. As discussed above, the only observation I would offer on this subject is that information technology is developing rapidly and that critical infrastructure protection needs to be an essential part of that development, if we are to build secure infrastructures. We should rely on the existing legal framework, to the extent we can assure ourselves that the system is working, is effective, and is providing the appropriate level of protection for proprietary, personal and other sensitive information.

Question 6. Should Congress approve more money for PKI?

Answer 6. Public Key Infrastructure (PKI) maximizes our capability to implement needed security services including confidentiality, integrity, authentication, non-repudiation and access control. PKI facilitates the secure exchange of information electronically. It is a key element for gaining increasing trust and confidence in the use of this medium for commercial applications.

Today, cryptography is the most viable means of protecting information in cyberspace. As mentioned, public key cryptography, based on a PKI, maximizes our capability to implement needed security services including confidentiality, integrity, authentication, non-repudiation and access control. Appropriate combinations of these services allow us to protect information stored and transmitted over the Internet from our lap-top and desk-top computers. The PKI also allows us to configure firewalls and other Internet components to protect the internal domain name services and routing table information. These PKI security services enable secure e-commerce, e-mail and a myriad of important large distributed applications including those that provide Government services.

Appropriated monies for PKI would be well spent in the following areas:

PKI Standards, Testing and Product Certification—As industry responds to a growing customer base for PKI products, innovative and enterprising solutions are finding their way into large international markets. Of critical importance to the Government is the interoperability of a Government PKI with those of the public and private sectors and other sovereign governments. It is unlikely that these industry PKI solutions will meet all the unique Government PKI requirements. Appropriate testing and high confidence certifications for Government PKIs often go well beyond the interoperability and testing requirements of other PKIs. Additional government activities in interoperability standards development and in testing and certification are needed.

PKI Research and Development—The Next Generation Internet (NGI) holds the promise of extremely high bandwidth, rich connectivity and extremely efficient large distributed applications. It is prudent to plan now for the security services that will likely be required for the NGI. Three interagency working groups are coordinating expertise to begin the process: The Large Scale Networking Next Generation Internet (LSN/NGI), the High Confidence Systems (HCSS) and the Critical Infrastructure Protection (CIP) communities have expressed interest in a Public Key Infrastructure for the Next Generation Internet. Additional government activities in defining the transition strategy from current PKI for the Internet to a PKI for the NGI is rightfully a research and development idea with low risk and high potential payoff for both our nations next generation critical infrastructures and our governments next generation needs and requirements.

Our models for secure e-commerce and e-mail have been tested with prototype implementations; but, not stressed. We need real experiences with a Government PKI that provisions security in large, scalable high-speed dynamic group communications similar to those used by our emergency response communications and messaging systems and other critical government systems. We know little about integrating PKI into large legacy applications used by the Government to provision services for the public. We know even less about integrating PKI into new, as yet untested, major applications that serve the public.

Operational Critical Systems—While PKI technology by itself cannot completely protect critical operational systems, PKI is considered a necessary component when cryptography is deployed. Biometric techniques used in conjunction with PKI can provide high-grade authentication of people accessing critical assets. In addition, digital signature techniques based on PKI can provide integrity and non-repudiation of information and transactions—a key element in audit trail techniques. The monies necessary to upgrade legacy systems with PKI technology often come out of agency security budget lines. Monies specifically approved for PKI by the Congress would have the immediate effect of forming the critical mass necessary to jumpstart the Government's PKI.

○