cc: Epstein
Rinaldi

COMMITTEE ON ARMED SERVICES

U.S. House of Representatives

Washington, DC 20515–6035

ONE HUNDRED SIXTH CONGRESS

FLOYD D. SPENCE, SOUTH CAROLINA, CHAIRMAN

February 18, 2000

Smith
Gibson

Dr. Neal Lane
Assistant to the President for Science and Technology
Office of Science and Technology Policy
1600 Pennsylvania Ave, N.W.
Washington, DC 20502

Dear Dr. Lane:

The House Armed Services Subcommittees on Military Readiness and on Military Research and Development will hold a hearing on "Information Superiority and Information Assurance: Meeting the Challenges of the 21st Century," on Thursday, March 8th at 3:00 p.m. in 2118 Rayburn House Office Building. The hearing is the fourth in a series of hearings since 1997 on the Department of Defense's information superiority program and the measures required by the U.S. armed forces and supporting agencies to achieve information superiority over any future adversary and to protect the defense information infrastructure and supporting critical civil information infrastructure. Of particular interest in this hearing is an overview of the progress made in the Administration's Critical Information Protection program and the information technology research and development programs and initiatives that support the program; and progress in achieving the objectives of the Department of Defense's information technology and assurance programs, program strategy, information assurance activities, program and budget requirements, and identification of critical deficiencies and shortfalls in the Department's program. You are invited to testify in order that the subcommittees may benefit from your perspective on these important topics.

The hearing will be conducted in two panels: the first to establish the overall context of the Critical Information Protection program and progress at the interagency level, and the second to discuss Department of Defense information assurance policy and programs and supporting programs of the military departments and defense agencies.

Committee Rule 13 provides that witness statements must be delivered to the committee at least 48 hours in advance of the hearing to facilitate distribution of the statement to the members. Therefore, it is requested that 100 copies of your prepared statement be delivered to 2340 Rayburn House Office Building by Monday, March 6. In addition, consistent with the House rule requirement to make materials from hearings

electronically available to the general public, Committee Rule 13 also requires that witness statements be provided to the committee in electronic form. It is therefore requested that along with the hard copies of your statement, you also forward an electronic copy on a 3.5-inch MS-DOS diskette, either in Microsoft Word, ACSII or DOS text format.

We appreciate your willingness to appear before the subcommittees and look forward to your testimony. Should you have any questions, please contact Mr. Jean Reed (202-225-5540) on the committee staff.

Sincerely,

Herbert H. Bateman
Chairman, Subcommittee on
Military Readiness

Curt Weldon
Chairman, Subcommittee on
Military Research & Development

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
NATIONAL SECURITY & INTERNATIONAL AFFAIRS DIVISION
494 OLD EXECUTIVE OFFICE BUILDING
WASHINGTON, DC 20502

DATE: **February 25, 2000** **PAGES (Including Cover): 35**

TO: **Neal Lane**
PHONE: **703-698-9578**
FAX: **703-698-1579**

FROM: **Gerald Epstein**
PHONE: **202-456-6061**
FAX: **202-456-6028**

****

Here is a draft of your written testimony. We have also provided some additional background for your information. We will prepare a draft for your oral remarks once the written remarks have been sent out to OMB.

A. Draft written testimony (10 pp.)
B. Presentation that outlines our interagency coordination process. We are preparing an additional presentation for your information that provides more detail about the interagency process (14 pp.)
C. Cybersecurity Fact Sheets released on January 7 and on February 15, 2000 (10 pp.)

DRAFT

TESTIMONY

OF DR. NEAL LANE

BEFORE THE HOUSE ARMED SERVICES COMMITTEE

8 March 2000

Mr. Chairman, members of the Committee, I would like to thank you for this opportunity to discuss research and development (R&D) activities that the federal government is conducting to improve our ability to protect the nation's critical infrastructures. You are all familiar with the challenges facing our nation as we take measures to ensure the robust and reliable operation of our critical infrastructures. This is truly a national challenge – one that goes beyond the traditional bounds of national security. Our economic security, competitiveness, and our way of life also rest upon the continuous and assured availability of the services provided by our infrastructures – reliable services that we all too often take for granted.

Research and development is – and must be – a key element of an integrated national agenda to protect our critical infrastructures. The President recognized this fact in May, 1998 when he issued Presidential Decision Directive PDD-63 on Critical Infrastructure Protection (CIP). Among other things, this Directive tasked the Office of Science and Technology Policy to coordinate the federal government's critical infrastructure protection R&D. Accordingly, I have made critical infrastructure protection R&D one of my national R&D priorities for the second year running. More recently, the President underscored the importance of protecting our national information infrastructure by requesting funds to establish an Institute for Information Infrastructure Protection. This Institute, working closely with the private sector and academia, will focus upon the development of technologies that neither the government nor the private

sector are currently developing, yet are crucial to the security of our information infrastructure. The importance of critical infrastructure protection R&D is reflected in the President's FY2001 budget which contains $606 million for CIP R&D, an increase of $145 million (31%) from last year's enacted funding level.

Coordinating Federal Critical Infrastructure Protection R&D

In recognition of the crucial role R&D plays in infrastructure protection, two years ago this month my office established an interagency working group and process to develop and coordinate the federal government's critical infrastructure protection R&D agenda. This group has operated through two budget cycles and has recently commenced work on a third. I emphasize the word "coordinate" – even before we created our working group, the federal government conducted many R&D programs that either directly or indirectly contributed to infrastructure protection. However, the heart of our interagency process is the coordination of these programs, ensuring that they all aim toward common goals and address crucial vulnerabilities and threats. We have gotten off to an excellent start, and I will share some of our successes with you shortly.

I would like to emphasize several key facets of our interagency process. First, all programs recommended in the R&D agenda are tied to vulnerabilities or R&D shortfalls. A number of recent reports, in both the private sector and government, have outlined vulnerabilities in our infrastructures. We ensure that each of our R&D programs, whether ongoing or a proposed new start, directly addresses one or more infrastructure vulnerabilities.

highlighted

Second, we ensure that each agency is aware of the others' R&D programs. Compiling information about each agency's R&D, and sharing this information with all other participating agencies, helps agencies leverage each other's investments and avoid duplication of effort. In this way, individual critical infrastructure protection R&D programs become a unified interagency product – a package coordinated and integrated across agency boundaries.

In selected areas of particularly high-priority research, our coordination activities go beyond this across-the-board information collection and sharing. In these areas, staff from my office work closely intensively with agency R&D managers to examine in detail each agency's research activities. We then discuss how each program should be modified to ~~take each other's programs fully into account,~~ building an integrated whole that is stronger than the sum of its parts. Such an intensive coordination effort is difficult to accomplish, but ~~it is~~ very ~~valuable~~ worthwhile. To give one example, representatives from my office, the Defense Advance Research Projects Agency, and Departments of Energy and Transportation have examined in detail their respective programs in infrastructure interdependencies – analyses of how each infrastructure relies upon others for its continuous operation. These representatives are developing a single, multiagency research program that strives towards common national goals, satisfies agency mission requirements, and eliminates duplication. We have recently begun a similar effort for intrusion detection and monitoring, and we plan to commence a third intensive coordination program for incident recovery and reconstitution R&D.

Third, we validate our R&D agenda by soliciting feedback and comment from technology experts in government, the private sector, or academia. ~~Much of~~ the technical expertise in

infrastructure protection resides in academic and government laboratories, and with the private sector owners, operators, maintainers, designers, manufacturers, and customers of our infrastructure systems. Consequently, we must draw upon their expertise as we build our R&D agenda. For example, we ~~briefed~~ our program ~~more than 20 times~~ last year, the majority of which were to private sector organizations. We have asked for – and received – excellent feedback our energy sector R&D programs from the Electric Power Research Institute. My office and the President's National Security Telecommunications Advisory Committee (NSTAC) jointly sponsored a critical infrastructure protection R&D exchange meeting at Purdue University in October 1998, and we are planning a follow-on event for later this year. ~~The motivation behind~~ these outreach efforts ~~is to~~ ensure that our R&D program heads in the right direction, addresses the key technical issues, and does not reinvent technology that is already on the shelf.

The Federal Critical Infrastructure Protection R&D Agenda

The President's FY2001 budget contains $606 million for critical infrastructure protection R&D, an increase of $145 million (31%) over last year's enacted level. Reflecting the diversity of our critical infrastructures and the R&D needed to protect them, this funding is distributed among numerous agencies, as illustrated in the following table.

Agency	FY2000 ($M)	FY2001 ($M)
Department of Agriculture	0.0	9.0
Department of Commerce	9.5	63.3
Department of Energy	3.0	14.8
Environmental Protection Agency	0.0	2.0
Department of Health and Human Services	0.0	2.0
National Science Foundation	26.0	33.0
National Security	418.5	463.5

Department of Transportation	0.0	10.4
Department of Treasury	3.9	8.0
Department of Veterans Affairs	0.5	0.3
TOTAL:	**$461.4**	**$606.3**

This overall R&D program addresses four primary themes, each of which draws on the resources of multiple agencies and covers a broad spectrum of both physical and cyber security issues. The four themes are:

- Threat/Vulnerability/Risk Assessments. As its name implies, this research focuses on threat, vulnerability, and risk assessments of all critical infrastructures. The initiative also includes modeling and simulation programs, metrics, and testbeds.

- System Protection. This theme covers both physical and cyber protection of individual systems, and it includes programs such as encryption, public key infrastructures, network security products, reliability and security of computing systems, physical barriers, robust controls for power grids, and secure supervisory control and data acquisition (SCADA) systems.

- Intrusion Monitoring and Response. This theme examines technologies to detect and provide immediate responses to intrusions or infrastructure attacks. R&D programs include network intrusion detection, information assurance technologies, mobile code and agents, network alarm systems, forensic tools for electronic media, network defensive technologies, and explosives detection devices.

- Recovery and Reconstitution. This theme concentrates on those technologies required to reconstitute and restore critical infrastructures in the aftermath of disruptions. Specific research programs include risk management studies and tools, system survivability technologies, and consequence analysis tools and supporting technologies.

Although the R&D agenda includes both physical and cyber security programs, the majority of the funding - $527 million – focuses on cyber security.

In summary, we have put substantial energy, analysis, and effort into developing and coordinating an interagency R&D agenda that addresses the key technical challenges of critical infrastructure protection. The result is an integrated program package that will help us ensure the reliable and robust operation of our nation's critical infrastructures.

The Institute for Information Infrastructure Protection (I^3P)

I would now like to turn to a major new critical infrastructure protection R&D initiative that the President has requested in his FY01 budget: the Institute for Information Infrastructure Protection (I3P). This concept originated with the President's Committee of Advisors on Science and Technology (PCAST), which proposed to the President in December 1998 that the federal government establish an institute to address crucial topics in information infrastructure protection R&D. As we are all aware, information technologies are evolving at an extremely rapid rate. PCAST was concerned that the federal government's information infrastructure protection R&D might not be able to keep pace with the explosive rate of technological change. The Committee believed that an independent, not-for-profit Institute, suitably designed, could act

flexibly and responsively enough to stay abreast of emerging information infrastructure threats and vulnerabilities. The PCAST concept incorporated three primary criteria for the Institute:

- The Institute must work in collaboration with the private sector manufacturers, owners, operators, and users of the information infrastructure to identify the most important research needs.

- The Institute must engage the nation's top technical talent in the nation to address these needs, whether that talent resides in industry, academia, government laboratories, or other research facilities.

- The Institute must operate flexibly enough to keep pace with the rapid evolution of information technologies.

In studying the PCAST proposal, the Administration analyzed whether such an Institute was needed; whether that need could be satisfied by existing facilities, either internal or external to the government; and whether the private sector supported such an Institute's establishment. The Administration commissioned the Institute for Defense Analyses (IDA) to review the concept in depth and to consult extensively with the private sector and academia. IDA's review demonstrated broad private sector support for the concept. In addition, OSTP and PCAST jointly hosted a meeting of Chief Technology Officers (CTOs) of 15 of the nation's leading information technology corporations last October. The CTOs, too, indicated that such an Institute is clearly needed.

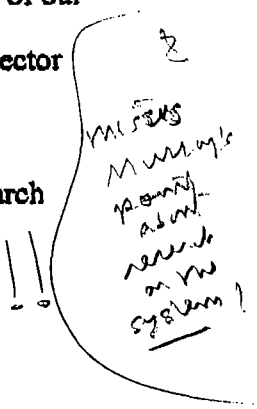
As the culmination of the Administration's review, the President announced on January 7 that he would request $50 million in his Fiscal Year 2001 budget for an Institute for Information Infrastructure Protection (I^3P). He has also requested $4 million in a supplemental appropriation for the current Fiscal Year to establish the Institute and get started on its first R&D projects. He stated that the I^3P "will fill research gaps that neither public nor private sectors are filling today," and that it will "bring to bear the finest computer scientists and engineers from the private sector, from universities, and from other research facilities to find ways to close these gaps." This Institute will be funded through the Commerce Department's National Institute of Standards and Technology (NIST), which has the mission of working with the industry to develop technology, measurements, and standards to strengthen our economy and improve our quality of life. NIST also has specific responsibility for developing standards and guidelines to assist Federal agencies in the protection of sensitive unclassified information systems. Together, these responsibilities uniquely qualify NIST to support the Institute, which must work closely with both industry and federal agencies.

Given the close and continuing relationships that this Institute must maintain with the private sector and academia, these sectors must be involved in its planning. I have therefore asked PCAST, working with additional experts in the private sector and academia, to conduct a short-term, rapid-turnaround study to advise me on the Institute's organizational structure, operational activities, staff recruitment/retention, and initial R&D priorities. PCAST sponsored a meeting with private sector and academic technology leaders on February 18 to commence the detailed

clean up

design of a recommended concept of operations and R&D agenda. Thanks to PCAST's leadership, we received the first detailed design papers on February 25.

To date, the participants in this effort have identified "gap-filling" R&D as the Institute's primary function. While the private sector clearly has a substantial information security R&D effort under way, there are important technologies that are unlikely to attract private investment: those that are too long-term, too risky, or too likely to benefit a large number of "bystander" firms who did not fund or conduct the original research. At the same time, federal agencies have traditionally supported research directly related to their mission needs, without necessarily addressing areas that are important to securing the national information infrastructure as a whole. The result is a gap between federal and private sector research – a gap that the government, private sector, and academic technology experts agree must be filled to ensure the security of our information infrastructures. This Institute, working closely with the government, private sector and academia, will identify and close these research gaps. As I noted previously, we are currently working intensively with the technology experts to identify the initial set of research projects.



Summary

Ensuring the robust, reliable, and assured operation of our critical infrastructures presents a serious challenge. Advanced technology will help us meet this challenge -- and for this reason, the Administration has developed a comprehensive critical infrastructure protection R&D agenda that is coordinated across many agencies. Each program in the agenda is tied directly to infrastructure vulnerabilities and addresses infrastructure protection R&D shortfalls. An

important new initiative in the FY2001 agenda is the Institute for Information Infrastructure Protection, which will enable our nation to protect its information infrastructure even as information technologies are rapidly evolving.

Mr. Chairman, the President directed that critical infrastructure protection be a national priority in PDD-63. We have developed a robust R&D program that will ensure our infrastructures continue to operate reliably even in the face of new threats in the 21st century.

Meet with Mark Montgomery:

- Are we looking at salary issues
- Centers of Excellence in 7 Jan fact sheet? What are these?
- Get list from Tony on who is on the Committee.
- GPRA - need to look at this? Q & A on this?
  - Include data on documentation for the subgroups - what we write each year.