

EXECUTIVE OFFICE OF THE PRESIDENT
PRESIDENT'S COMMITTEE OF ADVISORS ON SCIENCE AND TECHNOLOGY
WASHINGTON, D.C. 20502

December 10, 1998

President William J. Clinton
The White House
1600 Pennsylvania Avenue
Washington, D.C. 20500

Dear Mr. President:

You have made the protection of critical infrastructure a high priority, especially our interconnected electronic network which underpins our nation's monetary, national security, air traffic control, telecommunications, law enforcement, energy distribution and other such critical systems. Achieving this goal will require gaining a systematic understanding of information infrastructure vulnerabilities and developing and deploying new technology, equipment, software and procedures. We recommend the government establish and contract with a new not-for-profit laboratory, the Laboratory for National Information Infrastructure Protection (LNIIP), to create and disseminate the necessary knowledge to protect our information infrastructure. This technical organization in the private sector but with certain government oversight will complement the operational capability of the Department of Justice National Infrastructure Protection Center, created by PDD-63.

The new LNIIP should be governed by an interdependent board of directors drawn from leaders of the telecommunications, software and information technology industries and their customers, as well as from academia. The purpose of the Laboratory would be to conduct research and develop technology that would protect our critical information and communications systems from penetration and damage by hostile foreign national or subnational groups, organized crime, determined hackers, and from natural instabilities, internal design weaknesses or human failings that can cause major disruption of highly complex, nonlinear networks. This effort would include the development of a broad understanding of the robustness and resilience of such complex systems and would involve creation of means to assure graceful degradation under stress.

Information infrastructure issues affect the operations of virtually all elements of the private sector and the government. At present there is no technical organization dedicated to developing the knowledge and common technology base required to successfully address this problem and provide the basis for long term protection. The private sector does not have the incentive to develop the public knowledge and technology base required for the development of competing interoperable proprietary systems--thus federal support is needed. The justification for acquiring the needed knowledge and technology through government support of a new not-for-profit laboratory is that while most of the critical infrastructure lies outside the government, only the government is in a position to derive and make broadly available the information needed to assure the integrity of our nation's information network. Because of the complex relationships,

Pcast Letter on Critical Infrastructure Protection
December 1998

tight coupling between the government, information infrastructure providers and users is critical to the structure proposed to accomplish this coupling, as shown in the attached diagram.

Areas of LNIIP's technical program would include: (1) vulnerability detection and analysis; (2) security architectures and simulation systems; (3) encryption and authentication systems; (4) intrusion detection and warning systems; (5) system recovery; (6) component and software security assurance; (7) best practices for product evaluation; (8) training, and (9) human interface with complex systems. The Laboratory would also provide a linkage between government and industry and draw upon talent in academia for the purposes of: (a) serving as a clearinghouse for industry information and experience (with procedures that respect proprietary data); (b) setting and disseminating best practice information; and (c) carrying out training exercises and inspections to certify performance. The LNIIP would be concerned with creating knowledge, technology and tools; it would not be concerned with operations. We also believe that it is too ambitious to include in the baseline LNIIP charter other critical infrastructure vulnerabilities, i.e., vulnerability to terrorist chemical or biological attack, although these related considerations would necessarily play some role in the LNIIP technical program.

The LNIIP would focus on developing techniques for protection of the information infrastructure backbone; it would have the responsibility to interact with key functional areas both in government (notably defense, law enforcement, treasury, energy, transportation, and emergency services) and in the private sector (telecommunications, banking, power, airlines, manufacturing, et al). Thus, the functional industry groups and corresponding government agencies are the "clients" for the LNIIP product and must have a role in shaping the LNIIP work program.

How should the federal government accomplish coordination and oversight of the LNIIP program it sponsors while assuring that the needed close coupling with the private sector is maintained? We believe a federal council composed of those agencies that have an important interest in the information infrastructure problem is required. A federal coordinating committee acting on behalf of the council and composed of the Deputy Secretaries of Defense and Commerce and the Deputy Attorney General should provide effective management and oversight responsibility. We recommend that the Deputy Secretary of Defense chair the federal coordinating committee, although a rotating chair is an alternative.

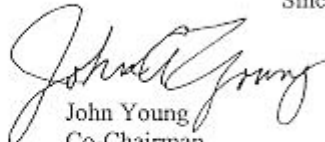
We urge that funding for the LNIIP be placed in a budget line in the Executive Office of the President under the control of OMB and the federal coordinating committee. We recognize that this is an unusual approach; however, we believe that it is justified because circumstances dictate that government security and law enforcement set requirements for what ultimately will be the private sector's responsibility to implement its own information protection programs. A second choice might be to assign budgetary responsibility to the DOD in deference to its size, responsibility and R&D management experience. But such an assignment will cause concern both in the public and industry that DOD will wield undue influence in determining the type and degree of protection which is warranted and this approach is therefore not recommended.

Without a specific work plan it is difficult to set a budget for the LNIIP with precision. However, we believe that about \$100 million per year would not be unreasonable after a start-up

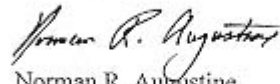
period. This money would come primarily from the federal government, although we anticipate that significant funds and in-kind support would also come from industry. Several independent groups have proposed the creation of a new information assurance technical organization such as we are recommending here. We have endorsed this step because we believe it is the quickest and most efficient way to develop and deploy information assurance technology. In particular, we believe it is preferable to allocating to agencies, through the critical infrastructure protection (CIP) process, all available funding for information infrastructure protection. There is a need for a centrally focused effort in the private sector to develop the needed technology as quickly as possible.

If you approve, OMB and OSTP will form a small working group from DOD, DOJ, and DOC, with inputs from others, to prepare a specific proposal for your consideration for inclusion in the FY2000 budget. The PCAST Security Panel will be available to advise this working group should that be desired.

Sincerely,



John Young
Co-Chairman
PCAST



Norman R. Augustine
Chairman
Security Panel

Attachments: Proposed LNIIP Flowchart

Office of Science and Technology Policy

1600 Pennsylvania Ave, N.W
Washington, DC 20502
202.395.7347