National Infrastructure Advisory Council

April 13, 2004

The Honorable George W. Bush
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC

Dear Mr. President:

We are pleased to submit the final report and recommendations of the National Infrastructure Advisory Council's (NIAC) study regarding best practices for considering any government intervention to enhance the security of national critical infrastructures. The NIAC would like to credit and thank Ms. Karen Katen, President, Pfizer Global Pharmaceuticals, for her leadership in this study, all the members of the study group and external reviewers for their dedicated efforts.

The interdependence of physical infrastructure and cyber security has become evident through the events of recent years. Public and private sector organizations are adapting rapidly to this new environment. Considerable investment is being made in security. More needs to be done. A key question for the NIAC has been: "What issues should the government analyze before considering any intervention into the market to address security?"

The report outlines a framework for the government and others to use as a guide, and does not recommend intervention by the government into any sector. Each sector is different. Before considering any intervention into the market, more information is needed about the characterization of the potential harm, the role the market is playing in the sector, and the intended and unintended consequences of any intervention. This report provides a useful framework for addressing and analyzing these issues. For example, the report finds government intervention in the information technology sector may blunt innovation, resulting in less consumer choice, economy, and security, and there is currently no case for government intervention in this market.

The Council believes the eight-factor framework provided in this report, and the seven best practices for discussing the issue with industry, will be useful to federal, state, and local agencies who support and oversee the safety and security of the nation's critical infrastructures. We recommend this report be shared with them for their information and consideration.

1401 Constitution Avenue NW Washington, D.C. 20230
Suite 6095 202.482.1929

Mr. President, on behalf of our fellow NIAC members, we thank you for the opportunity to serve our country through participation in this Council.

Sincerely,

Erle A. Nye
Chairman of the Board
TXU Corporation
Chairman, NIAC

John T. Chambers
President & CEO
Cisco Systems, Inc.
Vice Chairman, NIAC

Attachment: Summary of Report – Best Practices for Government Intervention to Enhance Security of National Critical Infrastructures: Final Report and Recommendation by the Council April 13, 2004.

cc: Vice President Dick Cheney
The Honorable Thomas Ridge, Secretary of the Department of Homeland Security

Introduction. The goal of this report is to address what issues the government should analyze before considering any intervention into the market place regarding security. Recognizing the need to improve security and mitigate risks and vulnerabilities in each critical infrastructure sector, the report lays out a framework for analyzing the security profile in critical infrastructure sectors.

Conclusions. With the insight and assistance of participants from the chemical, financial services, information technology, and water sectors, the NIAC found that public and private sector organizations are responding within their own institutions and across industry and sector boundaries, driven by the need to secure their own operations and protect business relations with customers and partners**.** Where market forces are free to operate, they will be the most efficient and efficacious vehicle to enhance the security posture of critical infrastructures. If market forces are unable to operate quickly and efficiently in a sector, government should consider timely intervention, but only with a good characterization of the potential harm that could occur from an attack, and a sound understanding of the role market forces play in promoting an improved security posture across a sector.

Analytical Framework and Best Practices

- A common framework can be used to analyze the issue
    - The report finds that considering these eight factors can lead to insights into sector dynamics and the possible effects of intervention:
        1. Are there network interdependencies,
        2. Do security concerns drive customers to change providers,
        3. Is voluntary sector activity already occurring,
        4. Can the sector exert peer pressure,
        5. Do attacks occur frequently,
        6. Could the attack cause catastrophic injury or economic damage,
        7. Is the industry profitability high enough to invest in security,
        8. Is there sufficient expertise to execute a plan?

- Identified best practices
    - When interacting with industry, the report identifies seven best practices:
        1. Develop plans in concert with industry,
        2. Mandate outcomes rather than specific actions,
        3. Ensure alignment between federal, state, and local regulations,
        4. Evaluate all new and existing rules through a “security filter”,
        5. Incorporate flexibility or sunset provisions,
        6. Funding may be necessary to fulfill government mandates,
        7. Implement interventions in phases.