National Infrastructure Advisory Council

February 18, 2005

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 (NIAC) study regarding the Prioritization of Cyber Vulnerabilities. The NIAC would like to credit and thank Mr. Martin McGuinn, Chairman and Chief Executive Officer of Mellon Financial Corporation, for his leadership in this study. The Council would also like to thank the members of the study group and external reviewers for their dedicated efforts.

A report was reviewed with the NIAC at the October 12, 2004, meeting at which the following key findings were reviewed:

- Dependency on network-based systems is pervasive across all sectors. Critical components of our national infrastructure rely on a variety of network-based systems.

- The answer to the question "are we ranking our critical infrastructures as to their vulnerability to cyber attacks?" is multi-faceted. The degree that any sector is vulnerable to a cyber attack is dependent upon a number of characteristics, such as type of attack, scope, blended attacks, time and duration.

- Sound business continuity practices, as well as information technology and cyber security best practices, provide some protection.

Based on these findings, the following seven recommendations were approved by the Council:

1. Direct lead agencies to work with each of the critical sectors to more closely examine the risks and vulnerabilities of providing critical services over network-based systems.

2. Direct DHS and the lead agencies to identify potential failure points across Federal Government systems. Encourage the private sector to perform similar cross-sector analysis in collaboration with DHS, as long as DHS can assure protection of sensitive results.

3. Encourage sector and cross-sector coordinating groups (councils) to establish and/or support existing cyber-security best practices or standards for their sectors.

4. Direct DHS to sponsor cross-sector activities to promote a better understanding of the cross-sector vulnerability impacts of a cyber attack.

5. Direct Federal agencies to include cyber attack scenarios and protective measures in their disaster recovery planning. Encourage sector coordinating groups to include cyber attack scenarios and protective measures in their disaster recovery planning.

6. Encourage law enforcement organizations to prosecute cyber criminals and to widely publicize efforts to do so.

7. Promote awareness of cyber security best practices at the corporate, government, small business, university, and individual levels.

Implementation of the above recommendations will help to promote a better understanding of the risks of cyber attacks across the critical infrastructures, and facilitate appropriate recovery and response planning. Such efforts are critical, given the large and growing dependency on network-based systems that is pervasive across the Nation's critical infrastructures.

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

Attachments: Final Report and Recommendation by the Council October 12, 2004.

cc: Frances Fragos Townsend, Special Assistant to the President for Critical Infrastructure Protection, Homeland Security Advisor
The Honorable Michael Chertoff, Secretary, Department of Homeland Security