National Infrastructure Advisory Council

August 21, 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 (NIAC) study regarding Evaluation and Enhancement of Information Sharing and Analysis. The NIAC would like to credit and thank Mr. Thomas E. Noonan, Chairman, President & CEO, Internet Security Systems, Inc., for his leadership in this study, as well as the members of the study group and external reviewers for their dedicated efforts.

Securing the homeland requires seamless coordination of the complex, interrelated efforts of state, local, and federal governments with the private sector. The private sector owns or operates 85 percent of the nation's critical infrastructure and is responsible for the overwhelming majority of cyber security research and development. Substantial improvement to the security of our critical infrastructures relies on effective information sharing. In this regard, the Council notes that it is equally important for the private sector and the federal government to supply and support each other with timely information and analyses.

This report analyzes the current environment for information sharing and analysis across the critical infrastructure sectors and makes recommendations that, if implemented, should enhance the flow of information within and between sectors and should increase the effectiveness of information sharing and analysis. To reach these recommendations, the NIAC explored four areas: business models for sharing and analyzing information; financial models for supporting information sharing processes; level of information analysis and aggregation; and information dissemination breadth and coverage.

The report outlines a framework for action, but does not recommend government intervention into any sector. Because each sector is different, there is no one-size-fits-all solution. However, each critical infrastructure sector has affirmed its requirement for a sector-specific Information Sharing and Analysis Center (ISAC) operation that is independent from the government. The report recommends that the government recognize and endorse the industry ISACs. This is an exceptional opportunity, since the private sector has the ability to provide unique, timely analysis and to determine what measures will best protect the infrastructure while continuing to provide essential services. In this regard, the private sector should be viewed as a full partner with the Federal Government.

The Council notes that privately funded ISACs are at varying levels of maturity. While many factors affect this maturity, the Council believes that government can favorably improve the effectiveness of ISACs by including them fully in government intelligence processes and by

providing focused financial support for key projects, like secure communications. Such actions in support of the ISACs will provide a means for a more productive partnership between private industry and the government.

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 – Evaluation and Enhancement of the Information Sharing and Analysis: Final Report and Recommendation by the Council July 13, 2004.

cc: Vice President Dick Cheney
Ms. Frances Fragos Townsend, Assistant to the President and Homeland Security Advisor, Homeland Security Council
The Honorable Thomas Ridge, Secretary of the Department of Homeland Security

SUMMARY OF REPORT – EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS, JULY 13, 2004.

Introduction – The goal of this report is to address the environment for sharing information in the private sector critical infrastructures with the government and between the sectors and to make recommendations to the government for enhancing information-sharing effectiveness while increasing the broad influence across the sectors. The Council would like to highlight the following two issues.

Issue # 1 – Cooperation between the Public and Private Sectors: The current business models for most ISACs have drawbacks regarding continuous flow of analysis and information to the members. The costs associated with start-up of operations and continuing secure operations are nearly insurmountable.

Recommendation:

The Federal Government should encourage ISACs to create tiered membership structures. This will assist ISACs in delivering basic alerts and advisories through them and provide the ability to scale dissemination throughout their sectors. These combined actions would increase 1) the volume of alerts and advisories for public use and consumption, and 2) the dissemination of the alerts and advisories that have cross-sector impact or interdependencies. For example, it would allow for passing of an alert to the Financial Services sector, while also passing the same alert to the Information Technology and Telecommunications sectors regarding cyber or connectivity issues facing the Financial Services.

Secure Communications: As the ISACs continue to mature their operations, work with DHS, and more importantly, among themselves, they are becoming greater targets for surveillance from adversaries. Assisting the private sector ISACs with procuring a commercial-grade secure telephone/conference system would be of great value in opening the channels of communication and coordination within industry. This increased coordination and communication will help industry secure the infrastructures. . This increased coordination is important not just in times of incidents and events, but also during routine operations when trust is gained and developed. Protection of industry communications and coordination during pre-attack activities such as network reconnaissance would block an adversary's ability to discern points of vulnerability, thereby limiting their target intelligence of our infrastructures.

Issue # 2 – Private Sector Capabilities: The Federal Government does not adequately understand the private sector's unique research and analytical capabilities and its desire to maintain its separate capability.

Recommendation:

Full integration: Private industry must be fully integrated into the Federal Government's Intelligence Cycle, which consists of determining information requirements, tasking, analysis, reporting, and dissemination. Private-sector information requirements must be included and integrated within the cycle. Also, private-sector analytical capabilities must be integrated into the private sector/government information sharing and analysis efforts to develop the most thorough and useful intelligence products possible in order to most effectively protect critical infrastructures.

Private industry has the ability to gather and analyze information about its systems and infrastructure. This is real-time business and infrastructure intelligence, based on current on-going operations and development/upgrading of operations. The Federal Government must learn to include industry experts as domestic intelligence assets, integral to improving infrastructure protection, and not just occasional customers of government intelligence products.

Two-Tier Information Dissemination: The Council recommends that a two-tier information dissemination mode be established for the private sector. This includes the incorporation of private-sector analysis and focus into the government's base message and outreach for communicating differentiated alerts.

- **General alerts and information (Reach)**. This is the first tier of information and dissemination. All non-aligned (to an ISAC) business and critical infrastructure ISACs would receive this information. It provides the early warning for alerts and notifications of incidents and potential attacks from newly announced vulnerabilities or exploits.

- **Sector-specific alerts and analysis (Analytical)**. This level of analysis is iterative and studies process interdependencies or weaknesses within and across systems. Those ISACs with the capability to do so would perform additional analysis and communicate issues across sectors and with the government to protect critical infrastructures. ISACs would deliver specific finished product analyses based on known information and intelligence requirements to their industry sectors.

Key Report Conclusion: Private sector information gathering and analysis capabilities and alert dissemination capabilities are substantial and are focused through the ISACs. The Federal Government should develop better means to work in a two-way fashion with these capabilities. ISAC capabilities could be improved (1) through Government support to procure a commercial-grade secure telephone/conference system and (2) by encouraging tiered structures for industry participants.