

National Infrastructure Advisory Council

June 23, 2008

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 National Infrastructure Advisory Council's (NIAC) Final Report and Recommendations on the Insider Threat to Critical Infrastructures. The NIAC would like to thank Study co-chairs Mr. Edmund G. Archuleta, President and CEO of El Paso Water Utilities, and Mr. Thomas E. Noonan, Former General Manager of IBM Internet Security Systems. The NIAC also would like to thank other NIAC Members who participated and numerous subject matter experts for their services to the study.

The NIAC initiated the study in response to a request that Homeland Security Secretary Michael Chertoff outlined in a letter to the NIAC on January 16, 2007. Secretary Chertoff asked the NIAC to study the insider threat in the context of critical infrastructure protection, and outlined seven key tasks:

1. Defining the "insider threat" both physical and cyber; and also examining the potential economic consequences.
2. Analyzing the dynamics and scope of the insider threat, and critical infrastructure vulnerabilities.
3. Defining the obstacles to addressing the insider threat.
4. Analyzing the potential impact of globalization on the critical infrastructure marketplace.
5. Identifying issues, potential problems, and consequences associated with screening employees.
6. Identifying legal, policy, and procedural aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators.
7. Developing policy recommendations on potential remedies, up to, and including, possible legislation.

The Report addresses each of these assigned tasks and includes recommendations to address policy and legal gaps that were identified as a result.

Mailstop 8500 245 Murray Lane, SW
Washington, DC 20528-8500

The insider threat to critical infrastructures constitutes a real and significant threat because of the potential a trusted insider has to inflict serious damage, including cascading and cross-sector effects and economic interruptions from critical infrastructure service losses. While many critical infrastructure operators have programs or measures in place addressing this threat to some degree, others do not fully understand or appreciate the threat posed by insiders, both to their company and also to our Nation.

The Report provides recommendations for government policy to help improve the security posture of U.S. critical infrastructures against this threat. The recommendations include low-cost, easily implemented policy solutions for near term effect. The NIAC recommends that policy makers move swiftly to implement the near term improvements and increase the security of our critical infrastructures.

The NIAC also found poorly understood, complex, and rapidly evolving challenges, and outlines steps forward for future research by properly resourced groups and organizations.

The Council respectfully submits the following recommendations to improve insider threat risk mitigation:

- **Executive leadership awareness.** Recommendations and a framework approach for improving executive leadership awareness of the insider threat to critical infrastructures. The recommendations include a request for White House leadership on executive awareness to coordinate government efforts and engage with critical infrastructure executive leadership on this important issue.
- **Employee screening and risk assessments.** Detailed findings and recommendations to improve critical infrastructure operator employee screening and risk assessments. The NIAC's recommendations concur with the recommendation in the 2006 Attorney General's Report on Criminal History Background Checks to expand private sector use of Federal criminal history sheet records, while preserving existing privacy protections that flow from the Fair Credit Reporting Act for most current private-sector background checks.
- **Role for DHS and Sector Coordinating Councils.** The Department of Homeland Security and the Sector Coordinating Councils (SCCs) should support critical infrastructure operators in developing insider threat risk assessments, insider threat policies, and risk mitigations.

The Honorable George W. Bush
June 23, 2008
Page 3

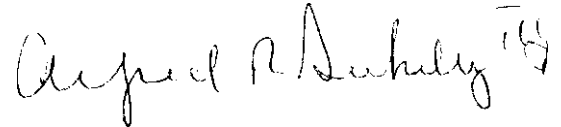
- **Technology policy.** Recommendations for improved technology policy to help critical infrastructure operators address the emerging Information Technology (IT) dynamic to the insider threat.
- **Information sharing.** Recommendations to improve insider threat risk assessments through information sharing, both among owners and operators in each sector and also with government on research and intelligence.
- **Future research.** NIAC identified key focus areas for future research on challenges presented by globalization, technology threats and solutions, and personnel risk assessments, where time, resources, and a current understanding of the insider threat limited specific policy recommendations.

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 Nye
Chairman Emeritus
TXU Corp.
Chairman, NIAC



Alfred R. Berkeley, III
Chairman and CEO
Pipeline Trading Systems, LLC.
Vice Chairman, NIAC

cc The Honorable Richard Cheney, Vice President
The Honorable Michael Chertoff, Secretary, Homeland Security