



To: Assistant Secretary Robert Stephan, DHS
John Sabo, Chairman, ISAC Council

From: Partnership for Critical Infrastructure Security

Re: PCIS Information Sharing Governing Principles

Date: September 25, 2006

The Partnership for Critical Infrastructure Security (PCIS) has established governing principles for information sharing, between and among the critical infrastructure sectors and with government. These governing principles provide a policy-level framework for describing the need to share information through secure and effective collection, analysis, and dissemination processes. These governing principles are intended to guide private-sector representatives building or strengthening cross-sector information-sharing capabilities.

Information Sharing Defined

In the context of critical infrastructure and key resources (CI/KR) as described in DHS' National Infrastructure Protection Plan, information is defined as information related to security incidents, threats, vulnerabilities, lessons learned, best practices, and protective measures. To the extent possible, this information shall be provided in a context that will prompt recipients to take appropriate action. There are multiple types of information that can be shared between and among sectors and with Federal, State, and local governments. Such types of information may include incident reports, operational activities, security plans, and other activities and data shared for awareness or action. This information may be time-sensitive for immediate action/response or it may allow for a longer suspense (a week, a month, etc.). The CI/KR sectors and the government will clarify specific types of information that is routinely shared and work to develop a protocol to improve dissemination.

Governing principles for information sharing are provided below, along with some illustrative activities that could support implementation. These principles serve as a reference for sectors with Information Sharing and Analysis Centers (ISACs), but are also applicable to sectors that have or are developing alternate information-sharing mechanisms.

PCIS established these governing principals for information sharing in its role as the private-sector cross-sector council. PCIS supports interactions among the Sector Coordinating Councils (SCCs) to address policy and strategy issues common to most or all of the SCCs, both with respect to interactions with the government and also among the

sectors. The ISACs or other information-sharing mechanisms are typically the tactical and operational arms of the sector's information sharing and analysis efforts. In that regard, these groups will be responsible for operational issues addressing information sharing and will use this policy with respect to how information sharing will be implemented.

These governing principles will be reviewed periodically. As the sectors face emergent issues, information-sharing capabilities will be tested and these principles can be refined in the context of the entire preparedness and response cycle. PCIS values the public-private partnership and trusts that DHS and the ISAC Council will find these governing principles helpful. We welcome feedback from the government as well as from the operational centers of the private sector.

Sincerely,

A handwritten signature in black ink that reads "Stuart Brindley". The signature is written in a cursive style with a large, sweeping initial "S".

Stuart Brindley
Chairman, Partnership for Critical Infrastructure Security

cc: Partnership for Critical Infrastructure Security Members