

ISAC Analytical Efforts

ISAC Council

White Paper

January 31, 2004

1. Introduction.

The ISACs are primarily organized by and focused on individual critical infrastructure sectors. Individual ISACs support their infrastructure and members with various levels of capabilities. Many are simply information conduits, some are oriented primarily to the cyber threat, and their analytical capabilities are varied as well.

2. Discussion - ISAC Analytical Capabilities.

Each ISAC will define for itself now and in the future its analytical requirements and capabilities. The ISACs provide, however, a basis for individual sector and cross-sector analysis that can be of great value to private industry and the Government as well.

In this regard, the ISAC Council makes the following recommendations:

- A. The current and planned analytical capabilities of the various ISACs be understood as a baseline for further inter-ISAC coordination and interaction. The analytical strengths of the ISACs should be recognized and provide for a synergistic basis for further inter-ISAC cooperation.
- B. Cross-sector/interdependency analysis be considered by the individual ISACs for further joint efforts. This cooperation will initially be based on the primary interdependencies of the various sectors and the maturation of the individual ISACs' capabilities.
- C. Government sponsorship and support of these analysis efforts must be considered and encouraged. A model that integrates private industry into the government intelligence cycle should be adopted.
- D. ISAC analysis should consider both physical and cyber, and should address immediate, mid, and long-term information/intelligence requirements.
- E. A capable and secure communications means should be established for the cross sector analytical efforts. CWIN should be considered to fill this role. Additional functionality may be required if CWIN is to be the communications backbone.
- F. Inter-ISAC analysis efforts should be pursued by the individual ISACs represented in the ISAC council.

- G. A second ISAC Summit, similar to the White House Summit, should be pursued by the Council once sufficient common issues are agreed to by the Council. This summit would be primarily sponsored by DHS as the Government proponent of the ISAC community. The overall subject of analysis could be one of the common issues to discuss among the ISACs and between the ISACs and the Government.

Information Sharing and Analysis Centers, or ISACS, are private sector operational organizations which today are collecting, distributing, analyzing and sharing sensitive information regarding threats, vulnerabilities, alerts and best practices in order to protect our national critical infrastructures.

Eleven ISACs -- Chemical, Electricity, Energy, Financial Services, Healthcare, Information Technology, Public Transit, Surface Transportation, Telecommunications, Truck, and Water -- have joined together as an ISAC Council, partnering with their sectors, with one another, and with government to advance the physical and cyber security of the critical infrastructures of North America.

Please note that this paper was written by the ISAC Council as a consensus document, with input and review by member ISACs. However, its views and findings do not necessarily represent the official position of each ISAC. For more information on the ISAC Council and the ISACs which form its membership, please visit www.isaccouncil.org.