

GOVERNMENT – PRIVATE SECTOR RELATIONS

ISAC Council
White Paper
January 31, 2004

Overview

The ISAC Council sees the need for a set of requisite understandings between the Department of Homeland Security (DHS) and the private sectors that are currently represented by the ISAC Council. Refer also to the related white paper, “Presidential Decision Directive-63; Current Gaps”.

Some of the issues included are more important than others and some must, of necessity, be on a fast track for resolution. Clearly everything stated herein is presented for debate with the goal being a clearly stated set of responsibilities for the Government agencies and private sectors. Once these are established, then action plans with business cases, proposed funding, and schedules can be aggressively prepared.

The ISAC Council believes that a strong government – private partnership is necessary for the continued protection of the critical infrastructures. Close relations between the private sectors and the Department of Homeland Security and between each sector and its Lead Agency are vital.

Summary

The ISAC Council is currently coordinating among eleven ISAC members. The areas of interest shared by the ISACs include:

1. Coordination and communication between the government and sectors.
2. Coordination and communication between the ISACs.
3. Incident data sharing.
4. Analytical information sharing.
5. Communications including mechanics and protocols.
6. Physical and cyber interdependencies between sectors.
7. Research and development requirements.

Issues

1. Clarify roles:
 - A. Department of Homeland Security (DHS). Establish the goals of the directorates and their relationships with the private sectors.
 - B. Other Federal Agencies.
 - C. State Agencies.
 - D. Sector Lead Agencies for Sector Liaison.
 - E. Sector Coordinators:

- a. Policy
 - b. Security planning
 - c. Operations oversight.
 - F. Information Sharing and Analysis Centers (ISAC).
 - a. Security operations.
 - G. National Infrastructure Assurance Council.
 - H. National Security Telecommunications Advisory Committee.
 - I. ISAC Council.
2. What is the interface between the DHS and the ISACs?
 - A. Organization
 - B. Mechanics to assure timely and reliable communications:
 - a. Telecommunications mechanics including out of band and secure communications.
 - b. Data / information sharing protocols.
 - c. Security clearances for sector personnel.
 - d. Routine cleared security briefings.
 3. Establish means to secure data/information that is provided to the governments. This assurance is necessary for national security and business proprietary reasons. What can the Government do to reduce the risk of disclosure of industry critical infrastructure information by States?
 4. Is there a sector situational role to be actualized by ISACs? This envisions dealing with crisis or severely abnormal conditions due to a variety of causation.
 5. Define clearly (with realization that this will be a dynamic area) the data/information requirements of the Government from the Sectors and the Sectors' requirements from the Government.
 6. Financial and resource support for the ISACs.
 7. For some Sectors the reach is cross border with Canada; this must be addressed with consideration to cross border reach between DHS and related Canadian agencies.
 8. Seek to assure sufficient understanding by the Government of the Sector operations to facilitate decision-making.
 9. Discuss the Homeland Security Advisory System and its applicability to the sectors. Develop means to utilize intelligence information to tailor threat alert levels on a geographical, sector, specific facility basis.
 10. Review the work done by the Government and Sectors regarding interdependencies between sectors. Plan for quantitative modeling issues that may emerge from short term analysis or that must, due to current circumstances, be on a longer term track.
 11. Consider a critical assets vulnerability database to assist in threat evaluation. Any such database should be capable of handling assessment data developed from a variety of programs and must be highly secure at the appropriate location.

12. Determine needs for spare equipment to support the critical infrastructures and the means for the spares acquisition, storage, and transportation when required.
13. Coordinate R&D projects among Government and the Sectors.

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.