

Reach of the Major ISACs

ISAC Council

White Paper

January 31, 2004

Introduction

The ISAC Council comprises eleven Information Sharing and Analysis Centers (ISAC). Each of the ISACs came together in the spring of 2003 to work on common operational themes and issues for exchanging information internally and externally.

The ISACs are a concept that was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998. PDD-63 recognized the potential for the infrastructures of the United States to be attacked either through physical or cyber means with the intent to affect the military or economic power of the country. For each major infrastructure within the US economy, the Federal Government assigned an Agency or Department to work with the Private Sector to “consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the National Infrastructure Protection Center (NIPC) will be determined by the private sector, in consultation with and with assistance from the Federal Government.”

PDD-63 was supplemented and partially superseded by Homeland Security Presidential Directive /HSPD-7 (Dec. 17, 2003), which revised the list of lead agencies for critical infrastructure sectors and provided that those agencies, and the Department of Homeland Security (DHS), would “continue to support sector-coordinating mechanisms . . . to facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.”

Each sector’s responsible lead agency from the Federal Government has encouraged the sector to initiate the formation of its ISAC to better inform its members, to communicate with other sectors and, when feasible, to communicate and coordinate with the Federal Government.

In this paper we have not tried to describe the sectors, but rather the degree of penetration or reach into the US economy / infrastructure that each of the ISAC has individually and collectively.¹ Further, we have refrained from discussing the financial and/or business models, in so far as they differ at this point.

¹ Data as of September 2003.

This information paper is designed to assist everyone, especially in DHS, in understanding the current value of the ISACs to reach into approximately 65% of the infrastructures of the United States economy held in private hands. The potential goal for the ISAC communities, as they mature, is to reach nearly 95% of those U.S. private infrastructures.

1. The Reach of the Chemical ISAC – Chemical ISAC

The Chemical Sector ISAC was established in April 2002 by the American Chemistry Council, and is operated through CHEMTREC, the chemical industry's 24-hour chemical emergency communications center, which permits immediate dissemination of alerts and information. Participants in the Chemical Sector ISAC are drawn from the member companies of the major chemical industry associations, including the American Chemistry Council (ACC), Chlorine Institute, National Association of Chemical Distributors, Dangerous Goods Advisory Council, Synthetic Organic Chemical Manufacturers Association (SOCMA), National Paint and Coatings Association, the Fertilizer Institute, Adhesive and Sealant Council, and others. The CS ISAC also includes member companies of the 22 state chemical industry councils (state chemical associations).

In addition to chemical producers, through the members of the ACC/SOCMA Responsible Care Partner program, value chain companies involved in transportation, warehousing and distribution of chemicals are also included. The Chemical Sector ISAC provides both physical and cyber related alerts and information and is primarily focused on US based operations. The CS ISAC works closely with other ISACs that are involved in the transportation and distribution (land and water) of chemical products or that have collateral/co-located operations (oil and gas refining, etc.).

2. The Reach of the Electricity Sector ISAC - ESISAC®

The Reach of the Electricity Sector ISAC - ESISAC®

The ESISAC was approved by the North American Electric Reliability Council (NERC) Board of Trustees and became operational October 2000. NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate and secure (physical and cyber). NERC maintains strong working relationships with American Public Power Association, Canadian Electricity Association, Edison Electric Institute, National Rural Electric Cooperative Association.

The ESISAC coverage whether direct to a given entity or/and via the eighteen Reliability Coordinators who cover the entire continental United States and Canada on a 24x7 basis is virtually 100%. There are thousands of entities that comprise the ES. These range in size from those serving major metropolitan areas and virtually entire provinces and states and those providing major generation resources, to those serving very small (yet still critical) communities or rural areas, and those operating perhaps a single generator.

The ESISAC maintains liaison with the US Nuclear Regulatory Commission (NRC).

3. The Reach of the Energy ISAC – Energy ISAC (Primarily Oil and Gas)

The Energy ISAC officially became operational on January 1, 2002. The Energy ISAC went to a corporate membership of 35 companies by mid-year, but it became clear that the hundreds of small to mid-sized companies within the sector needed to be included in the ISAC.

As a result, in the fall of 2002, the Energy ISAC requested the DOE Office of Energy Assurance to fund the ISAC to permit the ISAC to have 4000 member companies. The money from DOE was received about 90 days ago. Currently the Energy ISAC has 50 corporate memberships representing about 85% of the industrial facilities and has vetted over 250 individuals in those companies for access. The recent infusion of funding is allowing the numerous Oil and Gas Associations to solicit their members for application to the ISAC. As a result membership should increase substantially in the near term. Membership reaches into all industry segments, i.e., refining, pipelines, transportation, production and distribution.

4. The Reach of the Financial Services – FS-ISAC

In October, 1999, the Financial Services ISAC was formed (FS-ISAC). The FS Sector is estimated to consist of the following:

Banks 19,000
Insurance 3,200
Securities firms 5,000 (this includes many small firms)
Total: 27,200

Current FS-ISAC membership over 100 (plus four trade associations) with a reach of:

Banks 7,500
Insurance 20
Securities firms 600 (representing 99% of all securities business)
Total 8,120

The FS/ISAC was restructured in 2003 and launched a new FS/ISAC in December 2003. The new ISAC has multiple service levels designed to reach all eligible firms, addressing both physical and cyber threats, vulnerabilities, and events. The 2005 goal is to reach 99% of the eligible firms with Urgent and Crisis alerts within one hour of notification.

5. The Reach of the HealthCare ISAC – HealthCare ISAC

The HealthCare ISAC is in its formative stages. The initial Advisory Council, established in 2003, consists of representatives from nearly all aspects of the healthcare infrastructure, to include, research and academic, providers, pharmaceuticals, and several industry associations. The intent is to continue development of a similar analytical and alert capability found in the other ISAC organizations, and to maximize representation of all elements of the infrastructure associated with care delivery. A funding model is still under development.

6. The Reach of the Information Technology ISAC – IT-ISAC

In January, 2001, the Information Technology Association of America (ITAA) and the Founding Members announced the creation of the Information Technology ISAC (IT-ISAC). The membership of the IT-ISAC includes many of the world's leading information technology companies. The mission of the IT-ISAC includes detection, analysis and dissemination of cyber events that have the potential to threaten both the national security and economic viability of the United States. The IT-ISAC maintains close ties and ongoing communications with both other vertical sectors and with federal and state government agencies. The membership now includes 25 members with almost twice that number actively considering application. ITAA is working under contract with the IT-ISAC, leading efforts to recruit additional new members.

The reach of the IT-ISAC membership is global as the membership includes the major providers of software, hardware, services and security solutions. These companies supply the vast majority of the world's information technology goods and services. Their combined reach extends to about 90% of all desktop Operating Systems, 85% of all databases, 50% all desktop computers, 85% of all routers, and 65% of software security. Further, the IT-ISAC member companies are represented in nearly every major technology association and security group. These groups exchange information and analyses on the latest vulnerabilities and solutions.

Additionally, when necessary to communicate to a larger audience, the IT-ISAC can deliver information to the full ITAA membership regarding incidents and solutions. ITAA has over 500 direct members, has a close working relationship with approximately 50 regional IT associations (RITAs) in the United States and 41 leading IT associations around the world who are affiliated with the World Information Technology and Services Alliance (WITSA). WITSA, of which ITAA serves as the permanent Secretariat, provides a critically important platform for truly global outreach.

7. The Reach of the Surface Transportation ISAC – ST ISAC

In May 2002, the Association of American Railroads formally announced the creation of the Surface Transportation ISAC (ST ISAC).

The ST ISAC's membership includes the major North American freight railroads and AMTRAK to include the major Canadian and Mexican railroads. The Class 1 freight railroads comprise approximately 95% of the national railroad infrastructure. In addition, the ST ISAC is reaching out to the approximately 480 short line railroads through the American Shortlines & Regional Railroad Association (ASLRRA). Within the overall ST ISAC, the Public Transit community has established a Public Transit ISAC with approximately 100 of the major U.S. transit entities enrolled with a goal of 400 this year. The Public Transit ISAC reaches additional transit entities through the American Public Transit Association (APTA).

8. The Reach of the Public Transit ISAC – PT-ISAC

(A subset within the ST_ISAC)

In January, 2003, the American Public Transportation Association (APTA) was designated as the Public Transit Sector Coordinator by the U.S. Department of Transportation in the creation of a Public Transit ISAC (PT-ISAC) to further promote security for the public transportation industry. The PT-ISAC is an "ISAC within an ISAC" because it takes advantage of the already existing capabilities of the overarching Surface Transportation ISAC (ST-ISAC), sponsored by the Association of American Railroads (AAR).

As the designated Sector Coordinator, APTA serves as the primary contact to organize and bring the public transportation community together to work cooperatively on physical and cyber issues. The PT- ISAC serves both APTA members and non-members of the transit community.

APTA is a private nonprofit international association of over 1500 member organizations including public transportation systems and commuter rail operators; planning, design, construction and finance firms; product and service providers; academic institutions; and state associations and departments of transportation. APTA members serve more than 90 percent of persons using public transportation in the United States and Canada.

The public transportation market includes all multi-occupancy vehicle services designed to transport the public. These services are: private and public buses; rail, ferryboats; Amtrak, intercity bus, and taxi services under contract to a public transportation agency; any vanpool service operated by or under such a contract; and other transportation services for senior citizens and persons with disabilities.

Currently the Public Transit ISAC directly reaches approximately 100 of the major national transit entities. Participation agreements are being finalized with over 400 transit agencies.

9. The Reach of the Telecommunications Infrastructure ISAC – Telecom ISAC

In January 2000, the National Coordinating Center for Telecommunications was officially designated an ISAC due to its long history as a central hub for sharing critical information among Government and industry. Telecom-ISAC membership is open to companies that provide network services, equipment or software to the communications and information sector, and to select professional associations or companies with participation/presence in the communications and information sector. Currently, there are 30 member companies and 3 member associations, the Cellular Telecommunications & Internet Association (CTIA), the Telecom Industry Association (TIA), and the United States Telecom Association (USTA).

The National Communications System, now part of the Department of Homeland Security, Information Analysis and Infrastructure Protection Directorate, has operated a 24x7 watch and analysis operations center for the Telecom-ISAC since September 2001. Means of communications include email, alternate email, secure message forum, phone, fax, cell phone, and pager as well as in-person briefing with some member company representatives located on site at the Telecom-ISAC. Some member company representatives have Secret or Top Secret security clearances.

Through member companies and member associations, the reach of the Telecom ISAC within the United States includes:

- approximately 95% of wireline telecommunications service providers, by serving areas and subscribers,
- over 60 % of wireline telecommunications vendors, by sales volume,
- approximately 95 % of wireless telecommunications service providers, by serving areas and subscribers,
- over 90% of the wireless telecommunications vendors by sales volume,
- over 42% of the consumer Internet Service Providers subscribers,
- approximately 90% of the Internet Service Providers backbone networks,
- 6 of the top 10 system integrators in the U.S. Federal IT market,
- 15% of Domain Name Service root and global Top Level Domain operators

10. The Reach of the Truck ISAC – Truck ISAC

The American Trucking Association (ATA) operates the Truck ISAC, which is still in its infancy pending release of appropriated federal funding by TSA. The Truck ISAC is open to ALL trucking industry interests. The ISAC website postings are "public", as we are trying for the broadest possible dissemination to the 700,000+ entities that possess DOT numbers, of which 590,000+ are cargo motor carriers.

Regular communication is to over 3000 company contacts and the executives of the 65 state and national trucking organizations that make up the Trucking Security and Anti-Terrorism Working Group (TSWG). The organizations are in turn asked to use their internal communications to alert their respective members. Collectively, TSWG

represents 38,000 trucking companies with approximately 60% of the economic activity of the industry, employing about 1.5 million drivers. (This is about 50% of the 3 million or so long-haul operations). The vast majority of the 590,000 cargo carriers are independent operators with 1-5 vehicles, most of whom are not members of any organized industry group. The Truck ISAC has an additional vetted list of about 250 trusted corporate security directors (representing primarily the largest fleets and association executives).

The Highway Watch Call Center, which takes information from and pushes it to a population of over 6000 trained drivers, is operating in 27 states, with two more nearing implementation. A report of any security related information is immediately called to the Truck ISAC, which in turn passes the information to NIPC Watch, TSIS Watch and DOT's crisis center. The Highway Watch Call Center is targeting to expand the driver population by 300,000 in the first year of full implementation and to 600,000 total trained professionals in the second year.

11. The Reach of the Water ISAC – WaterISAC

Covering both Drinking Water and Wastewater Utilities around the Nation

The WaterISAC was launched in December 2002 through the Association of Metropolitan Water Agencies (AMWA). The Water Sector encompasses the nation's drinking water and wastewater. The magnitude and complexity of the sector cannot be overstated with utilities ranging in size from those serving a few hundred to systems serving millions of people. The nation's community drinking water systems number over 54,000 with over 17,000 publicly owned treatment works (POTW) or wastewater treatment facilities scattered throughout the country.

Currently, the WaterISAC is providing information to water and wastewater utilities who serve more than 40 percent of the nation's population. In addition, the WaterISAC, through AMWA, is developing the ability to push information out to all drinking water and wastewater utilities in highly critical circumstances or emergency situations serving over 200 million people.

Conclusion

The ISACs represent an extremely large portion of the US infrastructure. When considered collectively, these individual sector ISACs, as an "ISAC Community," possess an outreach and connectivity network to approximately 65% of the U.S. private critical infrastructure.

Over a short span of time and limited resources, the private sector ISACs have completed a tremendous growth phase and present a tremendous capability to conduct analyses of infrastructure vulnerabilities and threats and then move that into rapid dissemination throughout a sector or sectors, thus achieving the base goal for information sharing. ***

While individual ISACs and the ISAC Council take great pride in the current accomplishments, the ISACs know that there remains much more to accomplish to reach our desired goals. In defining what an ISAC is and how each sector employs that effort, it is our goal to share best practices not only in passing information, but more primarily in the analysis of that information. Government analytical efforts are critical, but private sector analytical efforts should not be overlooked and must be integrated into the federal processes for a more complete understanding. The private sector understands its processes, assets, and operations best and can be relied upon to provide required private sector subject matter expertise.

The private sector must be fully considered during all phases of the federal government's intelligence cycle: information/intelligence requirements, tasking, collection, analysis, and reporting and dissemination.

It is understood that the ISACs must continue to increase their reach into the US critical infrastructure. Further development of the ISAC value proposition is only one part of this effort. The ISAC Council is working on various operational, process, and other common issues to effectively analyze and disseminate information and where possible to leverage the work of the entire ISAC community.

The ISACs must enroll, and count among its members, companies who cannot afford to pay for ISAC membership. Government funding support is needed to assist the ISACs in their outreach to the innumerable small critical infrastructure entities throughout the nation.

The ISAC Council has reached out to the Federal Government and the resulting inclusion of various government participants in our Council deliberations has been a very positive development.

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. Members have contributed to this white paper.

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.

Annex A – Web Sites for ISAC Council Members

www.isaccouncil.org

<http://chemicalisac.chemtrec.com>

www.esisac.com

www.energyisac.com/index.cfm

www.fsisac.com

www.hcisac.org

www.it-isac.org

www.ncs.gov/ncc/main.html

www.truckline.com/insideata/isac/

www.surfacetransportationisac.org/
(Includes Public Transit)

www.WaterISAC.org

Annex B - PDD – 63 (portion regarding ISACs)

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.