

JANUARY 2009

SUBJECT: THE ROLE OF INFORMATION SHARING AND ANALYSIS CENTERS (ISACs) IN PRIVATE/PUBLIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION

PURPOSE: THIS PAPER PROVIDES RECOMMENDATIONS, ISAC COMMUNITY ACCOMPLISHMENTS, AND BACKGROUND INFORMATION FOR THE NEW ADMINISTRATION.

RECOMMENDATIONS:

What should be done?

- Leverage the expertise and experience of existing private/public sector critical infrastructure protection organizations to improve the resilience of the nation.
- Maximize the operational foundation of the ISACs that share information between the government and private sector critical infrastructures, as well as share information among sectors.
- Support the needs of all critical infrastructures to provide trusted and secure actionable information sharing and sector specific analytical capabilities while respecting the individuality of each sector.

Why ISACs?

ISACs are trusted entities established by critical infrastructure owners and operators.

- The ISACs have unique capabilities to provide comprehensive sector analysis and have the ability to reach extensively within their sectors, with other sectors, and with government to share critical information.
- The ISACs comprehensively respond to all aspects of security and “all hazards”. Critical technical, IT/cyber, and physical infrastructures and cross sector interdependencies are analyzed and addressed.
- After many years of experience, especially during events of national significance, ISACs have demonstrated successes in providing operational services such as risk mitigation, incident response, and information sharing that protects the nation’s critical infrastructures.
- The ISACs have a track record of responding to and sharing actionable and relevant information more quickly than DHS and doing so in an accurate manner.
- ISACs empower business resiliency through security planning, disaster response and execution. Most ISACs, by definition, have 24/7 threat warning, incident reporting capabilities which are critical to the success of protecting critical infrastructure.

ISACs ACCOMPLISHMENTS:

ISACs address physical and cyber threats, incidents and vulnerabilities by working across sectors through the ISAC Council, the Partnership for Critical Infrastructure Security (PCIS), and DHS, and play a key role in coordinating sector wide response to incidents.

1. During the recent Gustav and Ike hurricanes, ISAC operational staff was embedded at the DHS National Infrastructure Coordinating Center (NICC) to help establish, obtain and share ground truth information about the cross-sector impact of these events.
2. The ISACs, on a daily basis, exchange cross-sector information about the latest Internet threats, vulnerabilities and incidents.
3. Each week the ISACs meet to discuss physical security threats, vulnerabilities, mitigations and incidents.
4. When the DNS Cache Poisoning vulnerability was discovered, ISACs shared mitigation strategies, and several ISACs issued a joint Bulletin to each sector underscoring the urgency of the vulnerability and encouraging specific remediation activities.
5. The National Infrastructure Advisory Committee (NIAC) in its report entitled *Public-Private Sector Intelligence Coordination* identified the value to the nation of private sector information sharing and analysis through four case studies. The report reviewed information sharing and analysis during four events: the August 2003 Blackout, the July 2004 Financial Services Threat Alert, the July 2005 London Bombings, and the October 2005 New York Public Transit Threat Alert. The report cited conclusions and lessons learned from these four events, including:
 - In this age of continuing terrorist threats to U.S. interests, the Federal government must engage the private sector early in analyzing and disseminating information and intelligence. Private sector expertise is critical in knowing what bits of information are important, knowing who to contact with the information, and knowing what action to take as a result.
 - Existing communication architectures among private/public sector organizations are useful for sharing information and analysis. The private sector possesses a profound understanding of cyber security. Subject matter experts can analyze network information quickly and accurately to support analysis.
 - It became clear early on August 15, 2003 that coordination between the Electricity Sector Information Sharing and Analysis Center (ESISAC) and the Information Technology Information Sharing and Analysis Center (IT-ISAC) provided enough assurance to electric sector investigators to allow

them to focus on physical causative factors and restoration. The cyber investigation led by DHS confirmed these initial findings.

- During the London bombing incidents, DHS and other government information shared with critical infrastructure owner/operators lagged between three and four hours compared to information disseminated by the ISACs with the notable exception of NYPD Shield. In addition, initial reporting to other possibly affected sectors was from the PT/ST-ISAC.
 - Trusted relationships between private/public sector owners/operators and the IC [Intelligence Community] are keys to success. The ISACs have fostered these trusted relationships with many key law enforcement and intelligence agencies.
6. The ISACs routinely share trusted information within their respective sectors and across other sectors. Many ISACs operate at classified levels.
 7. Each sector has different public/private partnership information sharing needs. Some have developed the ability to share information with other members without attribution. This capability has been cited as critical to sharing information with competitors and building trust within sectors.
 8. ISACs have been active in supporting national level exercises such as TOPOFF3, TOPOFF 4, Cyber Storm I and II and the recent NLE02-08 DHS exercises. Some of the sectors have developed their own exercises such as the financial services sector's pandemic flu exercise in 2007 that had over 2,700 members participating and was operationally supported by the FS-ISAC. On August 1, 2008, a cross-sector table top exercise was conducted by the key private/public sector critical infrastructures and the ISACs played key facilitation roles during this event.
 9. The ISACs have formed an ISAC Council which all ISACs and sectors without ISACs are invited to participate. The objective of the ISAC Council is to establish and maintain an operational framework in order to maximize information flow across the various private sector critical infrastructures and with government.
 10. The ISAC Council co-sponsors the Critical Infrastructure Protection (CIP) Congress along with PCIS and InfraGard. This annual event serves as a focal point for cross-sector information sharing and brings together representatives from most of the critical infrastructures along with officials from DHS, law enforcement and state and local governments.

ISAC BACKGROUND INFORMATION:

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.

In PDD-63, the federal government asked each critical infrastructure sector to establish sector specific information sharing organizations to share information, within each sector, about threats and vulnerabilities to that sector. In response, many sectors established “Information Sharing and Analysis Centers” to meet this need.

By definition, an ISAC is a trusted, sector specific entity which performs the following functions:

- provides to its constituency a 24/7 secure operating capability that establishes the sector’s specific information sharing/intelligence requirements for incidents, threats and vulnerabilities;
- collects, analyzes, and disseminates alerts and incident reports to its membership based on its sector focused subject matter analytical expertise;
- helps the government understand impacts for its sector;
- provides an electronic, trusted capability for its membership to exchange and share information on cyber, physical and all threats in order to defend the critical infrastructure; and
- share and provide analytical support to government and other ISACs regarding technical sector details and in mutual information sharing and assistance during actual or potential sector disruptions whether caused by intentional, accidental or natural events.

ISACs continue to form and mature, and meet regularly through the ISAC Council. The ISAC Council comprises fourteen ISACs and was formed in 2003 to work on common operational themes and issues for exchanging information intra-ISAC and inter-ISAC. Since then, the ISAC Council has expanded its mission to exchange critical information with other sectors that do not have ISACs in place.

The current reach of the ISACs to the various critical infrastructures is extensive. When considered collectively, the individual private/public sector ISACs possess an outreach and connectivity network to approximately 85% of the U.S. critical infrastructure. The following are statistics regarding a select number of the ISACs’ reach within their respective sectors:

- ***Electricity Sector ISAC:*** Part of the North American Electric Reliability Corporation (NERC), the ES-ISAC’s coverage, direct to a given bulk power system entity or via the eighteen Reliability Coordinators covers the entire continental United States and Canada and is virtually 100%. The ES-ISAC is also working on developing the necessary communication and participation with non-bulk power system entities (i.e. smaller electric distribution organizations) to include relationships with their critical suppliers.

- **Financial Services ISAC:** has over 4,200 direct members and through 30 member associations, has the ability to reach 99% of the banks and credit unions and 85% of the securities industry, and nearly 50% of the insurance industry.
- **Information Technology ISAC:** through its members, it reaches 90% of all desktop operating systems, 85% of all databases; 76% of the global microprocessor market; 85% of all routers and 65% of software security.
- **Surface Transportation ISAC:** In 2002, at the request of the Secretary of Transportation, the Association of American Railroads created the ST-ISAC. The ST-ISAC supports 95% of the North American freight railroad infrastructure.
- **Public Transit ISAC:** The American Public Transportation Association (APTA) was designated by the US Department of Transportation as the sector coordinator for the US public transit industry. In this role APTA created the PT-ISAC to serve the needs of the industry. APTA's members serve more than 90% of persons using public transportation in the United States and Canada.
- **Communications ISAC:** The DHS National Coordinating Center partners with the private sector in the ISAC and provides 24x7 operational support. Members include communications equipment and software vendors, 95% of wire line communications providers, 90% of wireless communications providers, including satellite providers, and 90% of Internet Service Provider backbone networks.
- **Water ISAC:** Currently provides security information to water and wastewater utilities that provide services to more than 65% of the American population.
- **Multi-State ISAC:** includes all 50 States, the District of Columbia, four U.S. Territories many local governments. Additionally, the MS-ISAC continues to broaden its local government's participation to include all of the approximate 39,000 municipalities.

For further information please contact: ISAC Council Chairperson, Mr. Will Pelgrin, at William.pelgrin@cscic.state.ny.us, 528-473-4383

Please visit the ISAC Council public website at www.isaccouncil.org