NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

JULY 13, 2004

THOMAS E. NOONAN
WORKING GROUP CHAIR
CHAIRMAN, PRESIDENT & CEO
INTERNET SECURITY SYSTEMS, INC.

ACKNOWLEDGEMENTS

Mr. Noonan wishes to acknowledge the entire working group, their support staffs and all other contributors, listed below, for the efforts they devoted to this study. Their time, insight, and dedication are deeply appreciated.

- **Working Group Members**
  - Mr. Richard Davidson, Chairman, President & CEO, Union Pacific
  - Mr. John Chambers, Chairman & CEO, Cisco Systems
  - Mr. Archie Durham, Chairman, ConocoPhillips
  - Mr. Albert Edmonds, President U.S. Government Systems
  - Ms. Margaret Grayson, President & CEO, V-ONE Corporation
  - Mr. Enrique Hernandez, Jr., President & CEO, Inter-Con Security Systems, Inc
  - Mr. Charles Holiday, Jr., President & CEO, DuPont Company
  - Ms. Karen Katen, President, Pfizer Global Pharmaceuticals & Exec. V.P. Pfizer, Inc.
  - Commissioner Raymond Kelly, City of New York
  - Mr. Richard Kovaceich, Chairman & CEO, Wells Fargo
  - Mr. George Martinez, Chairman, Sterling Bank and Bancshares, Inc
  - Mr. Martin McGuinn, Chairman & CEO, Mellon Financial Corporation
  - Mr. Thomas Noonan, Chairman, President & CEO, Internet Security Systems, Inc
  - Mr. John Thompson, Chairman & CEO, Symantec Corporation
  - Mr. Thomas Weidemeyer, Chief Operating Officer, United Parcel Service

- **Study Group Members**
  - Mr. Scott Algeier, U.S. Chamber of Commerce
  - Mr. Peter Allor, Internet Security Systems, Inc.
  - Mr. Daryl Eckard, EDS
  - Dr. Chris Feudo, EDS
  - Mr. Bobby Gillham, ConocoPhillips
  - Ms. Suzanne Gorman, SIAC
  - Ms. Margaret Grayson, V-ONE Corporation
  - Mr. Rick Holmes, Union Pacific
  - Ms. Tiffany Olson – Jones, Symantec Corporation
  - Mr. Lou Leffler, NERC
  - Mr. Aaron Meckler, Wells Fargo
  - Mr. John Nallin, UPS
  - Mr. Glen Rust, Bank Sterling
  - Mr. Randolph Smith, UPS
  - Mr. Ed Ternan, Inter-Con Security Systems, Inc.
  - Mr. Christopher Terzich, Wells Fargo
  - Ms. Susan Vismor, Mellon
  - Mr. Kenneth Watson, Cisco Systems

- **Other Study Contributors**
  - Mr. William Marlow
  - Mr. Paul Wolfe, EWA Information and Infrastructure Technologies, Inc.
  - Mr. Jack Legler, American Trucking Association
  - Mr. Robert Wright, BellSouth
  - Ms. Diane Van DeHei, Association of Metropolitan Water Agencies
  - Ms. Peggy Lipps, Bank of America

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND AND METHODOLOGY

Introduction

The National Infrastructure Advisory Council (NIAC) was created by Executive Order 13231 of October 16, 2001, as amended by Executive Order 13286 of February 28, 2003. The Executive Order tasks the NIAC with advising the President on matters and issues dealing with the security of information systems for the nation's critical infrastructure, supporting the following sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government service.

On April 22, 2003, the NIAC agreed to undertake a project to analyze the current environment for information sharing and analysis across the critical infrastructure sectors and make recommendations to the government regarding enhancements, increased effectiveness and broader influence across industry sectors.

Approach

Initially, the NIAC decided to explore four areas in order to satisfy the assigned task:

1. Business models for sharing and analyzing information;
2. Financial models for supporting the information processes;
3. Level of information analysis and aggregation; and
4. Dissemination breadth and coverage.

It was further decided that the Evaluation and Enhancement of Information Sharing (EEIS) study would leverage existing information and analyses — in particular, the body of work produced by the Information Sharing and Analysis Center (ISAC) Council.[1] The ISAC Council has delivered its work to the Department of Homeland Security's (DHS) Information Assurance and Infrastructure Protection Directorate (IAIP) and is now working to implement many of its recommendations.

ISAC Council White Papers, January 31, 2004:

- Government-Private Sector Relations
- HSPD-7 Issues and Metrics
- Information Sharing and Analysis
- Integration of ISACs into Exercises
- ISAC Analytical Efforts
- Policy Framework for the ISAC Community
- Reach of the Major ISACs
- Vetting and Trust for Communication Among ISACs and Government Entities[2]

The White House:

[1] A federation of 11 ISACs as members and three liaison ISAC members.

[2] Sources of material (www.isaccouncil.org)

- Presidential Decision Directive (PDD)-63 (May 22, 1998)
- Homeland Security Presidential Directive (HSPD)-7: Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003)
- HSPD-8: National Preparedness (December 17, 2003)

General Accounting Office

- "Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors" (April 21, 2004)

FUNDAMENTAL PRINCIPLES

The responsibility for the defense of our nation does not lie solely with the Federal Government. Rather, it depends on coordinating the complex, interrelated efforts and infrastructures of the government and the private sector. It is generally estimated that the private sector owns 85 percent of the critical infrastructure, and is overwhelmingly responsible for research and development contributing to enhanced operations and new systems design. Most private industry sectors have heeded the call to share information contained in PDD-63 and have instituted ISACs as a means to support increased security to the nation and its critical infrastructures. This has proven to be a costly undertaking and the overarching support for maintaining this significant security capability and rich area of expertise falls short in funding and in design. Even so, the sectors have achieved a limited set of objectives that they set for themselves. The successes to date are owed to a variety of factors, including sector governance, industry security strategies developed in response to past threats and government regulations.

Future development and improved effectiveness depend on understanding the desired outcome and degree of interdependence. Participants in the private sector must understand what the government expects them to accomplish and to what extent the government is willing to provide support in pursuit of that goal. Likewise, the private sector must continue cross-industry cooperation independent of governmental participation, and, to a larger degree, supply and support the Federal Government with timely information and analyses. Without this, the partnership that defends the nation will be weak and ineffective. Further, the Council recognizes that all sectors maintain a strong desire to contribute to the nation's defense, but vary significantly in governance strategies and capabilities. Therefore, we strongly recommend against any government attempt to impose a single, cookie-cutter organizational model.

During the course of this study, the NIAC reached the following conclusions:

- □ From the inception of this task on April 22, 2003, there have been significant changes in the landscape affecting information sharing, including:
    - ■ The White House release of HSPD 7 and 8 in December 2003, superseding PDD-63.[3]

[3] PDD-63 is the initial document that suggested the private sector assist in defending critical infrastructures and also called for the implementation of ISACs.

- DHS's significant staffing and procedural development.[4] While changes will continue, the rate of change has slowed to a point where the government and the private sector can coordinate more effectively on a regular basis.

- A number of private-sector ISACs have come together to form the ISAC Council.[5] At times, the Council has also dealt with some matters directly impacting ISAC operations referred to as Operational Policy. Other, broader issues were left for the Sector Coordinators to take up as a matter of policy and coordination with the Federal Government.

- Several ISACs are undergoing restructuring. Currently, Financial Services and Information Technology, two of the major ISACs, are restructuring their operations to better serve the market-driven members desiring a deeper and more comprehensive set of analyses and notification, and recall procedures. The restructuring efforts also enable sector-wide means of notifications for alerts and advisories — a major step toward achieving the government goal of 100 percent notification throughout a sector.

  This change was brought about after a major study commissioned by the Department of Treasury to extend the effectiveness of the Financial Services ISAC to the entire industry sector. The Information Technology ISAC is also leveraging the study, and is restructuring to achieve the same goals, which are:
  - Passing alerts and advisories from DHS;
  - Transmitting sector-specific information and alerts/advisories;
  - Creating a broader security set of information from sector analysts;
  - Using sector-specific institutional knowledge;
  - Building links and information from other sectors through vetted trust circles; and
  - Generating links and communications channels with the Federal Government.

  These two ISACs have tiered membership levels to allow all organizations within the respective sectors to achieve baseline connectivity for alerts and advisories, and to allow for market-driven analysis and reporting.

- Sector Coordinators now have a more formal working relationship. Half-way through this study's research phase, Partnership for Critical Infrastructure Security[6]

[4] Congress established DHS in November 2002, partly in response to the September 11, 2001, attacks on the United States. DHS began setting up its operations in early 2003 and for the Information Analysis and Infrastructure Protection Directorate, the basic outline of personnel, duties, and roles, and responsibilities were not filled until the fall of 2003. This has a continuing effect as new procedures are implemented and positions are filled, which will impact the work between government and industry and, ultimately, this study.

[5] To date, the ISAC Council has written and published, eight white papers, which outline major issues affecting operations among ISACs and between ISACs and the government.

[6] U. S. critical infrastructure sectors identified by PDD-63, companies and associations belonging to the critical infrastructure sectors listed in PDD-63, risk management and investment professionals, and other members of the business community that interact with these sectors are welcome. Government agency representatives, members of Congress, and staff are invited to participate in working group discussions and Partnership meetings.

reorganized itself around the Sector Coordinators. The group is working to set its agenda and goals.

- □ Coordination between DHS, the ISAC Council, and Sector Coordinators is increasing. While each individual ISAC has links to DHS for communicating individual needs for information and coordination,[7] formal meetings of the groups are now taking place on a regular basis. Since the summer of 2003, the ISAC Council has invited IAIP leaders to their meetings to discuss collective issues regarding the sharing of information, analysis, and alerting. These monthly meetings expanded in December 2003, when the ISAC Council set up the Critical Infrastructure Protection Retreat, co-hosted with the sector coordinators, with participants from DHS and the White House. The cooperation fostered by these meetings, along with the development of issue-related white papers, increased the collective ability to coordinate activities.

- □ Information sharing has many levels. While many use the term "information sharing" universally, there are unique interpretations for what it means. During the course of this study, the NIAC did not review the analysis or reporting capabilities of the intelligence community, law enforcement, nor that of first responders because their requirements are significantly different than those of the owners and operators of critical infrastructure companies. However, as stated below, some conclusions were reached regarding the different approaches to information sharing.

  - ■ **Strategic** — This level of information sharing is focused on the threat and its potential to harm critical functions to include the sector infrastructures. It is heavily oriented and focused on terrorism. This area is predominantly led by the intelligence community and/or federal and state law enforcement.

  - ■ **Operational** — This level of information sharing is focused on the critical infrastructures/sectors and how they support systems to provide services to large numbers of people or support the economy and defenses of the nation. Each critical infrastructure has physical and cyber aspects. In the first instance, physical is sector specific — shaped by the evolution of the industry, often over a period of decades. Interstate commerce and regulation, along with developed practices, make the physical response unique to each infrastructure, and, in turn, each infrastructure has developed responses to suit its unique requirements. By contrast, cyber responses are universal because each infrastructure is using essentially the same sets of hardware, software, and deployment to communicate and control business functions. At the operational level or critical infrastructure level, the focus for physical issues is internal, while the cyber aspects and conditions are external and interdependent. Many of the sectors and their ISACs are more focused on information sharing that is cyber-related.

  - ■ **Tactical** — This level of information sharing is centered on first response to incidents. The range of incidents varies widely for emergency services, fire, and law

[7] Coordination is done primarily through IAIP's Infrastructure Coordination Division (ICD).

enforcement, but information sharing at this level is predominately related to the physical or terrorism.[8]

- □ Information sharing has many elements. During the course of this study, the NIAC came to recognize that many organizations had differing opinions as to what constituted information sharing. The list below addresses the cyber aspects of information sharing, which are almost universal across the sectors. Many organizations become focused on a single aspect, such as early warning or threat. While the NIAC understands the importance of each element, it believes that all must be taken into consideration in order to prevent attacks on critical infrastructures.

  - ■ **Vulnerability Information** -- What is the attack vector and what does it affect?[9]
  - ■ **Exploits** -- An attack usually written to take advantage of a specific software or system vulnerability. It represents how a vulnerability is exploited.
  - ■ **Threats** -- Who will attack a system using one or more exploits against vulnerabilities?[10]
  - ■ **Incidents** – The result when a system is attacked or compromised by an exploit.
  - ■ **Best Practices** -- Provide the means, methods and processes to protect an organization or infrastructure from malicious attacks or behavior.
  - ■ **Early Warning System** -- A system of sensors or intelligence that provides advance notification of probable attack or duress on a system or infrastructure.

- □ Delivery of information to the private sector is executed through two general means: the ISACs of sector critical infrastructures, or through other, non-aligned, mechanisms for the remaining businesses and organizations.

  - ■ **Critical Infrastructures** — Some sector-specific delivery mechanisms are through an operations center dedicated to providing communications and analysis in response to market-driven demands and requirements

  - ■ **Non-Aligned Businesses** — Many organizations and institutions have not joined an ISAC to date. Reasons for this include unfamiliarity with the ISAC concept, a lack of endorsement for ISAC capabilities and coordination and costs associated with membership. These organizations either rely upon their own research, that of the U.S. Government, or they individually have one of several commercial operations deliver the information they require to maintain situational awareness.

- □ Cross-sector operations have been initiated between ISACs. The trust developed through mutual discussions and deliberations within the ISAC Council has led the major ISACs to implement daily conference calls between ISACs and to establish sector-managed mailing lists. While DHS's U.S. Computer Emergency Readiness Team (CERT) is a regular participant, this private sector exchange allows any ISAC to establish communications between any or all of the other ISACs. This empowers ISACs to coordinate efforts, such as

[8] From all hazards including: physical, terrorist, or cyber events.
[9] For example, the weakness that could be compromised or exploited.
[10] Threats could include individuals, hacking groups, hired hackers for organized crime, terrorists, and nation states.

providing sector-specific information to each ISAC's membership in times of incidents or major vulnerability announcements.

- □ Many ISACs are now communicating with their lead government agencies and DHS to cover a wide range of information-sharing issues affecting individual sectors, and their operations. Much of this increased communication is due to the support provided by the lead agencies. Increased communication has been instrumental in helping define common areas of interest.

- □ ISACs are at different levels of maturity.

Suggested Maturity Model for ISACs:

Maturity >> **Dimension**	**Level 1 Framework and Policies Established**	**Level 2 Procedures Developed**	**Level 3 Procedures for Communications and Responses Implemented**	**Level 4 Procedures and Responses Tested**	**Level 5 Procedures, Communications and Reponses, are Integrated Cross-Sector**
Vulnerability Analysis	Identified	Defined	Distributed– Primarily Alerting	Impact Advice and Mitigations Available	Trend Analysis and Cross-Sector Integration
Threat Analysis	Identified	Defined	Distributed – Primarily Alerting	Impact Advice and Mitigations Available	Trend Analysis and Cross-Sector Integration
Cross-Sector Coordination	None	Some	Moderate – 30% to 50% of Sector Participation	Majority of Sector Participates	Cross-Sector Integration
Data Availability – Real-Time Flow	Little Except Vendor-Specific	Some	Can Be Collected From Sector and Vendors	Readily Available	Standard Repository and Analysis Available
Response Time	Uncertain	Key Enterprises can Prevent or Diminish Impacts	Most Sectors can Diminish Impacts Quickly	Most Threats Have Little or Localized Impact	Anticipates Emerging Threats

Issues and Recommendations

The NIAC identified four major issues for the President.

<u>Issue 1</u> – The definitions, roles, and responsibilities of ISACs and Sector Coordinators are not well understood by many ISACs, Sector Coordinators, and government leaders. They are not adopted universally by the Federal Government.

<u>Recommendation:</u>

Embrace the following roles for ISACs and Sector Coordinators:

- The ISAC as a central source in each sector for dissemination, sharing and communication of information on cyber, physical, and all threats, vulnerabilities and incidents in order to defend the critical infrastructure.
- The U.S. Government should recognize and support the mission and role of the ISACs as a conduit/focal point to the private sector for information sharing and analysis.
- Sector Coordinators should address overarching critical infrastructure issues and contribute to policy development. They should also monitor sector-wide vulnerability analyses for risk mitigation and provide the coordination sector governance for Homeland Security issues.

Government and the private sector should work to support:

- Refining of the roles and responsibilities of the Sector Coordinator.
- Developing of communications and alert facilities with the ISACs.
- Encouraging the use of ISAC communications.
- Clarifying of the relationship between Sector Coordinators and their ISACs, for those sectors represented by ISACs.
- Establishing criteria to determine if a critical infrastructure sector or a key asset meets the definition in the Patriot Act and in HSPD-7.

SUB ISSUE

Definition of an Information Sharing and Analysis Center (ISAC)

"An ISAC is a trusted, sector-specific entity, which provides to its constituency a 24/7 Secure Operating Capability establishing the sector's specific information/intelligence requirements for incidences, threats and vulnerabilities. Based on its sector-focused subject matter analytical expertise, the ISAC then collects, analyzes, and disseminates alerts and incident reports to its membership and helps the government understand impacts for their sector. It provides an electronic, trusted ability for the membership to exchange and share information on cyber, physical, and all threats, in order to defend the critical infrastructure. This includes analytical support to the 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 or natural events."

<u>Issue 2</u> **– The current business models for most ISACs have drawbacks regarding continuous flow of analysis and information to the members.**

<u>Recommendation:</u>

Enhance private sector ISACs' reach through infrastructure enhancements without delivery of private sector data or meta-data.

- Assist ISACs in delivering basic alerts and advisories to their sectors. Increase the volume of alerts and advisories for public use and consumption. Increase dissemination of the alerts and advisories that have cross-sector impact or interdependencies (for example, passing an alert to the financial services sector, while not passing the same alert to the information technology sector).

- As the ISACs continue to mature operationally, working with DHS and more importantly, between themselves, they are becoming greater targets for surveillance from adversaries. While clearances and secure telephones would enable a limited degree of interoperability, a commercial-grade system and key would be of greater value in opening the channels of communication and coordination. This is important not just in times of incidents and events, but also during the trust and routine operations phase, where an adversary would most likely target and learn the interdependent centers of gravity.

Facilitate ISAC operations and leadership security clearances. To further aid in this effort, DHS should establish processes for security clearances based on a "need to know" and "need to act" to support homeland or national security. Various sectors have personnel in positions of leadership, which may not qualify them for attaining a clearance through other channels. This support would allow the private sector to better partner with the Federal Government. Provide commercial grade encryption voice communication systems for use between sectors

- Provide sector-specific and broad-based strategic information, thus, increasing ISAC value and government communication,

- Provide base-level resources for the ISACs to deliver critical, urgent, lower tier information within their sector free of charge.

<u>Issue 3</u> **– There is a lack of government understanding with respect to the private sector's unique research and analytical capabilities.**

<u>Recommendation:</u>

Private Industry must be fully integrated into the Government's Intelligence Cycle, which consists of information requirements, tasking, analysis, reporting, and dissemination. Private-sector information requirements must be established and private-sector analytical capabilities must be integrated into the private sector/government information sharing and analysis efforts.

Create a two-tier information dissemination mode for the private sector with incorporation of private-sector analysis and focus into the government's base message and outreach for communicating differentiated alerts.

- **General alerts and information** (reach). This is the first tier of information and dissemination. All non-aligned business and critical infrastructure ISACs would receive this information. It provides the early warning for alerts and notifications of incidents and potential attacks from new announced vulnerabilities or exploits.

- **Sector-specific alerts and analysis** (analytical). This level of analysis is iterative and studies process interdependencies or weaknesses within systems. Those ISACs with the capability to do so would perform additional analysis and communicate issues across sectors and with the government to protect critical infrastructures. ISACs would deliver specific finished product analyses based on known information and intelligence requirements.

Issue 4 – The Federal Government has yet to establish a uniform system for collecting data from the private sector and has not made clear what type of information they want the private sector to share.[11]

Recommendation:

Provide for timely flow of unique private-sector information to the government.

- Analysis conducted by private-sector ISACs, which have a working relationship with DHS and knowledge of DHS requirements, is the appropriate means of ensuring that information is available to protect the critical infrastructures they own, and for government use in defending the nation. The processes[12] already in use by some ISACs in partnership with the government should be expanded and established as one of the working mechanisms for private sector and government cooperation.

- Most infrastructures are owned or operated by the private sector, so companies within sectors often house the only means to take action during incidents, and are uniquely positioned to defend these national assets. Further, the private sector is more flexible and can adjust priorities in rapidly changing and dynamic situations. This can complement government efforts.

- The concept of government as a "supported organization," is a paradigm shift for both the government and for the private sector. The NIAC supports the belief that the nation's critical infrastructures can be best secured through public-private collaboration. Such collaboration balances the private sector's business and security interests with the government's mandate to defend the nation and its supporting

[11] DHS is in the process of implementing the Critical Infrastructure Information Act of 2002, which is attempting to address this issue. More information is available at www.dhs.gov/pcii.

[12] These processes refer to the analyst and intelligence information exchanges and meetings.

structures. Successful collaboration requires the government to apply resources to support the efforts of the private sector.

CONCLUSION

Scaling ISAC membership to include most infrastructure owners and operators in each sector would provide a broader base for information collection about threats for ISAC analysis and warnings. It would also provide a broad base to transmit warnings, countermeasures and other solutions. Federal funding support may enable ISACs to include a greater percentage of their sectors than they are currently capable of doing. Successful research toward real-time, cross-sector event correlation will add significant value to threat warning, trending and analysis. Enhancing trust models will encourage cross-sector and public-private information sharing, thereby enabling the federal government to make timely decisions regarding possible attacks on the United States.

Issue 1 – The definitions, roles, and responsibilities of ISACs and Sector Coordinators are not well understood by many ISACs, Sector Coordinators and government leaders, and are not adopted universally by the Federal Government.

It is generally accepted that information sharing is essential and must be more effective. To this end, it is important to establish clear definitions and roles of an ISAC, Sector Coordinator, Critical Infrastructure and other key assets. The roles must be articulated at a national level so all participants in this partnership can be cognizant of their responsibilities.

Sub-Issue

□ Clear definitions are necessary.

■ The NIAC proposes the term ISAC be defined as follows:
"A trusted, sector specific entity, which provides to its constituency a 24/7 Secure Operating Capability establishing the specific sector's information/intelligence requirements for incidences, threats, and vulnerabilities. The ISAC collects, analyzes, and disseminates alerts and incident reports to its membership, and helps the government understand impacts for that sector by relying on its sector-focused, subject matter, and analytical expertise. It provides an electronic, trusted ability for the membership to exchange and share information on cyber, physical, and all threats, vulnerabilities and incidents, in order to defend the critical infrastructure. This includes analytical support to the 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 or natural events."

■ Roles need to be more clearly defined (i.e. Sector Coordinators to ISACs and to government).

The Role of the Sector Coordinator and how to become one during the past six months has become unclear. Some believe Sector Coordinators are the means to communicate to a sector or to collect data. In many instances, Sector Coordinators are not staffed or resourced to accomplish these tasks. While many Sector Coordinators participate within their sector ISAC, some ISACs do not have a Sector Coordinator or the Sector Coordinator is not part of the ISAC structure. Properly defining the role of Sector Coordinator is important to assist in sector governance.[13]

[13] As the financial services sector has done.

Recommendations:

Embrace the following roles for ISACs and Sector Coordinators:

- The ISAC should be a central source in each sector for dissemination, sharing and communication of information on cyber, physical, and all threats, vulnerabilities and incidents in order to defend the critical infrastructure.
- The mission and role of the ISACs should serve as a conduit/focal point to the private sector for information sharing and analysis, with encouragement from the U.S. government
- Sector Coordinators, as the lead to address critical infrastructure issues and contribute to policy development. They should also monitor sector-wide vulnerability analyses for risk mitigation and provide for coordinating sector governance on critical infrastructure protection.

Government and the private sector should work to support:

- Refining of the roles and responsibilities of the Sector Coordinator.
- Clarifying of the relationship between Sector Coordinators and their ISACs, for those sectors represented by ISACs.
- Establishing criteria to determine if a critical infrastructure sector or a key asset meets the definition in Homeland Security Presidential Directive-7.

Issue 2 – The current business models for most ISACs are limiting with regard to the continuous flow of analysis and information to the members.

- □ **Various Business Model Frameworks.** Each ISAC has picked one of three general methods to achieve operations:

  - ■ **Association** — This model is driven by industry trade associations, which support the responsibilities for ISAC operations and information delivery to its members. The advantage of this model is the built-in membership base and the use of the membership list for information sharing. However, it can be difficult for a trade association's operations center to satisfy market-driven requirements and initiate an information-sharing system that covers the entire sector beyond the infrastructure already in place.

  - ■ **Government Centered** — This model is driven by government and is created to provide continuity of basic services and for coordination essential to government operations. The advantage of this approach is that the Federal Government handles the high infrastructure and operational costs. The disadvantage is that it limits the ability of the public and private sectors to share information with each other. For example, to receive government data, private sector personnel must attain government security clearances. This complicates re-assignments and the ability to adjust to rapidly changing events. In addition, the passing and storing of private, commercially sensitive data on a government system can inhibit sharing of information, especially as the ISACs move to a live data-feed and will have to share a set of mechanisms for early warning and incidents.

  - ■ **Market Driven** — This model is driven by industry and is created for the benefit of the industry sector it serves. The industry market derives usage out of value, necessity, and the need for coordination and communication. Such an ISAC is established as an independent organization and obtains funding through the membership and subscription fees it charges for access to its information. The advantage to this approach is that the organization is independent and therefore able to act in accordance to its charter — defined for the members — rather than by obligations defined by a parent entity. The charter will reflect market-driven requirements that benefit the protection of the infrastructure based on business and government needs. The disadvantage to this approach is that the cost of start-up and ongoing operations may be capital intensive, requiring a price curve that prohibits smaller organizations from joining. This limits the extent of information dissemination within a sector.

Recommendation:

Enhance reach of private sector ISACs through funding of infrastructure enhancements without delivery of private sector data or meta-data.

- Assist ISACs in delivering basic alerts and advisories to their sectors. Increase the volume of alerts and advisories for public use and consumption. Increase the alerts and advisories that have cross-sector impact or interdependencies (for example, passing an alert related to a potential cyber attack to the financial services sector, but not passing the same to the information technology sector).[14]

- Facilitate ISAC operations and leadership security clearances. To further aid in this effort, DHS should establish processes for security clearances based on the "need to know" and "need to act" to support homeland and national security. Further, various sectors have personnel in positions of leadership, which may not qualify them for attaining a clearance through other channels. This support would allow the private sector to better partner with the Federal Government.

- Provide sector-specific and broad-based strategic information, thus increasing ISAC value and government communication.

- Provide base-level resources to ISACs thus enabling the delivery of critical and urgent information (lower tier information) within each sector free of charge.

[14] As the ISACs continue to grow operationally, working with DHS and more importantly between themselves, they are becoming a larger target for surveillance from many adversaries. While clearances and secure telephones would enable a limited degree of interoperability, a commercial-grade system and key would be of greater value in opening the channel of communication and coordination. This is important not just in times of incidents and events, but also during the trust and routine operations phase, where an adversary would most likely target and learn the interdependent centers of gravity.

Sub Issue – Reported Federal Government Funding of ISACs

- Below are listed the responses from U.S. government agencies regarding federal funding support to ISACs for all years:
  - DoE -- Grant 2003 for $629K to Chemical ISAC
  - EPA -- to Water ISAC
    - Fiscal Year 2001-2002 -- $1.1 million to scope requirements and design operations.
    - Fiscal Year 2003 -- $1 million to begin operations.
    - Fiscal Year 2004 -- $2 million estimated to continue and expand operations.[15]
  - Federal Transportation Agency -- $1.2 million to Public Transit ISAC
  - Treasury Department -- $2.0 million to Financial Services ISAC

- Below are listed the responses from the private-sector ISACs regarding federal funding support from DHS or other lead federal agencies:

Sector	**2003**	**2004**	**2005**
Water	1.0 M	1.5 M	
Public Transit	1.2 M	1.2 M	
Energy	629 K	629 K	629 K
Chemical	None	Request In-process	
Surface Transportation[16]	None	None	
NCC Telecom	Government Funded	Through NCC / DISA	
Information Technology	None	None	None
Electric	None	None	None
Financial Services	None	2.0 M	None
Trucking	40 K	2.5 M (15% of Grant)	2.5 M
Health Care	None	None	

[15] This figure is under negotiation.

[16] The Seven Class I Railroads are not funded, however funding for the approximately 500 short line rail roads is under consideration for 2005.

<u>Issue 3</u> – There is a lack of government understanding with respect to the private sector's unique research and analytical capabilities.

- □ **Some ISACs can provide unique sector analysis and research**

  - ■ Private-sector owner/operators understand their unique operational problems. Creating, designing, building, and owning portions of an infrastructure provide the private sector with unique insights. Operating that infrastructure affords an added understanding to how the sector works and, more importantly, how some parts do not work. This knowledge is the basis for sector analysis and is often the springboard to further research in designing the construction of new mechanisms and processes. The government would find this body of knowledge and experience useful in analyzing problem sets. To be more effective at delivering useful information, the government needs more clarify the requirements for information/intelligence and the mechanism for funding unique deliverables — such as refined intelligence products from the private sector.

  - ■ Private-sector analysis grows with trust and communication — focused primarily on sector vulnerabilities (operational). The lines of communication continue to expand and the need for more refined data collection and analysis will expand concurrently. The government should continue to encourage the sector-to-sector communication and assist in providing the means to bring others into this circle of trust and research. The study of interdependencies between the sectors would be an appropriate starting point.

  - ■ To enable ISACs to provide refined analyses, as opposed to raw data, there must be a better understanding of government requirements for analytical products. The sectors are not just consumers of intelligence, nor are they only producers of raw information. Some ISACs have an enormous ability to study an issue and produce daily information or to generate finished analytical products, but those resources are not being fully utilized to the benefit of government or of the ISACs themselves.

<u>Recommendation:</u>

Create a two-tier information mode by incorporating private-sector analysis and focus on the government's reach and communication for alerting.

- ■ **General alerts and information** (reach). This is the first tier of information and dissemination. All non-aligned business and critical infrastructure ISACs would receive this information. It provides the early warning for alerts and notifications of incidents and potential attacks from newly announced vulnerabilities or exploits.

- ■ **Sector-specific alerts and analysis** (analytical). This level of analysis is iterative and studies process interdependencies or weaknesses within systems. ISACs would perform additional analysis and communicate issues across sectors and with the government to protect critical infrastructures. ISACs would deliver specific finished product analyses based on known information and intelligence requirements.

ISSUE 4 TAB 4

Issue 4 – The federal government has yet to establish a uniform system of collecting data from the private sector and has not made clear what type of information they want the private sector to share.

Sector-specific analysis of unique data can become actionable intelligence. However, the government has not made clear what type of information it wants from the private sector, hindering efforts by the private sector to share information. A system that clearly defines data requirements will simplify information sharing, and will also help ensure that meta-data and proprietary information is not shared by the Federal Government with others in the private sector, or otherwise misused.

Recommendation:

Provide for timely flow of unique private-sector information to government.

- The best way to ensure private-sector analytical support and information flow is for DHS to clearly define and identify its informational requirements.

- The government should request analytical support from and apply the recommendations of the private sector to be more effective.

- Enhance and develop public-private cooperation. The concept of government as a "supported organization," is a paradigm shift in thought for the government and for the private sector. The NIAC supports the belief that the nation's critical infrastructures can be best secured through public-private collaboration. Such collaboration best balances the private sector's business and security interests as well as the government's mandate of defending the nation and its supporting structures. Successful collaboration requires that the government apply resources to support the efforts of the private sector in protecting critical infrastructure.