U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

NHTSA
www.nhtsa.gov

DOT HS 812 076

October 2014

Assessment of the Information Sharing and Analysis Center Model

DISCLAIMER

Suggested APA Format Citation:

McCarthy, C., Harnett, K., Carter, A., & Hatipoglu, C. (2014, October). *Assessment of the information sharing and analysis center model.* (Report No. DOT HS 812 076). Washington, DC: National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT HS 812 076		

4. Title and Subtitle	5. Report Date
Assessment of the Information Sharing and Analysis Center Model	October 2014
	6. Performing Organization

7. Author(s)	8. Performing Organization
Charlie McCarthy, Kevin Harnett, Art Carter, Cem Hatipoglu	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
The Volpe National Transportation Systems Center, Security and Emergency Management Division 55 Broad Street Cambridge, MA	11. Contract or Grant No. DTNH22-12-V-00085 DTFH61-12-V00021

12. Sponsoring Agency Name and Address	13. Type of Report and Period
National Highway Traffic Safety Administration Office of Program Development and Delivery 1200 New Jersey Avenue SE. Washington, DC 20590	Final Report 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This report presents findings from an assessment of the Information Sharing and Analysis Center (ISAC) model, and how ISAC's are effectively implemented in other sectors. The report also explains how a new sector ISAC could be formed by leveraging existing ISAC models.

This publication supports the goal of facilitating the establishment of a cybersecurity information sharing forum in the automotive sector (Goat 2).

17. Key Words	18. Distribution Statement
Cybersecurity, NIST, NHTSA, Guidelines, Risk Management, Baseline, Use cases, Best Practices	Document is available to the public from the National Technical Information Service www.ntis.gov

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22
Unclassified		46	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Foreword

NHTSA's Automotive Cybersecurity Research Program

The National Highway Traffic Safety Administration established five research goals based on a systems engineering approach to address cybersecurity issues associated with the secure operation of motor vehicles equipped with advanced electronic control systems. This program covers various safety-critical applications deployed on current generation vehicles, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity. These goals are:

1. Build a knowledge-base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;
2. Facilitate the implementation of effective industry-based best-practices and voluntary standards for cybersecurity and cybersecurity information sharing forums;
3. Foster the development of new system solutions for automotive cybersecurity;
4. Research the feasibility of developing minimum performance requirements for automotive cybersecurity; and
5. Gather foundational research data and facts to inform potential future Federal policy and regulatory decision activities.

This report

This report presents findings from an assessment of the Information Sharing and Analysis Center (ISAC) model, and how ISACs are effectively implemented in other sectors. The report also explains how a new sector ISAC could be formed by leveraging existing ISAC models.

This publication supports the goal of facilitating the establishment of a cybersecurity information sharing forum in the automotive sector (Goal 2).

Table of Contents

Figures

Tables

List of Acronyms

ABA	American Bus Association
A-ISWG	Aviation Information Security Working Group
APTA	American Public Transportation Association
BCA	Boeing Commercial Aircraft
CERT	Computer Emergency Response Team
CI	critical infrastructure
CI/KR	critical infrastructure key resource
CIP	critical infrastructure protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISCP	Cybersecurity Information Sharing and Collaboration Program
COA	courses of action
CRADA	Cooperative Research and Development Agreements
DHS	Department of Homeland Security
DIB-ISAC	Defense Industrial Base Information Sharing and Analysis Center
DoD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
EMR-ISAC	Emergency Management and Response Information Sharing and Analysis Center
EO	Executive Order
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOUO	for official use only
FS-ISAC	Financial Services Information Sharing and Analysis Center
GCC	Government Coordinating Council
HHS	Department of Health and Human Services
HSPD	Homeland Security Presidential Directive
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
ISAC	Information Sharing and Analysis Center
ISP	Internet service provider
IT-ISAC	Information Technology Information Sharing and Analysis Center
LEA	law enforcement agency
MSC	Maritime Security Council
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCC	National Coordinating Center for Telecommunications
NCCIC	National Cybersecurity and Communications Integration Center
NCI	National Council of ISACs

List of Acronyms

NCPS	National Cybersecurity Protection System
NDA	non-disclosure agreement
NH-ISAC	National Health Information Sharing and Analysis Center
NIPP	National Infrastructure Protection Plan
NO&I	National Cybersecurity and Communications Integration Center Operations and Integration
NSA	National Security Agency
OEM	original equipment manufacturer
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PPD	Presidential Policy Directive
PT-ISAC	Public Transit Information Sharing and Analysis Center
SCC	Sector Coordinating Council
SOC	Secure Operations Center
SSA	sector-specific agency
SSP	sector-specific plan
ST-ISAC	Surface Transportation Information Sharing and Analysis Center
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TLP	threat level protocol
TSA	Transportation Security Administration
TTP	tactics, techniques, and procedures
US-CERT	United States Computer Emergency Readiness Team

Executive Summary

An Information Sharing and Analysis Center (ISAC) is a trusted, sector-specifi[1] entity that can provide a 24-hour per day and 7-day per week secure operating capability that establishes the coordination, information sharing, and intelligence requirements for dealing with cybersecurity incidents, threats, and vulnerabilities. An ISAC can serve as an industry resource by which to gather key information about cybersecurity events and issues and identify, communicate, and analyze potential impacts of such concerns to the sector.

Common Capabilities of an ISAC

An ISAC can provide important capabilities:

- **Vulnerability and Incident Information Sharing:** As their primary function, all ISACs have a process in place for gathering and disseminating information to mitigate risks to particular industry sectors. First, the ISAC receives information on cyber incidents from members or trusted sources. The information is then verified and, under the operating structure of most existing ISACs, the source is made anonymous[2] to protect the source before distribution to ISAC members. Once an incident or threat has been verified, members are alerted to provide them the opportunity to protect their own critical systems and assets against the newly identified threat.

- **Vulnerability and Threat Analysis:** An ISAC could provide the capability to support analysis and carry out fieldwork to investigate known or reported incidents, as well as zero-day attacks.[3]

- **Relationships and Possible Cross-Sector Partnerships With Other ISACs:** Most ISACs closely work with other ISACs to benefit from the collective knowledge base gained across industries. An ISAC provides a forum for communication with other cybersecurity subject matter experts within the same sector and related sectors. When there is a common threat or vulnerability to portions of a particular industry, the ISAC for that sector will provide an efficient and effective means of sharing pre-competitive information that should assist in providing solutions and mitigation strategies. The ISAC could provide a mechanism for valuable interactions with peers from other manufacturers and suppliers to share and understand non-public details of the industry threats and vulnerabilities.

[1] A sector is defined as a key part of the economy

[2] Anonymity does not apply to information that a company has a legal/regulatory responsibility to share. Its goal is to keep the information from malicious people.

[3] A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability.

- **Incident Response:** An ISAC could potentially provide incident response through the use of "incident response teams" to support discovery, forensic analysis, and recovery efforts. These teams could also provide mitigation strategies and recommendations for improving overall network and control systems security. Trusted analysis can improve an organization's incident response and guide informed decision-making on cyber security issues. If a cyberincident was to occur, it is beneficial to have the mechanisms in place so that it can be handled properly.

- **Cyber Security Training:** An ISAC could provide specialized and focused training to member organizations in order to raise the level of awareness and preparedness across the entire industry.

Summary of Conclusions

A number of ISACs have been established and are operational today, providing cybersecurity services to their members in a number of industries. ISACs exist in many critical infrastructure sectors.[4] In collaboration with their members, other ISACs, and government agencies, these ISACs provide a centralized organization that enhances the ability of the sector to prepare for, respond to, and recover from cyber threats, vulnerabilities, and incidents. The success of these ISACs is best defined by their longevity in service and the continued introduction of new ISACs in other industries, such as the latest ISAC under formation within the retail industry.

As exemplified by the retail-ISAC[5] activities, the formation of a new ISAC can be expedited by leveraging the capabilities of existing ISACs. This can also help alleviate organizational risks to setting up, managing, and operating such an entity. This approach can potentially reduce the costs of the formation and operation through the reuse and tailoring of an existing charter, membership and legal agreements, and by defining membership levels, funding, and participation based on knowledge of other ISACs. ISACs are self-defined entities.

[4] There are 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; water and wastewater systems. The transportation systems CI includes: aviation; rail (both passenger and freight), maritime, and automotive/highways. Retail-ISAC does not fall in one of these CIs.
[5] www.rila.org/rcisc/RetailISAC/Pages/default.aspx

1.0 Introduction

1.1 Purpose of This Report

An ISAC is a trusted, sector-specific entity that can provide a 24-hour per day and 7-day per week secure operating capability that establishes the coordination, information sharing, and intelligence requirements for dealing with cybersecurity incidents, threats, and vulnerabilities. An ISAC can serve as an industry resource by which to gather key information about cybersecurity events and issues and identify, communicate, and analyze potential impacts of such concerns to the sector.

ISACs exist in many critical infrastructure sectors. Leveraging the capabilities of existing ISACs can expedite the formation of a new ISAC, while also alleviating the organizational risks associated with its setup and management.

ISACs are useful when there is a benefit to be realized from sharing sector information, such as threats, intelligence data, vulnerabilities (both potential/validated), and known incidents. The threat that one industry-specific organization is facing today may very well be one that other organizations in that industry will face tomorrow; thus, mutual sharing of this information would benefit the sector at large. An ISAC would provide an industry with an information sharing capability that could allow the sector to protect itself and respond more efficiently to emerging cyber-attacks.

This report will assess how current ISACs are implemented, describe their operational models, and explain how they are formed. It will also outline an approach to establishing an ISAC based on a review of the formation and operation of current ISACs.

1.2 Background on Information Sharing and Analysis Centers

In 1998, the Clinton Administration issued Presidential Decision Directive 63 (PDD-63) [1], where the Federal Government asked each critical infrastructure sector to establish a sector-specific information sharing organization that would:

- Assess the vulnerabilities of the sector to cyber or physical attacks;
- Recommend a plan to eliminate significant vulnerabilities;
- Propose a system for identifying and preventing attempted major attacks; and
- Develop a plan for alerting, containing, and rebuffing an attack in progress and then rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

In response, the Critical Infrastructure Key Resource owners and operators established ISACs.

In 2003, Homeland Security Presidential Directive 7 (HSPD-7) [2] extended PDD-63 by directing that the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect the U.S. critical infrastructure. Ten years later, in 2013, Presidential Policy Directive 21 (PPD-21) [3] updated the national approach on critical infrastructure security and resilience. This PPD replaced HSPD-7 and aimed to create a stronger alliance between physical and cyber security and resilience of critical infrastructure with three strategic imperatives:

- Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
- Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
- Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

The same day PPD-21 was issued, President Obama issued Executive Order (EO) 13636 [4]. This EO aimed to enhance critical infrastructure cybersecurity by improving information sharing efforts among government agencies, as well as between government and the private sector, while increasing the volume, timeliness, and quality of cyber threat information sharing.

As described above, the formation of sector-specific ISACs has been used to support the security needs for many important sectors and the methods used by critical infrastructure ISACs would be useful to consider when forming a new ISAC, even in a non-critical infrastructure sector.

1.2.1 ISACs in Critical Infrastructure Sectors

ISACs have been used in other CI sectors to bring together industry and government, and to provide a means of quickly reaching those affected by cyber events. ISACs have the capability to provide comprehensive sector coverage and to reach extensively within their sectors, with other sectors, and with government to share critical information. Below, statistics provided by the National Council of ISACs illustrate a select number of the ISACs' reach within their respective sectors [5]. These ISACs are highlighted because of their maturity, increased membership over the years, and the many lessons learned and success stories to share collaboratively. Many of them are "cross-sector" ISACs (e.g., communications, information technology, multi-state, etc.) with the ability to reach CI/KR owners and operators in multiple industries. The key ISACs that will be highlighted throughout this paper include:

- **Financial Services ISAC:** It has over 4,600 members and, through 30 member associations, has the ability to reach 99 percent of the banks and credit unions, 85 percent of the securities industry, and nearly 50 percent of the insurance industry.
- **Information Technology ISAC:** Through its members, it reaches 90 percent of all desktop operating systems, 85 percent of all databases, 76 percent of the global microprocessor market; 85 percent of all routers, and 65 percent of software security.
- **Communications ISAC:** The Department of Homeland Security National Coordinating Center partners with the private sector in this ISAC to provide "24/7" operational support.

Members include communications equipment and software vendors, 95 percent of wire line communications providers, 90 percent of wireless communications providers, which includes satellite providers, and 90 percent of Internet service providers backbone networks.

- **Water ISAC:** It currently provides security information to water and wastewater utilities that service more than 65 percent of the American population.
- **Multi-State ISAC:** It includes all 50 States, the District of Columbia, four U.S. Territories, and many local governments. Additionally, the MS-ISAC continues to broaden its local government participation to include all of the approximate 39,000 municipalities.

Transportation has been identified as one of the key sectors, with four existing transportation ISACs:

- **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 percent of the North American freight railroad infrastructure.
- **Motor coach ISAC**: In 2013, the American Bus Association with support from the ST-ISAC initiated an ISAC. The ABA provides security alerts and information on a password-protected section of its Web site as appropriate.
- **Public Transit ISAC (PT-ISAC):** The American Public Transportation Association was designated by the U.S. Department of Transportation as the sector coordinator for the U.S. public transit industry. In this role, APTA created the PT-ISAC. APTA's members serve more than 90 percent of public transportation users in the United States and Canada.
- **Maritime ISAC:** This ISAC is an independent, nonprofit entity sponsored and managed by the Maritime Security Council. The Maritime ISAC works with U.S. and international maritime shipping, seaport, and government regulatory oversight communities as a trusted agent, collecting and analyzing proprietary data (stowaway rates and locations, drug seizures overseas, terrorist threats, etc.), which it then disseminates to participating industry and government constituents.

In addition, the two newest ISACs are of interest. The Aviation ISAC is currently in implementation phase and is expected to be operational by the fall of 2014. The retail ISAC has been established and launched expeditiously in 2014.

- **Aviation ISAC:** In 2012, Boeing Commercial Aircraft initiated the planning/development of an Aviation ISAC and Aviation Information Security Working Group to support e-enabled aircraft. Members include Boeing, Airbus, Bombardier, and Embraer, several trade associations (e.g., Airlines for America, Regional Airline Association, and International Air Transport Association), the Federal Aviation Administration, the Transportation Security Administration, DHS, and others.
- **Retail ISAC:** The ISAC component of the Retail Cyber Intelligence Sharing Center functions as a forum for retailers to share threat information and leading practices with each other to enhance the security of the retail industry's networks and protect consumer data. The Retail ISAC, through dedicated analysts, process and distill information about real-time

cyber threats, such as new strains of malware, underground criminal forum activity, or potential software vulnerabilities. This information is further translated into actionable intelligence, in usable and timely form for retailers. Anonymized information is also shared with Federal Government and law enforcement entities, such DHS, the U.S. Secret Service and the Federal Bureau of Investigation.

As exemplified by the Retail-ISAC activities, the formation of a new ISAC can be expedited by leveraging the capabilities of existing ISACs. This can also help alleviate organizational risks to setting up, managing, and operating such an entity. This approach can potentially reduce the costs of the formation and operation through the reuse and tailoring of an existing charter, membership and legal agreements, and by defining membership levels, funding, and participation based on knowledge of other ISACs. ISACs are self-defined entities.

2.0 One Approach to Forming an ISAC

2.1 Defining a Mission and Objective

The mission of an ISAC is to enhance the ability of the sector to prepare for and respond to cyber threats, vulnerabilities and incidents, by providing a centralized organization to monitor, disseminate information, and help mitigate cyber security risks and provide protection. The primary objective is to get accurate, actionable, and relevant critical information to the most comprehensive range of those that need the information. A strong secondary objective is to keep this information confidential and away from malicious people, as deemed necessary by the ISAC members.

In order to accomplish this mission and objectives, the ISAC would:

- Provide an effective forum for ISAC members to conduct information sharing within the particular sector, with other CI/KR organizations, and with the U.S. Government as appropriate;
- Provide analysis on relevant threats, vulnerabilities, and incidents;
- Share threat alerts, warnings, advisories, notices, and vulnerability assessments with ISAC members; and
- Provide rapid response in the case of an emergency through the ability to effectively contact and coordinate with members.

The ISAC could serve as the primary security communications channel for the sector, supporting information sharing among the ISAC members, with other ISACs, and between the ISAC and government agencies and private industry.

2.1.1 Interaction with the Federal Government

The following subsections describe the various potential roles the Federal Government has in the support of an ISAC.

2.1.1.1 Department of Transportation

With the updates to the national approach on critical infrastructure security and resilience, PPD-21 identified 16 critical infrastructure sectors and designated associated Federal sector-specific agencies, or in some cases co-SSAs. The SSA is a Federal agency or department whose role is to provide institutional knowledge and specialized expertise, and to lead/support security and resilience programs within the sector [3].

As the co-SSA for the Transportation Systems Sector (with DHS), the Department of Transportation is responsible for providing technical assistance to CI owners and operators and facilitating access to and exchange of information necessary to strengthen and protect the security of the transportation critical infrastructure.

2.1.1.2 Department of Homeland Security

The Department of Homeland Security works with industry and State, local, tribal, and territorial governments to secure critical infrastructure and information systems. DHS works to analyze and reduce cyber threats and vulnerabilities, distribute threat warnings, and coordinate response to cyber incidents to ensure the safety of computers, networks, and cyber systems.

DHS plays a vital role in securing the Nation's critical infrastructure in all sectors including transportation. DHS functions and capabilities that could support a new ISAC are described in the sections below.

DHS National Cybersecurity and Communications Integration Center

DHS operates the National Cybersecurity and Communications Integration Center, which is a 24-hour center responsible for coordinating cyber and communications warning information across Federal, State, and local governments, intelligence and law enforcement communities, and the private sector. This Operations Watch and Warning Center serves as a centralized location to facilitate activities that provide a greater understanding of cybersecurity and communications situation awareness, vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

DHS Cybersecurity Information Sharing and Collaboration Program

In 2011, DHS launched the Cyber Information Sharing and Collaboration Program to improve the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. The program incorporates government participants, ISACs and other CI/KR owners and operators to create a mechanism through which private sector partners could share data directly with government through a cross-sector secure portal.

As of May 2013, the CISCP had signed 40 Cooperative Research and Development Agreements (CRADAs), and was in the process of finalizing agreements with 66 additional entities to formalize a streamlined information sharing process. Since December 2011, the CISCP has released over 900 products containing approximately 18,000 cyber threat indicators based on information gleaned from participant submissions, open source research, and from sensitive government information [7].

The fully integrated branches of the NCCIC allow for a holistic[6] approach to addressing cybersecurity and communications issues at the operational level.

DHS National Infrastructure Protection Plan Sector Partnership Model [8]

The DHS National Infrastructure Protection Plan (NIPP) sector partnership model provides a mechanism for interaction between private and public sector partners to protect critical infrastructure and reduce security risks. This model encourages CI/KR owners and operators to identify or establish sector coordinating councils that would:

- Represent a primary point of entry for government into the sector for addressing the entire range of critical infrastructure protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between critical infrastructure owners, operators, and suppliers, and, as appropriate, with the government during emerging threats or response and recovery operations, as determined by the sector;
- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector;
- Facilitate inclusive organization and coordination of the sector's policy development regarding critical infrastructure protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements;
- Advise on the integration of Federal, State, local, and regional planning with private-sector initiatives
- Provide input to the government on sector research and development efforts and requirements

[6] "Holistic," as in "end-to-end," meaning prevention, protection, mitigation, response, and recovery efforts.

A government coordinating council is formed as a counterpart to the SCC. Its primary functions include:

- Providing interagency strategic communications and coordination at the sector level through partnership with DHS, the sector-specific agency, and other supporting agencies across various levels of government;
- Participating in planning efforts related to the development, implementation, update, and revision of the National Infrastructure Protection Plan and the sector-specific plans;
- Coordinating strategic communications and discussion, and resolution of issues among government entities within the sector; and
- Coordinating with and supporting the efforts of the SCC to plan, implement, and execute the nation's critical infrastructure protection mission.

Several of the other sector ISACs have GCCs in place and coordinate relevant cybersecurity issues with the private sector SCC and the sectors ISACs, such as:

- Communications ISAC is operated by the DHS's National Coordinating Center;
- PT-ISAC (Public Transit), TSA, and ST-ISAC (Surface Transportation) and DOT;
- FS-ISAC (Financial Services) and Department of Treasury;
- NH-ISAC (Health) and the Department of Health and Human Services;
- Aviation ISAC, DOT, and FAA; and
- EMR-ISAC (Emergency Response) and the Federal Emergency Management Agency.

The Critical Infrastructure Partnership Advisory Council provides the operational mechanism for carrying out the sector partnership structure. It provides the framework for valuable interaction between the GCCs and the SCCs, where members can freely share sensitive information and advice about threats, vulnerabilities, protective measures, and lessons learned.

2.1.1.3 Department of Justice: Federal Bureau of Investigation

PDD-63 requires the Federal Bureau of Investigation to take on a more active role in the cyber protection of critical infrastructure.

The FBI's Cyber Division's main focus is on cyber intrusions, working closely with the bureau's Counterterrorism and Counterintelligence Divisions. FBI investigators in the field can send their findings to specialists in the FBI Cyber Division's Cyber Watch command, who can look for patterns or similarities in cases. The 24/7 post also shares the information with partner intelligence and law enforcement agencies—like DHS, the Department of Defense, and the National Security Agency—on the FBI-led National Cyber Investigative Joint Task Force.

Many of the sector ISACs have formed collaboration and partnerships with the FBI's Cyber Division and Technology Cyber Intelligence Unit. A new ISAC could form a partnership with the Cyber Division to coordinate any law enforcement agency support of that sector's cybersecurity incidents.

2.1.2 Coordination with other Organizations

2.1.2.1 National Council of ISACs

One of the strengths of the ISAC 'system' is the sharing of data and lessons-learned with other related ISACs. One mechanism to share information is the National Council of ISACs [9]. Formerly known as the ISAC Council, NCI is a group of volunteer ISAC representatives who meet to develop trusted relationships among the sectors, and address common issues and concerns. Each ISAC has four designated representatives to the Council. The mission of NCI is to advance physical and cyber security of the nation's critical infrastructures by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. The NCI meets monthly via teleconference and quarterly in person to discuss current issues. In addition, through the NCI the ISACs can participate on daily "cyber calls" in order to keep abreast of pertinent matters. NCI also sponsors an annual Critical Infrastructure Protection Congress to bring together the critical infrastructure community for networking, learning, and addressing issues of concern to CI/KR stakeholders.

2.1.2.2 Partnership for Critical Infrastructure Security

The mission of the Partnership for Critical Infrastructure Security is to coordinate common CI/KR cross-sector initiatives that promote public and private efforts to help ensure secure, safe, reliable, and resilient critical infrastructure services [10]. PCIS was designated as the Private Sector Cross-Sector Council in the DHS National Infrastructure Protection Plan to provide leadership on cross-sector initiatives and critical infrastructure planning. Current PCIS membership spans across the 16 critical infrastructure sectors listed below (as defined in the Critical Infrastructure Security and Resilience directive, PPD-21), including transportation systems, which is represented by aviation, highway, motor carrier, public transit, and rail. According to PPD-21, the 16 critical infrastructure sectors are:

1. Chemical,
2. Commercial Facilities,
3. Communications,
4. Critical Manufacturing,
5. Dams,
6. Defense Industrial Base,
7. Emergency Services,
8. Energy,
9. Financial Services,
10. Food and Agriculture,
11. Government Facilities,
12. Healthcare and Public Health,
13. Information Technology,
14. Nuclear Reactors, Materials, and Waste,

15. Transportation Systems,[7] and
16. Water and Wastewater Systems.

2.2 Scope Considerations for the Formation and Operation of an ISAC

The ISAC functions to consider are covered below.

- Key Services
- Vulnerability and Threat Analysis and Incident Response
- Risk Assessments
- Cyber Security Training
- Cyber Security Working Groups

2.2.1 Key Services

Many of the other industry ISACs offer key services outlined in this section to their members in order to promote information sharing and awareness to prepare for and respond to cyber threats and vulnerabilities. The following topics are described below.

- Vulnerability and Incident Information Sharing
- Threat Level Protocol and Sensitivity Criteria Levels
- Severity Levels and Data Confidence
- Alert Indicator Levels

2.2.1.1 Vulnerability and Incident Information Sharing

The ISAC would first create a process for gathering information from members or trusted sources. Sources can include Government agencies like DOT, DOJ, DoD, DHS, Computer Emergency Response Teams, manufacturers, suppliers, academic sources, or ISAC members. Other sector ISAC members, or State/local law enforcement or intelligence agencies can also be trusted sources. An urgent point of contact would ideally be established, with a triage mechanism in place, so that users know who to contact in the event of a cyber-incident. Once information has been gathered, the vulnerabilities may be anonymized before distribution to ISAC members.

Information that has been gathered would then be categorized to ensure its distribution to the correct and target audience. Examples of target audiences include:

[7] The transportation systems CI includes aviation, rail (both passenger and freight), maritime, and automotive/Highways.

- **Operational individuals:** Individuals responsible for applying patches, configuration changes, or other changes to critical infrastructure components;
- **Management:** Individuals responsible for analyzing technical and business issues that determine the applicability and timing for operational action; and
- **Executives:** Individuals responsible for analyzing high level technical and business risk issues and determining appropriate response and communications.

2.2.1.2 Threat Level Protocol and Sensitivity Criteria Levels

The FS-ISAC Threat Level Protocol Matrix [11] could be tailored for the sector to ensure that information is shared with the correct audience. The TLP matrix was developed by the FS-ISAC, but it is used by many other ISACs. The TLP uses a set of four colors to indicate different degrees of sensitivity and sharing considerations, as shown in Table 1. The originator of the information should label that information with the appropriate TLP classification.

Table 1: FS-ISAC Threat Level Protocol Matrix

Classification	Target Audience
Red	Restricted to a defined group (e.g., only those present in a meeting or recipient of defined group.) Information labeled RED should not be shared with anyone outside of the group.
Yellow	This information may be shared with ISAC members, generally kept behind the ISAC secure portal.
Green	Information within this category may be shared with ISAC members and partners (e.g., DHS, other government agencies and other ISACs). Information in this category is not to be shared in public forums.
White	This information may be shared freely and is subject to standard copyright rules.

This safeguarding is to protect sensitive data based on who should have access to it and how much harm would be done if it were disclosed. A sensitivity level ranging from one to four could be used [12] in order to control distribution to the appropriate audience, as shown in Figure 1.

Sensitivity determines the individual vetting level required for any person receiving the data, where members must complete a corresponding background check to receive data from a given level. ISACs routinely have a vetting process in place to deal with trusting data and properly label it.

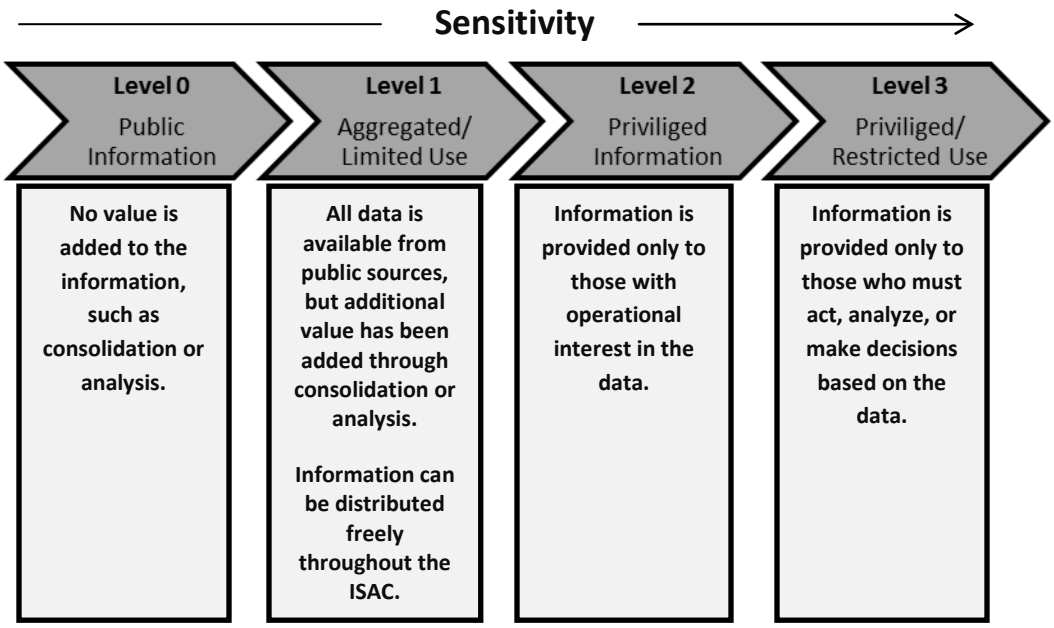

Figure 1: Sensitivity Level Criteria

2.2.1.3 Severity Level Criteria and Data Confidence Levels

The data categorization described in Section 2.2.1.2 ensures that information is available to appropriate and target audiences; however, information must also be categorized to determine the severity and confidence level (measure of reliability) to ensure the appropriate response and timing of distribution. Data severity level indicates the potential impact of the information and the need for timely action. Table 2 shows the severity conditions that could be assigned to information before dissemination [12].

Table 2: Severity Level Criteria

Severity Condition	Requirements
0 **Information Only**	Routine traffic of interest, does not require alert
1 **Awareness**	Reflects the normal determined, global, 24/7 attacks experienced by all infrastructure segments
2 **Vigilance**	Requires increased vigilance/action due to focused, patterned attacks
3 **Action**	Requires immediate action due to an increase in attacks
4 **Urgent Action**	Requires immediate, decisive action. Reflects a potentially catastrophic problem for an infrastructure segment (or group of infrastructure segments)

Assigning a confidence level to the information validates the reliability of the source and information, and in some cases allows information to be distributed timely before full analysis is complete. Data can be assigned a confidence level of high, medium, or low, as shown in Table 3. While the data confidence level is a useful tool in categorizing the information, it should not be used as a substitute for providing additional assessment.

Table 3: Data Confidence Levels

Confidence Level	Degree of Certainty
High	Greater than 90%
Medium	50-90%
Low	Less than 50%

2.2.1.4 Alert Indicator Levels

All ISACs provide alerts to their membership once an incident or threat has been verified. These alerts allow those within the ISAC to receive timely information designed to help protect their critical systems and assets. Basic alerts would provide members with a description of the incident, its severity level, and potential solutions to mitigate impact. A new ISAC could adopt the alert indicator used by the MS-ISAC [13], which shows the current level of malicious cyber activity, and reflects the potential for, or actual damage. Table 4 shows the five levels used to categorize alerts.

Table 4: MS-ISAC Alert Indicator

Alert Level	Definition
Low	Insignificant or no malicious activity has been identified
Guarded	Malicious activity has been identified with minor impact
Elevated	Malicious activity has been identified with a moderate level of damage or disruption
High	Malicious activity has been identified with a major level of damage or disruption
Severe	Malicious activity has been identified with a catastrophic level of damage or disruption

Tailored alerts are also useful because not all members need or want to know about the same types of issues. Members would create a cybersecurity profile, which would specify areas of particular interest and level of service, or opt to receive all alerts. Then, information would be delivered based on members' cyber security profiles. A new ISAC could provide both basic alerts and tailored alerts.

2.2.2 Vulnerability and Threat Analysis and Incident Response

Once an ISAC is established, an operating structure that can be used to gather information regarding potential cyber incidents and to provide alerts based upon quantified incidents, can be set up.

After information has been gathered, a mechanism would ideally be in place to analyze the information. The new ISAC could provide the capability to support analysis and carry out field work to investigate known or reported incidents, as well as zero-day attacks, which exploit a previously unknown vulnerability.

A new ISAC could partner with other organizations, like ICS-CERT or US-CERT, or develop an internal cyber testing lab to provide services such as testing of viruses/malware, performing penetration testing of systems, and assessing the impact of cyber-attacks. In the long-term, the new ISAC could establish incident response teams to respond to cyber threats and vulnerabilities that are industry-specific or deploy the ICS-CERT teams (if needed).

2.2.3 Cyber Security Training

ISACs are not unique for providing training but focused, sector-specific cyber security training is a service that could be offered to members as a way to mitigate risks. Training can either be performed by the ISAC, or outsourced to external firms, and is necessary to increase cyber awareness within the industry. Guides and other resources could be available to further the education and awareness of cyber security issues in the industry.

2.2.4 Cyber Security Working Groups

Many of the existing ISACs have instituted special interest working groups, based on member needs, dedicated to a specific topic. These special working groups would allow members to concentrate efforts where necessary.

2.3 Forming an ISAC

2.3.1 Common Elements

Common elements for forming an ISAC are considered next and include:

- Board of Directors,
- Funding Model,
- Information Collection and Distribution,
- Secure Operations Center and Portal Environment Capabilities, and
- Vetting Individuals and Organizations.

For more detailed information, see the Water ISAC-NCI Survey Results table in Appendix C. This table contains the responses to a 2013 survey conducted by NCI, where Council members were asked to provide information about their respective ISAC structures, membership, and operations. The information gathered provides detail to allow members to compare and contrast their ISACs on a basic level. For instance, if a sector ISAC, seeing that the Water-ISAC has members in other countries, might wish to learn how the Water-ISAC compartmentalizes its portal to prevent access by non-U.S. members to certain “For Official Use Only”-marked information. This information could assist a new ISAC to better understand and possibly leverage the capabilities that have been developed by other ISACs.

2.3.1.1 Board of Directors

ISACs typically set up a board of directors comprised of five to ten elected representatives from the membership, which would include a president and vice-president. The board provides strategic direction

to the ISAC management team. The board also determines member eligibility, enforces member eligibility verification, and provides oversight of the operation of the ISAC.

2.3.1.2 Funding Model

ISACs are typically funded in any combination of three sources: membership dues, Federal funding/grants, and subsidies from private sponsors. A number of key sectors have either complete or partial Federal funding for ISAC operations.

Membership dues for ISACs typically range annually from $1,000 to $50,000. The membership fees would depend on the services provided (and could be based on annual revenues of the member companies). Many ISACs provide basic information sharing services at no cost, while other services such as monitoring and assessments are provided fee-for-service.[8] Dues could also be based on the level of membership, in order to make membership more attractive to smaller firms.

As an example, the minimum guidelines to join the FS-ISAC are shown in Table 5 below. In this case, a firm's membership level is based on its assets and revenue [14].

Table 5: FS-ISAC Membership Guidelines

Membership Level	**Core $850/yr**	**Standard $5,000/yr**	**Premier $10,000/yr**	**Gold $24,950/yr**	**Platinum $49,950/yr**
Financial Institutions, Insurance Companies and Securities/Brokerage Firms	Assets: $1B - $10B	Assets: $10B - $20B	Assets: $20B - $100B	Assets: $100B - $250B	Assets: > $250B
Processors and Utilities	Revenue: < $100M	Revenue: $100M - $1B	Revenue: $1B - $2.5B	Revenue: $2.5B - $5B	Revenue: > $5B

2.3.1.3 Information Collection and Distribution

Characteristics Common to All ISACs:

- Method to maintain privacy and anonymity: verifiable process for accepting incidents, and determining who has access once accepted;

[8] For example, a comparison of various services provided to each level of membership in the FS-ISAC can be found at www.fsisac.com/join. Tiered membership meets the needs of many industries (e.g., first- and second-level suppliers and some academia organizations would not need the complete set of services and they would have a lower membership annual dues and commensurately less services provided).

- Method for data categorization: verifiable process for categorizing incident data/reports, and determining who has access;
- Incident data from external sources: quantifiable process to determine if an incident applies to the ISAC scope, and a framework to analyze data and determine its validity and how it impacts the sector; and
- Incident data from members: Secure e-mail or portal through which to share suspicious activity and security incident reports.

Additional Characteristics to Consider:

- Will incidents be published to a portal/Web site for archiving?
- Will response resources (e.g., malware analysis, forensics, code analysis, mitigation recommendations) be available?
- What means will be used to disseminate information to members (via secure Web site portal, public Web site, mass email/phone call/text message, etc.)?
- What products will be available (e.g., newsletters, threat alerts, library of documents/reports, webcasts/webinars, training, conferences, daily analytical reports)?

2.3.1.4 Secure Operations Center and Portal Environment Capabilities

All ISACs typically have some type of secure computer environment capabilities to securely share and manage data.

Characteristics Common to All ISACs

- Secure computer environment (e.g., portal) to manage, store, and receive information and products and securely disseminate information to members
- Ability to identify participants and personnel that are cleared to receive and analyze classified information (e.g., with DHS and/or DoD)
- Resiliency and redundancy measures to ensure accuracy and integrity of data
- Internal and external audits to ensure and verify the security of SOC processes and activities

Additional Characteristics to Consider

- Will activities be outsourced or handled internally within the ISAC?
- Will a physical operations center be staffed in person 24/7?
- How many full-time employees will be necessary? What about contract support?

2.3.1.5 Vetting Individuals and Organizations

Information must be available to all appropriate (based on membership definitions) parties, yet it must be protected (i.e., kept out of hands of malicious people, and not arbitrarily re-distributed to unauthorized individuals). Therefore, information should only be distributed to sponsored individuals in vetted organizations. Most ISACs have some mechanism in place to ensure anyone receiving information

has been properly vetted. Individuals should have some level of background check completed before they are able to receive shared information.

2.3.2 Leveraging Existing Resources

Many applicable capabilities from other existing ISACs could be leveraged to reduce the costs and reduce the time to set up and operate an ISAC. Four are covered below.

- Charter
- Web site and Portal Management
- ISAC Information Protocol Exchange
- Specific Capabilities from the FS-ISAC

2.3.2.1 Charter

An organization's charter describes the scope, objectives, and participants of the organization. ISACs generally have a charter, which could contain the following information: background, purpose, mission, membership composition, leadership, roles/responsibilities, costs, and membership fee structure, working groups/subject matter experts, meetings/teleconferences schedule, and information exchange protocol. An existing ISAC charter can easily be tailored to meet the needs of the industry in question.

2.3.2.2 Website and Portal Management

One particular existing capability that would be beneficial to use to reduce setup costs is a Web site/portal management system to share threat/vulnerability information. While most ISACs have created their own secure portals, others use commercially available collaboration platforms like Microsoft SharePoint. Several ISACs have begun using an anonymity-based cross-sector portal. NCI has signed a letter of intent to use a specific platform and recommend its use to its members. So far, six ISACs have signed on to use the recommended portal and four more are expected to sign on soon. In addition, the FBI and DHS also plan to join the same portal and submit threat information.

2.3.2.3 ISAC Information Protocol Exchange Capability

Currently, much of the process used to review cyber threat data, such as comparison, is completed manually by cyber security analysts, which takes a great deal of time and effort. However, as the information is mainly coming from trusted sources, most of this data should be able to be vetted automatically using computer systems that conform to certain protocols, described below. In an effort to standardize the language used to securely exchange threat information, the NCI is supporting the implementation of MITRE's Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information [15], described below.

Structured Threat Information Expression

STIX is an open community effort sponsored by the DHS Office of Cybersecurity and Communications. It provides a common language for describing cyber threat information so it can

be shared and stored consistently to facilitate automation. STIX characterizes an extensive set of cyber threat information, to include:

- Indicators of adversary activity (e.g., IP addresses and file hashes);
- Adversary tactics, techniques and procedures;
- Exploitation targets; and
- Courses of action.

Together, this information more completely characterizes the cyber adversary's motivations, capabilities, and activities, and thus, how to best defend against them.

Trusted Automated Exchange of Indicator Information

As the main transport mechanism for cyber threat information represented using the STIX language, TAXII allows organizations to share the information in a secure and automated fashion. It defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries.

STIX and TAXII allow for information to be described and distributed in an automated and relatively easy manner. Both STIX and TAXII are being used operationally on a daily basis by several ISACs, such as the FS-ISAC, IT-ISAC, and the Defense Industrial Base ISAC. By using a uniform standard to communicate and share information, the ISAC can more readily absorb, analyze, and share information to allow for earlier detection, understanding, and preparations. A new ISAC could work with the NCI to implement this capability.

2.3.2.4 Specific Capabilities from the Financial Services ISAC

The FS-ISAC was formed in 1999 with only six member companies and has grown to over 4,600 members. This ISAC has built up a large member base, procedures, and infrastructure that have been adapted by many of the ISACs over the years. Currently the FS-ISAC leadership is working closely with other sectors, to assist them with the planning and implementation of their sector ISACs.

As the most mature ISAC, the FS-ISAC can provide valuable tools and documents to guide the formation of an ISAC.

Tools

- **TLP Matrix**: a set of four colored indicators showing different degrees of sensitivity to ensure information is shared with the correct audience.
- **Secure Portal:** FS-ISAC has developed a cyber-intelligence information sharing repository that supports the DHS automated intelligence sharing protocols, STIX, and TAXII, and supports the goal of a national centralized network for sector and cross-sector cyber intelligence information sharing.

Documents

- Several documents developed by the FS-ISAC could be tailored when forming a new ISAC, such as the ISAC charter, non-disclosure agreements, and the board of directors structure. Other industries such as IT, health, multi-State, aviation, and oil and natural gas[9] have successfully leveraged these documents to form their sector ISACs.

2.4 Potential alternatives to forming a sector-specific ISAC

Potential alternatives to creating an ISAC could include:

- *Using a master electronic mail subscription service* (such as LISTSERV[10]). This could facilitate relevant cyber information to be sent to interested stakeholders. While this approach could implement an interim solution for information dissemination among participants, effective management of secure, layered and scalable communication flow for stakeholder participation is not well defined in this approach unlike the case with the ISAC model. Further, it would be a challenge to influence other ISACs to share intelligence information with this service.

- *Industry members (of a sector without an ISAC) joining an existing ISAC established in another sector for a nominal annual fee.* This could be an interim step or a longer-term solution for a sector depending on the fit. The challenge would be to identify an existing ISAC model that is designed for one specific sector to work for another sector. As described in this document, ISACs are self-defined entities and its functions are catered to the needs of its founding sectors.

3.0 Conclusions

The mission of an ISAC, in collaboration with the members, other ISACs, and other government agencies, would be to enhance the ability of the sector to prepare for, respond to, and recover from cyber threats, vulnerabilities and incidents. This could be achieved by providing a centralized organization to monitor and disseminate information; to help mitigate cyber security risks; and to provide protection expeditiously to as many industry participants as possible.

ISACs are widely used tools to address cybersecurity through increased communication and collaboration among the stakeholders in an industry sector. Many aspects of an ISAC already exist in other industries (including those designated as critical infrastructure). The successful implementation of these ISACs in those sectors suggests that many of the aspects of the existing ISACs could be adopted for use in other industry sectors. This can also help alleviate organizational risks to setting up, managing,

[9] See www.ongisac.org as an example of the new oil and natural gas ISAC that has been based on the FS-ISAC model.

[10] LISTSERV is the original automatic e-mail list management software.

and operating such an entity. This approach can potentially reduce the costs of the formation and operation through the reuse and tailoring of an existing charter, membership and legal agreements, and by defining membership levels, funding, and participation based on knowledge of other ISACs.

Appendix A: Works Cited

[1] Presidential Decision Directive 63 (PDD-63): Policy on Critical Infrastructure Protection, 63 FR 41804, 1998. Available at www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865

[2] Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, 2003. Available at www.dhs.gov/homeland-security-presidential-directive-7

[3] Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, 2013. Available at www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[4] Executive Order 13636: Improving Critical Infrastructure Cybersecurity, 78 FR 11739, February 19, 2013. Available at www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[5] National Council of ISACs. (2009, January). The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection. Retrieved from www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf.

[6] Department of Homeland Security. (2013). About the National Cybersecurity and Communications Integration Center. Retrieved from www.dhs.gov/about-national-cybersecurity-communications-integration-center

[7] Written testimony of NPPD Office of Cybersecurity & Communications Acting Assistant Secretary Roberta Stempfley, and National Cybersecurity and Communications Integration Center Director Larry Zelvin for a House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies hearing titled “Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities.” (2013, May 16). Available at www.dhs.gov/news/2013/05/16/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-hearing

[8] Department of Homeland Security. (2013 Critical Infrastructure Sector Partnerships, 2013. (Web page). Available at www.dhs.gov/critical-infrastructure-sector-partnerships. [Accessed October 2013].

[9] D. Anderson. (n.a.) *Information sharing initiatives in critical infrastructure protection and resilience*. National Council of ISACs.

[10] National Sheriffs Association. (2011, November 11). Partnership for critical infrastructure security. Retrieved from www.sheriffs.org/content/partnership-critical-infrastructure-security

[11] Financial Services ISAC. (2011, May). Overview of the FS-ISAC. Retrieved from www.fsisac.com/sites/default/files/FS-ISAC_Overview_2011_05_09.pdf

[12] National Council of ISACS. Vetting and trust for communication among ISACs and government entities. (2004, January 31). Retrieved from www.isaccouncil.org/images/Vetting_and_Trust_013104.pdf

[13] Center for Internet Security. (2013) . Multi-State Information Sharing & Analysis Center. Retrieved from http://msisac.cisecurity.org/alert-level/

[14] Financial Services Information Sharing and Analysis Center. (2013). Membership benefits. Retrieved from www.fsisac.com/join

[15] MITRE Corporation. (2012). STIX: Structured threat information expression Retrieved from http://stix.mitre.org/index.html

Appendix B: Vehicle Cyber Security Incidents Table

Vehicle Cyber Security Incidents

Date	Article Title	Incident Category	Description of the Incident and/or Article	Hyperlinks
4/3/2013	Long Beach police stumped by car thefts	Car Theft	An unknown handheld device, possibly a scanner to try many vehicle remote signals, is used to steal cars by disabling the alarm and unlocking the doors.	http://abclocal.go.com/kgo/story?section=news/state&id=9053653 http://ktla.com/2013/04/04/high-tech-car-burglars-strike-in-long-beach/#axzz2TwNlVdF3 http://news.msn.com/science-technology/high-tech-car-thieves-break-into-vehicles-without-leaving-a-trace
12/28/2012	Pirate radio jammed keyless car entry systems	Unintentional	A pirate radio station was jamming the signal certain cars were using for their keyless fobs. It is unlikely the operator of the radio station knew that he was blocking signals.	www.sun-sentinel.com/news/broward/hollywood/fl-pirate-radio-hollywood-20121229,0,5142922.story
12/3/2012	Engine Computer Hackers Show You How To Disable The VW Golf R's Stability Control	DIY, Performance Enhancing Community	This article describes how to disable stability control to allow for drifting and engine tuning in order to change speed thresholds.	http://jalopnik.com/5965289/engine-computer-hackers-show-you-how-to-disable-the-vw-golf-rs-stability-control
10/26/2012	Denial of Service (DoS) to phones, Ford Edge		Two Wi-Fi chips with a validation error in their firmware have enabled a DoS exploit that makes the affected device unable to send or receive Wi-Fi signals, including the Wi-Fi built into a Ford Edge.	http://arstechnica.com/security/2012/10/dos-vulnerability-affects-older-iphones-androids-even-a-ford-car/ http://clickfortechnology.com/2012/11/in-the-iphone-4-found-dangerous-vulnerability.html
10/17/2012	Programming a Replacement Keyless Entry Remote	DIY	This do-it-yourself article describes how to reprogram key fobs to work on multiple vehicles.	http://filear.com/?p=131

Date	Article Title	Incident Category	Description of the Incident and/or Article	Hyperlinks
8/6/2012	Car-hacking: Remote access and other security issues	Disgruntled Spouse/Employee, Car Theft, Insider Attack	This article describes several different reports of car hacking, including a former employee who remotely disabled dealership-leased vehicles, BMW thefts in the UK, and the future possibility of increased car hacking.	http://geinvestigations.com/blog/tag/arizona-department-of-public-safety/
7/8/2012	BMW Fob Hacking Allows Theft	Car Theft	This article describes how key fobs can be cloned to break into/steal cars.	www.neowin.net/news/bmw-security-flaw-allows-theft-in-180-seconds-or-less www.obd2be.com/car-key-programmer-c-8.html http://nakedsecurity.sophos.com/2012/09/18/bmw-stolen-hacking-kit/ http://forums.overclockers.co.uk/showthread.php?p=18402066
7/27/2011	War Texting' Lets Hackers Unlock Car Doors Via SMS		A technique called “war texting” is used to unlock doors or start a car via mobile phone apps such as GM’s OnStar. The article also mentions similar apps for BMW and Mercedes.	www.csoonline.com/article/686802/-war-texting-lets-hackers-unlock-car-doors-via-sms www.blackhat.com/html/bh-us-11/bh-us-11-briefings.html#Bailey
5/3/2011	Hacker hacks police cruiser and lives to tell tale	Man in the Middle Attack	A man tapped into police car video systems to record and stream A/V from cameras on cars, as well as control the DVR.	www.theregister.co.uk/2011/05/03/cop_car_hacking/
4/26/2011	Enhance your key fob via CAN bus hacking	DIY, Performance Enhancement Community	An Arduino board with CAN interface shield can allow a key fob to roll car windows up/down.	http://hackaday.com/2011/04/26/enhance-your-key-fob-via-can-bus-hacking/

Date	Article Title	Incident Category	Description of the Incident and/or Article	Hyperlinks
1/6/2011	Car Theft by Antenna	Man in the Middle Attack, Car Theft	This article describes research done by ETH Zurich in Switzerland, where cars were remotely started by intercepting the signal between the car and the wireless keys. They reproduced the signal and tricked the cars into starting.	www.technologyreview.com/news/422298/car-theft-by-antenna/
9/16/2010	Real world Cyber-attack case #1	Disgruntled Spouse/Employee	A man plants a device in his ex-wife's and ex-mother-in-law's car. The lighter-sized device tracked the vehicles using GPS and, via a cell phone command, could turn on and off fuel to the engine.	
6/12/2010	The Top 4 Newest Trends For Car Thieves	Odometer Fraud, Carjacking, Component Theft, Car Theft	This article describes four popular auto-related crimes: odometer fraud, car cloning where stolen cars get a VIN number from a legitimate vehicle cloned to them, component theft, and standard carjacking.	http://autos.aol.com/article/new-car-theft-trends/
4/20/2010	Local computer security expert investigates police practices		A man obtains supposedly deleted video recordings taken in a police vehicle.	www.seattlepi.com/local/article/Local-computer-security-expert-investigates-887914.php#page-1
3/17/2010	Hacker Disables More Than 100 Cars Remotely	Disgruntled Spouse/Employee, Insider Attack	A former employee uses a remote immobilization system to disable 100 cars and set off horns.	www.wired.com/threatlevel/2010/03/hacker-bricks-cars/

Appendix C: Water ISAC – NCI Survey

Water ISAC – NCI Survey

ISAC Name (Coded for Anonymity)	In what year did you begin operations?	Type of Organization	What are your core areas of focus? (Select all that apply.)				What is your annual budget?	What are your two or three largest sources of revenue, including Federal funding?
			Physical infrastructure security	Cybersecurity	Emer Mgt & Response	Other or Add'l Information		
1	1999	A stand-alone non-profit organization.	Y	Y	Y		$1 million+	Member Dues, Conferences/ Sponsor Support
2	2001	A stand-alone non-profit organization.		Y			Under $1 million	100% Member funded
3	2004	Service of for-profit corp.		Y			N/A	Federal, State, local
4	2011	A stand-alone non-profit organization.		Y				Membership Funds
5	2004	Service of an association.	Y	Y				Federal Grant Funding
6	2003	Service of an association.	Y	Y		Physical is primary but we include the other two listed, as well as overseas awareness and terrorism and also weather events.	Unable to answer at this time (less than $200K)	Member association annual dues
7	2003	A community of institutions.		Y			$900,000	Membership dues; private subsidy
8	2005	Service of for-profit corp.	Y			Theft awareness	$95,000	No Federal Funding/ Subscriptions
9	2002	A stand-alone non-profit organization.	Y	Y	Y		$1,160,000	Member dues, Federal memberships

ISAC Code	How many FTEs (including contract support) do you have?	Which of these functions does your contract support have primary responsibility for? *Not just engaged in.* (Select all that apply.)					Do you have a physical operations center that is staffed in person 24/7?	How do you disseminate your information to your members, including urgent threat alerts? (Select all that apply.)						
		General mgt	Web site/portal mgt	Threat analysis	Information dissemination to members	Other or Add'l Info		A secure Web site portal	A public Web site	Mass e-mail	Mass phone calling (aka robo-calling)	Mass text messaging	Twitter	Other (please specify)
1	14, will grow to at least 18 in 2013					Conference program and some special interest groups Special interest group needs	N	Y	Y	Y	Y			
2	3	Y	Y	Y	Y		N	Y		Y				
3	26	Y	Y	Y	Y	Incident Response, Network Monitoring, Vulnerability Assessments	Y	Y		Y	Y	Y		Phone calling and texting functionality begin later this month.
4	7		Y	Y	Y		N	Y		Y				
5	3					NA	N	Y		Y				
6	1.5 FTEs, 1 FTE, the .5 is a mixture of time for 3 individuals						N	Y		Y				
7	6						Y	Y	Y	Y			Y	
8	2 FTEs/support from 24/7 Monitoring group/1 IT Contractor		Y				Y		Y	Y				
9	3.5		Y	Y	Y		N	Y		Y				

ISAC Code	Is your membership comprised of individuals, organizations with designated representatives or both?	How many individuals have memberships in your ISAC?	How many organizations have memberships in your ISAC?	Do you have membership tiers where one tier gets one set of services while others get lesser sets?	What is your range of membership fees?	Do you use HSIN or another government owned and operated portal as your ISAC portal? If not, what portal technology/ software do you use?		Are members vetted or screened to ensure they have a need-to-know qualification to receive your materials or have access to your portal?	Are members required to consent to some sort of confidentiality or non-disclosure agreement?	Do you allow individuals or organizations in other countries to be members?
1	Orgs, with designated individuals.	N/A	4,300	Y	0-$50k	N	Moving to NC4 in 2013	Y	Y	Y
2	Orgs, with designated individuals.	0	About 25	Y	$3,000-25,000	N	We used in house resources.	Y	Y	Yes. The Board has formal policies for evaluating membership, including whether admission of an applicant would hurt trust.
3	Orgs, with designated individuals.		350	Y	Basic services are provided at no cost. Other services (monitoring, assessments, etc.) are provided on a fee-for-service basis.	Y	Gov't portal	Y	Y	N
4	Orgs, with designated individuals.	0	50	N	Free-$50,000	N	Proprietary portal	Y	Y	N
5	Both	2000	200	N	Membership is free.	N	Internally designed secure Web site and database	Y	Y	International members do not have access to secure Web site and database. Document distribution is limited.
6	Both	this is in transition at this time	9 associations	N	Flat fee, $20K annually	N	SharePoint	Y	Y	N
7	Orgs, with designated individuals.		370	Y	$700 to $900; although going up significantly in the coming year	N	Wiki	Y	Y	"Five Eyes" (AU, CA, NZ, UK, US)
8	Both	2612	797	N	$0-$500.00	N		Y	N	Canada
9	Both	8,000 in the lower service tier	1,560 orgs in the upper service tier (3,700 Individuals in these orgs)	Y	$0-$7,000	N	Internally designed secure Web site and database	Y	Y	"Five Eyes" (AU, CA, NZ, UK, US); limited FOUO information is available to them.

ISAC Code	Products of your ISAC (Select all that apply.)							Which is the HIGHEST classification level of information you generally share with your members?	Do you use the traffic light protocol when sharing info with members?	Is your portal mobile friendly?
	Newsletters	Threat alerts	Library of documents, reports, guides, etc.	Webcasts	Training	Conferences	Others (please specify)			
1	Y	Y	Y	Y	Y	Y		Unclass/FOUO	Y	Y
2	Y	Y					Daily analytical reports, weekly tech calls, twice a month Special Interest Group calls	Unclass/FOUO	N	
3	Y	Y	Y	Y	Y	Y	Incident Response, Network Monitoring, Vulnerability Assessments, etc.	Secret	Y	N
4	Y	Y	Y	Y	Y			Unclass/FOUO	N	Security certificates are setup so that mobile is not an option.
5	Y	Y	Y	Y				Unclass/FOUO	Y	N
6		Y	Y				Coordination events for local, State and Federal exercises, training, meetings and events	Unclass/FOUO	Y	N
7		Y	Y	Y	Y	Y	Daily Watch Report, Feeds of threat indicators, Mailing list, IRC communications, Special Interest Groups, Security Event Information Sharing	Confidential	Y	N
8		Y			Y		Two weekly Cargo Theft bulletins includes incident information, training event info, industry news, Advisories	Unclass/FOUO	N	We are currently in the process of upgrading
9	Y	Y	Y	Y	Y		Biannual threat analysis; risk assessment tools; various databases	Unclass/FOUO	N	Our new portal will be mobile-friendly.

ISAC Code	If your portal is *NOT* HSIN-based, what user authentication methods are in place? (Select all that apply.)					From which Federal agencies do you regularly receive threat information? (Select all that apply.)							
	Strong Password	90-day password reset requirement	RSA Tokens/Keys or similar	"Regular" username and standard password	Others or Add'l Information	DHS	CIA	FBI	TSA	DOD	HHS/ CDC	DOE	Others
1	Y		Y			DHS		FBI		DOD			Various others
2					We create and issue certificates	DHS							
3	Y		Y			DHS		FBI					
4	Y		Y			DHS							Various
5	Y					DHS		FBI	TSA				Federal, State and local law enforcement entities/ agencies
6	Y					DHS		FBI	TSA				NCTC (not as regularly and via fusion centers)
7	Y					DHS		FBI					
8		Y		Y				FBI					Various
9	Y	Y				DHS		FBI					

ISAC Code	Which of the following are your PRIMARY sources of content (e.g., threat information, papers, guides, news, etc.)? (Select all that apply.)								Do you invite your members to share suspicious activity and security incident reports directly with your ISAC?	As a matter of routine, do you share suspicious activity and security incident reports with government law enforcement or intelligence entities?			
	Federal govt. agencies	Non-govt. publicly accessible sources	Private intelligence collection and analysis firms	Other ISACs	Fusion centers	Other State or local law, intel or emergency management government agencies, excluding fusion centers.	We author our own products.	Your own members		Yes, but only with permission of the source or entities involved	Yes, and without needing the such permissions	N	Other (please specify)
1	Y	Y	Y	Y				Member incident submissions, threat viewpoint whitepapers, listserv information from members	Y	Y	Y		According to Traffic Light Protocol
2	Y	Y		Y					Y	Y			
3	Y	Y	Y	Y	Y				Y	Y	Y		Depends on the circumstances.
4		Y		Y					Y	Y			
5	Y	Y				Y	Y		Y	Y			
6	Y	Y	Y		Y				Y			N	We do not routinely share partner info with the government but if we do it is coordinated
7	Y	Y	Y				Y	Y	Y	Y			
8		Y	Y	Y	Y	Y	Y	Members can post incident information	Y		Y		
9	Y	Y		Y	Y		Y		Y			N	Case-by-case basis, with permission from provider.

ISAC Code	Do you participate in intelligence/threat analyst briefings with Federal intelligence, analysis or law enforcement agencies?		Which marketing tools do you use to attract new members? (Select all that apply.)										
	Yes, regularly	Yes, irregularly	Print advertising	A booth at conferences	Conference presentations	One-on-one meetings/calls	Earned media (e.g., articles in industry magazines)	Communication within our own association members	Endorsements by other organizations in the sector	Procured mailing lists	Facebook	Twitter	Others
1	Y			Y	Y	Y		Y	Y	Y			
2		Y			Y	Y	Y	Y	Y				Member referrals
3	Y			Y	Y	Y							
4	Y			Y	Y	Y	Y	Y	Y		Y	Y	
5	Y				Y			Y	Y				
6		Y				Y							
7		Y		Y	Y			Y	Y				
8	Y				Y	Y		Y					Linkedin
9		Y			Y		Y	Y					

ISAC Code	Which TWO or THREE of these marketing tools have been especially successful?										If you offer trials or special incentives, please describe them.	If you use marketing strategies other than those mentioned here, please tell us about them.	If you have anything additional to share, please do!
	Print advertising	A booth at conferences	Conference presentations	One-on-one meetings and/or calls	Earned media (e.g., articles in industry magazines)	Communication within our own association members	Endorsements by other organizations in the sector	Direct e-mail	Facebook	Other			
1			Y	Y							6-month free trial		
2			Y		Y						Legal documents do not permit this		
3		Y	Y	Y									
4			Y	Y		Y					None but maybe a discount if the organization signs up for 2 years as opposed to 1.		
5			Y			Y	Y						
6				Y									
7						Y	Y						
8			Y			Y				Linked in	30-90 free trials	Allow membership with purchase of other services	We are planning to establish a Board of Directors for our ISAC and want to include management from Gov Agencies involved with our industry.
9						Y		Y			3-month free trials		

DOT HS 812 076
October 2014

U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

11002-101614-v2