NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

CROSS SECTOR INTERDEPENDENCIES AND RISK ASSESSMENT GUIDANCE

FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

JANUARY 13, 2004

MARTIN G. MCGUINN
WORKING GROUP CHAIR
CHAIRMAN AND CHIEF EXECUTIVE OFFICER
MELLON FINANCIAL CORPORATION

ACKNOWLEDGEMENTS

Mr. McGuinn wishes to acknowledge the efforts of the entire working group and their support staffs (listed below) and particularly extends his appreciation to Susan Vismor (Mellon Financial Corporation), Chris Terzich (Wells Fargo & Company) and Teresa C. Lindsey (BITS) for their dedication to this effort.

- **Working Group Members**
  - John T. Chambers, President and CEO, Cisco Systems, Inc.
  - George H. Conrades, Chairman and CEO, Akamai Technologies
  - Richard K. Davidson, Chairman, President and CEO, Union Pacific Corporation
  - Archie W. Dunham, Chairman, ConocoPhillips
  - Margaret E. Grayson, President and CEO, V-ONE Corporation
  - Richard M. Kovacevich, Chairman and CEO, Wells Fargo
  - Martin G. McGuinn, Chairman and CEO, Mellon Financial Corporation
  - Thomas E. Noonan, Chairman, President and CEO, Internet Security Systems, Inc
  - Thomas H. Weidemeyer, Chief Operating Officer, United Parcel Service (UPS)

- **Study Group Members**
  - Susan Vismor, SVP, Mellon Financial Corporation, Study Group Chair
  - Chris Terzich, Wells Fargo and Company
  - Peter Allor, Internet Security Systems, Inc.
  - Bob Bergman, United Parcel Service
  - Andy Ellis, Akamai Technologies
  - Bobby Gilham, ConocoPhillips (Also listed as sector coordinator)
  - Rick Holmes, Union Pacific Corp.
  - Douglas Hurt, V-One Corporation
  - Ken Watson, Cisco Systems, Inc.

- **Other Study Contributors**
  - Teresa C. Lindsey, Chief of Staff, BITS
  - Aaron Meckler, Wells Fargo and Company
  - Michehl Gent, North American Electric Reliability Council, Energy *
    - Lou Leffler, NERC
    - Dave Nevius, NERC
  - Bobby Gilham, ConocoPhillips, Inc., Energy *
  - Kathryn Condello, CTIA, Information and Telecommunications *
  - Matthew Flanigan, TIA, Information and Telecommunications*
    - David Thompson, TIA Online
  - Harris Miller, ITAA, Information and Telecommunications*
    - Greg Garcia, ITAA
  - Ed Merlis, USTA, Information and Telecommunications*
    - David Kanupke, USTA
  - Ed Hamberger, Association of American Railroads, Transportation*
    - Nancy Wilson, Association of American Railroads

- Rhonda MacLean, Bank of America, Financial Services *
  - Peggy Lipps, Bank of America
  - Roger Callahan, Bank of America
- Diane Van DeHei, Association of Metropolitan Water Agencies, Water *
- Tim Zoph, Northwestern Memorial Hospital, Healthcare
- Nancy Wong, DHS
- Eric Werner, DHS
- Clay Woody, DHS

** Accepted to participate (or send substitute)*

TABLE OF CONTENTS

Our basic systems are at risk from threats we may not yet foresee. We need to anticipate these threats to our infrastructures, design systems that are inherently safer and more robust, and be prepared to restore them when they fail.[1]

BACKGROUND AND METHODOLOGY

At the April 22, 2003 meeting of the National Infrastructure Advisory Council (NIAC), a Working Group led by Mr. Martin McGuinn and other NIAC Members with support from their knowledgeable staffs was established to study cross-sector interdependencies and provide risk assessment guidance. In retrospect, it was overly optimistic to presume that a voluntary, private-sector working group could bring to bear the resources necessary to address a topic as complex as this. However, we did bring our "business" perspective and concentrated on capturing high-level recommendations with practical, short-term deliverables. The Study Group reviewed previously published studies[2] and recruited participation from all critical infrastructures——broadening the Study Group's composition beyond the members' experience represented on the NIAC.

No matter how long we study interdependencies or how much risk assessment guidance we provide, we cannot protect ourselves against every eventuality. However, we can prepare ourselves. Part of that preparation is thinking through the management of events. As the Study Group studied interdependencies, it necessarily examined how to coordinate event management between the critical infrastructures. **The Working Group concluded that cross-sector crisis management coordination is fundamental to the rapid restoration of critical infrastructure(s) and integral to sustain the public's confidence in those infrastructures.**

FUNDAMENTAL PRINCIPLES

Our nation's preparedness——inclusive of cross-sector interdependencies——has been entrusted to the Department of Homeland Security (DHS). DHS is a colt, struggling to stand and gain its balance. We have every confidence that it will stand, and stand tall. As it grows and develops, we recommend that DHS adopt the following set of fundamental principles:

- Projects must be structured to provide short-term deliverables that address the most pressing issues in a useful, if non-optimal, fashion. Many of the initiatives, while impressive in vision, have time horizons that span several years.
- Projects must be monitored to ensure that adequate progress is being made on the suggested deliverables.
- The partnership between the public and private sectors must be a two-way street. Often the public sector involves the private sector in issues after critical planning decisions have already been made. Only with the timely and substantive exchange of information during planning processes will the partnership grow to be the "trusted" partnership that we all desire.

[1] *Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems*, Richard G. Little, National Research Council

[2] See Appendix of this report for a matrix of studies reviewed

The recommendations that follow assume the principles above are adopted. **We can mitigate the risks we face due to cross-sector interdependencies by defining short-term deliverables, establishing a method to monitor progress of those deliverables, and fostering the commitment of the public and private sectors to partner for progress.**

ISSUES AND RECOMMENDATIONS

The Working Group identified nine issues for the NIAC that if not addressed, could polarize efforts to coordinate across sectors before, during, and after an event. Each issue is followed by a recommendation to mitigate the risk posed. Further, where appropriate, issues correlate to a tab in this report. For example, we have provided the high-level recommendations in this Executive Summary. For more detail, refer to the materials in the tab that correspond to the respective issue.

Issue 1 – Inconsistencies exist in the definitions of the critical infrastructures. *(See Tab 1 for more detail)*

Recommendation: Promote organizational consistency using the definitions for Critical Infrastructures contained in Homeland Security Presidential Directive (HSPD) 7: *Critical Infrastructure Identification, Prioritization, and Protection,* dated December 17 2003**. The NIAC also recommends that each of those critical infrastructures develop a sector coordinating mechanism, an information sharing mechanism, and representation on the NIAC.**

We recommend that organizational consistency be established by using the definitions and policy guidelines in Homeland Security Presidential Directive (HSPD) 7: *Critical Infrastructure Identification, Prioritization, and Protection,* dated December 17, 2003, as the basis for appointment or establishment of critical infrastructure support roles, including sector coordinating mechanisms, information sharing mechanisms, and NIAC appointments.

Issue 2 – The "sector coordination" role is not broadly understood by industry and therefore is not viewed as a focal point for crisis management coordination within and across the sectors. Further, sector coordinating mechanisms have not been identified for all critical infrastructures. *(See Tab 2 for more detail)*

Recommendation: The NIAC strongly supports the concept of sector coordination mechanisms participating in, coordinating, and supporting private/public and cross-sector collaborative efforts that promote the nation's economic stability, national security, and infrastructure integrity. Define and publicize the role of sector coordination mechanisms to their respective constituencies. Collaborate with appropriate private sector entities and continue to support sector coordination mechanisms.

A communication plan should be devised to make the CEOs, CIOs, and crisis managers of private organizations aware of the role and responsibilities of the sector coordinator role. Contact information should also be provided for use in emergency situations.

DHS has described best practices for the sector coordination role and other parties with an interest in a resilient critical infrastructure. This document is included in Tab 2. The NIAC is in agreement with the general principles outlined in the document. In addition to the following recommended modifications, the NIAC would appreciate the opportunity to comment on the document before it is finalized.

- A sector coordination mechanism should be responsible for insuring that a crisis management plan exists for the respective sector. As part of the crisis management plan, each sector coordination mechanism will provide 24/7 contact information.
- The sector coordination mechanism should act as the cross-sector liaison for the sector.

<u>Issue 3</u> – Crisis management plans do not exist for each sector and are not tested end-to-end across the sectors. *(See Tab 3 for more detail)*

<u>Recommendation:</u> Encourage and support the development, implementation, and testing of crisis management plans for each sector. Testing should include validation of cross-sector coordination. Assuring the testing and exercising of sector crisis management plans should be under the purview of the sector coordinating mechanisms.

In the private sector, businesses are required to have crisis management processes in place for all critical functions. This includes the development and maintenance of business recovery plans, as well as testing of these plans, on an annual basis. There is a growing realization that these plans need to encompass not only internal processes, but must also consider any dependencies with suppliers and customers

This same crisis management discipline needs to be applied to the nation's critical infrastructures. Each sector needs to have a recovery plan that is clearly defined and articulated, and shared (as appropriate) with other critical sectors who are users or suppliers of the infrastructure.

Recommended Short-Term Actions:

1. Create automated call trees via an automated notification system. Call trees should include sector liaisons, sector coordinators, and Information Sharing and Analysis Center (ISAC) contacts at a minimum.
2. Encourage each sector coordinating mechanism to establish a "Virtual Command Center" via an open bridge line to be used during a crisis. This number should be made available to the appropriate contacts in private industry—including the liaisons, coordinators, and ISAC contacts for other critical infrastructures—and used appropriately in a given situation.

Recommended Long-Term Actions:

Encourage development of crisis management plans for each sector. They should be tested annually and include validation of cross-sector coordination. Each crisis management plan should clearly

define responsibility for testing. Consideration should be given to establishing common terminology, resource management, and communication protocols.

Issue 4 – A National Command Center does not exist as a confluence point for the private sectors during times of crisis. *(See Tab 4 for more detail)*

Recommendation: Establish a virtual command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency situation.

The Homeland Security Operations Center (HSOC):

- Maintains and shares continuous domestic situational awareness
- Conducts initial information assessment and threat monitoring to detect, deter, and prevent terrorist incidents
- Coordinates and monitors homeland security operations

As impressive as this charter is, it does not include the private sector and it is the understanding of the NIAC that private sector inclusion will not occur for two years. Therefore, we recommend that until the plan to include the private sector is implemented, HSOC devise a private sector virtual command center and brief the critical infrastructures as appropriate.

Issue 5 – Government-sponsored exercises (e.g., TOPOFF2) should actively solicit private industry representation. *(See Tab 5 for more detail)*

Recommendation: DHS should sponsor crisis management exercises that include the participation of the critical infrastructures, as soon as possible, and annually thereafter.

In private industry, critical business functions are required to be tested at least on an annual basis. We recommend that regional, cross-sector exercises are held on an annual basis in major U.S. cities.

Issue 6 – There is an underestimation of the dependency of the nation's critical infrastructures on the Internet. *(See Tab 6 for more detail)*

Recommendation: Enhance awareness of Internet dependencies.

Most organizations, regardless of sector, tend to underestimate their reliance on the Internet. This underestimation generally comes in two forms: either the organization assumes it still has sufficient fallback processes to return to pre-Internet business models, or it discounts the damage that a critical, non-failure event can have (such as a worm or virus). Many organizations, in making their early transitions to Internet-based models, kept in place legacy processes in the event a fallback was required. Over time, these processes became outdated, personnel were no longer proficient in them, or the support infrastructure was no longer in place to manage them. Internal departments have made strides in adopting new technologies, which may not be visible to upper management. Both factors contribute to a belief at executive levels that the Internet itself is not a critical system. Most faults in critical systems are believed to be failure-oriented (such as the recent blackout across the

Northeast). For the Internet, many faults are not failure-oriented——indeed the most devastating attacks are from worms and viruses that infect systems, sometimes impacting back-end systems such as a bank's ATM network or manufacturing systems. These non-failure faults are generally not considered when assessing Internet reliance.

Issue 7 – Coordination in planning and response between public emergency management (federal, state, and local) and private critical infrastructure is inadequate and/or inconsistent. *(See Tab 7 for more detail)*

Recommendation: Provide a framework for public and private emergency management interaction including national, sector, state, regional and local levels. This framework should integrate with public and private information sharing models and must account for ISACs and InfraGard, as well as review of significant regional public/private partnerships.

DHS should create a framework for public and private emergency management interaction that includes private companies and critical infrastructure sectors in its scope, as well as geographic and governmental levels of local, regional, state and federal emergency managers.

The Incident Command System (ICS) has been widely adopted as the standard for command, coordination and communication between diverse government and emergency response entities. At present, the National Incident Management System (NIMS) is the program DHS is currently developing to establish formal incident management protocols throughout the United States, likely encompassing ICS.

While public emergency managers using ICS at the state and local level occasionally address private-sector critical infrastructure issues, it is not consistent and does not adequately account for all infrastructure sectors, nor does it provide uniform structure for interaction with these sectors at all government levels.

If NIMS is intended to replace ICS as the structure for incident management throughout the United States, detailing a critical infrastructure role within NIMS can effectively ensure the public/private partnership in emergency management planning and crisis response at all government levels.

Identification of critical infrastructure as a role within NIMS should include at a minimum: identification of critical infrastructure organizations within the planning area; communication authorities and credentialing of infrastructure company staff for interaction with emergency functions, such as an Emergency Operations Center (EOC) and for access into company property within disaster-impacted areas; and priority designation of resources to aid cross-sector critical infrastructure recovery and reconstitution.

Two significant problems hamper effective information sharing and crisis management today:

1. Some federal, state, and city entities have implemented their own information-sharing initiatives. While these initiatives may increase the sharing of information to fight terrorism, they are not well coordinated and consequently risk creating partnerships that may actually limit some participants' access to information and duplicating efforts of some key agencies in each level of government. Moreover, while beneficial to these participants, the initiatives do not necessarily integrate others into a truly national system and may for this reason

inadvertently hamper information sharing. A lack of effective integration could increase the risk that officials will overlook or never even receive information needed to prevent a terrorist attack[3].

2. There seems to be redundancy and potentially competing objectives between DHS and the Federal Bureau of Investigation's (FBI) InfraGard.[4]

In order to aid emergency managers in working with private critical infrastructure companies, DHS should promote a model for the private sector that is similar in principle to ICS (see *Business Incident Coordination System* below). In particular, consideration should be given to the designation of a role—Homeland Security Officer—within a private sector-company as the primary interface with public emergency management entities.

Recommended Short-term Actions:

1. Immediately review the upcoming National Incident Management System to ensure inclusion of privately held critical infrastructures in final version.
2. Ensure there is no duplication of efforts between InfraGard (FBI) and DHS. If conflicting or competing objectives exists, the issue should be escalated for resolution within the federal government.
3. Provide short overview guide to critical infrastructure crisis management for private companies (see *Business Incident Coordination System* in Tab 7) and for governors, including recommendation for designation of Homeland Security Officers for companies.

Recommended Long-Term Actions:

1. Crisis and emergency management require trusted and reliable communication networks, both digital and human. As a result, a public/private emergency management framework must leverage the same networks used to share information about threats and risk mitigation. DHS should develop a national framework for information sharing and emergency management (see *National Crisis Management Partnership* diagram in Tab 7), accounting for and integrating with significant information sharing networks, particularly ISACs and InfraGard.
2. Ensure this model includes a regional component. Significant regional models throughout the United States should be reviewed to develop a single best model, including ChicagoFIRST, Portland, Oregon RAINS, and other large-scale models.
3. DHS should include interaction between public and private emergency management in a guidebook (mentioned above) for critical infrastructure protection and crisis management written for use by critical infrastructure companies and state and local emergency management agencies. The guide may be similar to *"A Governor's Guide to Emergency Management Volume Two: Homeland Security"*.[5]

---

[3] Homeland Security – Efforts to Improve Information Sharing Need to Be Strengthened (GAO-03-0760)

[4] InfraGard is a partnership between the FBI and 9,000 private companies through 56 local InfraGard Chapters. Infragard was created to provide a forum for sharing between law enforcement and other local officials and private sector companies.

[5] http://www.nga.org/cda/files/GOVSGUIDEHS2.pdf

Issue 8 – There is a lack of incentives that would help defray the additional expense burden resulting from strengthening the resiliency of the critical infrastructures. *(See Tab 8 for more detail)*

Recommendation: Explore the potential for creating tax incentives or other instruments to incent the private sector to enhance the resiliency of the critical infrastructures.

Post 9/11, there is certainly a heightened corporate awareness of the need to strengthen the resiliency and security of the critical infrastructures. The cost burden associated with these corporate investments is substantial. However, it is critical for our nation and our economy that these improvements are made as rapidly as possible. This is especially true for corporate entities considered to be part of our nation's critical infrastructure. A single incident with one of these entities could have catastrophic cascading effects on interdependent organizations and services.

To encourage private-sector investment in strengthening our infrastructures, we recommend that financial incentives be provided to these companies. Without incentives to help defray the additional expense burden, many organizations will be forced into protracted and/or delayed implementations while our nation remains potentially vulnerable.

Issue 9 – Sophisticated modeling capabilities exist at the national laboratories and multiple research and development (R&D) studies on cross-sector interdependencies have been completed. *(See Tab 9 for more detail)*

Recommendation: The national laboratories should focus their interdependency modeling and research on the regions and sectors whose failure would have the highest impact on the economy and national security. The Study Group suggests starting with modeling the telecommunications and energy sectors and the interdependencies among them and the other critical infrastructures. Additionally, existing R&D studies need to be indexed and cross-referenced in such a way as to make these materials accessible to appropriate parties.

It is clear that substantial effort and investment has gone into an equally substantial number of modeling efforts and studies on cross-sector interdependencies. The Study Group reviewed and abstracted 37 studies and received a briefing on the capabilities of the National Infrastructure Simulation and Analysis Center (NISAC). The information resulting from both the modeling efforts and the studies needs to be leveraged by appropriate parties so that the lessons learned can be implemented and built upon before additional efforts are launched.

CONCLUSION

> *"Understanding, analyzing, and sustaining the robustness and resilience of these infrastructures require multiple viewpoints and a broad set of interdisciplinary skills. The key point is that interdisciplinary expertise and research are needed to address these dimensions. To be successful, this effort will require cooperation and collaboration among infrastructure and interdependency experts from government, industry, academic and research institutes, and the national laboratories. It also will necessitate focused education*

and awareness efforts to prepare professionals to understand fundamental interdependency concepts and issues and the "system of systems" paradigm."[6]

Cooperation and collaboration: these two words most succinctly and definitively express our best defense against risks resulting from cross-sector interdependencies. Our critical infrastructures are inextricably linked. The NIAC respectfully submits that the infrastructures' human counterparts should likewise be linked——cooperating and collaborating for our nation's security.

[6] *Infrastructure Interpendencies: Overview of Concepts and Terminology*; James Peerenboom, Infrastructure Assurance Center, Argonne National Laboratory

CRITICAL INFRASTRUCTURES TAB 1

Issue 1 – Inconsistencies exist in the definitions of the critical infrastructures.

Recommendation: Promote organizational consistency using the definitions for Critical Infrastructures contained in Homeland Security Presidential Directive (HSPD) 7: *Critical Infrastructure Identification, Prioritization, and Protection,* dated December 17 2003**. We also recommend that each of those critical infrastructures have a sector coordinating mechanism, an Information Sharing and Analysis Center (ISAC), and representation on the NIAC.**

We recommend that organizational consistency be established by using the definitions and policy guidelines in Homeland Security Presidential Directive (HSPD) 7: *Critical Infrastructure Identification, Prioritization, and Protection,* dated December 17 2003, as the basis for appointment or establishment of critical infrastructure support roles, including Sector Coordinators, ISACs, and NIAC appointments.

CRITICAL INFRASTRUCTURES AND FEDERAL LIAISON ORGANIZATIONS

Sector	Lead Agency
Agriculture	Department of Agriculture
Food: *Meat and poultry* *All other food products*	 Department of Agriculture Department of Health and Human Services
Drinking Water and Water Treatment Systems	Environmental Protection Agency
Public Health and Healthcare	Department of Health and Human Services
Emergency Services	Department of Homeland Security
Government: *Continuity of government* *Continuity of operations*	 Department of Homeland Security All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy (including the production refining, storage, and distribution of oil, gas and electric power)	Department of Energy
Transportation	Department of Homeland Security
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

The following chart illustrates the gaps that exist between critical infrastructures, sector coordinators, ISACs, and representation on the NIAC.

SECTOR	SECTOR COORDINATOR	ISAC	ISAC CONTACT	NIAC
1. Agriculture				
2. Food - Meat and Poultry - All Other		Food ISAC	Tim Hammonds Tim Weigner	
3. Water	Diane VanDe Hei	Water ISAC	Susan Tramposch	American Waterworks Service Company, Inc.
4. Public Health	Tim Zoph (Interim)	HC ISAC in development		
5. Emergency Services	Dave Christler			City of Albuquerque City of New York
6. Government		NASCIO	Chris Dixon	
7. Defense Industrial Base				
8. Information and Telecommunications	Harris Miller – ITAA Matthew Flanigan – TIA Daniel Pyhthyon – USTA –Steve Largent - CTIA	IT ISAC Telecom ISAC	Pete Allor Ernie Gormsen	Akamai Cisco E-Bay EDS Intel Inter-Con Security Systems Internet Security Systems Symantec V-One Corporation
9. Energy	Mike Gent – NERC Bobby Gillham - ConocoPhillips	Electric ISAC	Lou Leffler	ConocoPhillips TXU Corp
10. Transportation	Ed Hamberger Greg Hull David Plavin	Surface Transportation ISAC	Paul Wolfe	American Airlines Union Pacific
11. Banking and Finance	Rhonda MacLean	Financial Services ISAC	Suzanne Gorman	Mellon Financial Corp. NASDAQ Sterling Bank & Bancshares Wells Fargo & Company
12. Chemical Industry and Hazardous Materials				DuPont Company Pfizer Global
13. Postal and Shipping				United Parcel Service
14. National Monuments and Icons				
15. Education (Not in National Strategy)				James Madison University

STATUS OF CURRENT ISACS

Financial Services ISAC
ISAC Lead: Chairperson, FS-ISAC Board of Managers
Date ISAC created: October 1, 1999
Membership: 57 member entities (about 50% of credit assets in U.S. represented——composed of banks, brokerages, financial markets representing $23 trillion/17 trillion dollars and all of the equity markets)
ISAC Hosting Structure: LLC with outsourced operations

Electric ISAC
ISAC lead: Chair, CIPWG/NERC
Date ISAC created: October 2000
Membership: Represents 70% of U.S. and Canada's power companies (all 19 reliability coordinators and regions are associated)
ISAC Hosting Structure: NERC runs operations

Energy ISAC
ISAC lead: American Petroleum Institute
Date ISAC created: November 1, 2001
Membership: 35 members representing the majority of the major oil and gas companies
ISAC Hosting Structure: LLC with outsourced operations

Telecom ISAC
ISAC Lead: National Communication System's National Coordination for Security, Infrastructure Protection, and Counterterrorism
Date ISAC created: Operational since 1984, became 24/7 operation after September 11, 2001, and official ISAC on January 7, 2002
Membership: Approximately 22 members, 90% of telecom market share, 99.8% of wireless industry
ISAC Hosting Structure: Physically located in a government facility with outsourced operations

Information Technology ISAC
ISAC Lead: Director of Operations, ISAC Boards of Directors (senior members of IT companies)
Date ISAC created: July 15, 2001
Membership: 20 companies
ISAC Hosting Structure: Non-profit LLC with outsourced operations

Surface Transportation ISAC
ISAC Lead: Association of American Railroads (AAR) and American Public Transportation Association
Date ISAC created: May 8, 2002
Membership: Members of the Association of American Railroads, American Public Transportation Association (recent member), and American Trucking Association (potential member)
ISAC Hosting Structure: AAR with operations outsourced

Chemical ISAC
ISAC Lead: American Chemistry Council and The Chemical Transportation Emergency Center (CHEMTREC)
Date ISAC created: April 24, 2002
Membership: Approximately 100 members of the American Chemistry Council registered, began rolling out invitation to transporters (88) in October, 2003, next group will be distributors
ISAC Hosting Structure: Sponsored by the American Chemistry Council and operated by CHEMTREC

Water ISAC
ISAC Lead: AMWA
Date ISAC created: December 2002
Membership: Municipal and privately owned water facilities
Hosting Structure: AMWA/Water ISAC; selecting vendor to outsource operations

Food ISAC
ISAC Lead: FMI
Date ISAC created: February 15, 2002
Membership: Members are associations, supermarkets, and restaurants
Hosting Structure: Operated by FMI

SECTOR COORDINATORS TAB 2

Issue 2 – The "sector coordination" role is not broadly understood by industry and therefore is not viewed as a focal point for crisis management coordination within and across the sectors. Further, sector coordinators have not been identified for all critical infrastructures.

Recommendation: The NIAC strongly supports the concept of sector coordination mechanisms, participating in, coordinating, and supporting private/public and cross sector collaborative efforts that promote the nation's economic stability, national security, and infrastructure integrity. Define and publicize the role of sector coordination to their respective constituencies. Collaborate with appropriate private sector entities and continue to support sector coordination mechanisms. Currently there are no coordination mechanisms for the following critical infrastructures:

- **Agriculture**
- **Food**
- **Chemical and Hazardous Materials**
- **Government**
- **Postal and Shipping**
- **National Monuments and Icons**

A communication plan should be devised to make the CEOs, CIOs, and crisis managers of private organizations aware of the role and responsibilities of the sector coordinator role. Contact information should also be provided for use in emergency situations.

DHS has described best practices for the sector coordination role and other parties with an interest in a resilient critical infrastructure. This document is included in Tab 2. The NIAC is in agreement with the general principles outlined in the document. In addition to the following recommended modifications, the NIAC would appreciate the opportunity to comment on the document before it is finalized.

- A sector coordination mechanism should be responsible for insuring that a crisis management plan exists for the respective sector. As part of the crisis management plan, each sector coordination mechanism will provide 24/7 contact information.
- The sector coordination mechanism should act as the cross-sector liaison for the sector.

The following document was prepared by the Department of Homeland Security and outlines best practices with respect to critical infrastructure protection.

ROLES AND RESPONSIBILITIES WITH RESPECT TO CRITICAL INFRASTRUCTURE PROTECTION (PRE-HSPD 7)

The federal government is aligned to interface directly with the private sector to protect critical infrastructures. Almost eight-five percent of the United States' critical infrastructure is owned and operated by private industry. The President's *National Strategy for Homeland Security*, which identified the thirteen critical sectors, outlines a sector-based organizational system for government and private industry to work together to protect America's critical infrastructures and key assets. The organizational framework provides a foundation for public-private-sector interaction and advances a cooperative environment in which government and industry can effectively and efficiently share information and work together to protect critical infrastructures. Each critical sector identified has a federal department or "lead agency" with an individual designated to serve as the "sector liaison". The sector liaison serves as the private sector's primary interface with the government. In addition, each sector liaison has an industry counterpart or "sector coordinator" that is appointed by the federal department or agency to serve as a neutral party to facilitate the sector's coordination for planning and activities to secure critical facilities and systems. This document contains descriptions of the following entities and describes their evolving roles in critical infrastructure protection:

- Federal Government's Role
- Sector Specific Agency *(federal government)*
- Sector Liaison *(representative from lead agency)*
- Department of Homeland Security (DHS)
- Private Sector's Role
- Sector Coordinator *(private sector)*

Federal Government's Role
The federal government's role in the context of homeland security is to organize, convene, and coordinate activities across governmental jurisdictions and with the private sector. The federal government will coordinate the complementary efforts and capabilities of government and private institutions to raise the level of protection across our critical infrastructures and key assets. Two major components make-up the federal government's participation in critical infrastructure protection efforts: the Department of Homeland Security (DHS) and the designated sector-specific agencies.

The following chart depicts the federal government organization for protecting America's infrastructures and key assets, and indicates the departments and agencies that have primary responsibility for interacting with particular critical infrastructure sectors.

Sector	Sector-Specific Agency
Agriculture	Department of Agriculture
Food:	Department of Agriculture

Sector	Sector-Specific Agency
Meat and poultry *All other food products*	Department of Health and Human Services
Drinking Water and Water Treatment Systems	Environmental Protection Agency
Public Health and Healthcare	Department of Health and Human Services
Emergency Services	Department of Homeland Security
Government: *Continuity of government* *Continuity of operations*	 Department of Homeland Security All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy (including the production refining, storage, and distribution of oil, gas and electric power)	Department of Energy
Transportation	Department of Homeland Security
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

Sector Liaison (federal government)

A sector-specific agency designates an individual to serve as a sector liaison, the private sector's interface with the sector-specific agency of the federal government. The sector liaison (or sector liaison body) works with the private sector through the sector coordinator to organize and facilitate the coordination of the sector's critical infrastructure protection activities. The sector liaison works closely with the sector coordinator on the development of tools, technology, and science necessary to make our infrastructures even stronger. The sector liaison should engender trust, facilitate communication, and expand voluntary information sharing on critical infrastructure protection issues—both among sector members and with the government. Through the sector liaison, a sector-specific agency is able to work with a sector coordinator to reach the infrastructure owners and operators in that sector and facilitate the overall protection of that sector's critical infrastructure. Sector liaisons may identify a representative(s) at the working level for day-to-day activities.

Department of Homeland Security

The Department of Homeland Security (DHS) will enhance the effectiveness of this model by providing overall cross-sector coordination. DHS will provide overarching leadership and serve as the primary facilitator for cooperation between the federal government and the critical infrastructure sectors and states. This responsibility includes maintaining a comprehensive, accurate, and up-to-date assessment of critical assets, systems, and functions of national-level importance. It also entails determining criticality, vulnerability, and risk across the sectors of the U.S. economy. DHS is further

responsible for employing information derived from those activities to assess threats, develop indications, and disseminate warnings to threatened infrastructures or organizations. Additionally, DHS is the sector-specific agency for certain critical infrastructure sectors (i.e., Emergency Services, Postal and Shipping, Information and Telecommunications, and Government: *continuity of government*)*. DHS will work together with the appropriate federal sector agencies to provide consistent, tailored guidance and criteria for information sharing and protection planning efforts in the critical infrastructure sectors. Much of the interaction will take place with the Information Analysis and Infrastructure Protection Directorate (IAIP).

Private Sector's Role

Because private industry owns and operates approximately eighty-five percent of America's critical infrastructures and key assets, the federal government needs to engage the private sector in an unprecedented partnership. The private sector brings expertise and a unique perspective to the collaboration process.

Owners and operators have long been responsible for protecting their assets against unauthorized intruders. However, the threat to our critical infrastructures has changed and the government must work with industry to help cope with significant military or terrorist threats, or the cascading economic and psychological impact they may entail.

Sector Coordinator (private sector)

For each of the major sectors of our economy that are attractive to terrorist attack, the federal government, designated sector-specific agencies, and DHS will help the private sector to organize and coordinate members of the sector on protection activities. A sector coordinator identified by the sector-specific agency and DHS within private industry to coordinate its sector, inclusively, acting as an honest broker to organize and bring the sector together to work cooperatively on sector infrastructure protection issues. The sector coordinator can be an individual, an institution, or a council of institutions from the sector. Sector coordinators may also identify a representative(s) at the working level for day-to-day activities.

Sector coordinators will provide the central conduit to the federal government for the information needed to develop an accurate understanding of what is going on throughout the nation's infrastructures on a strategic level with regards to critical infrastructure protection activities. Coordinators will work in coordination with the established channels for providing information from the private sector to government.

Functions for a sector coordinator/sector coordination mechanism include:

- Organize the sector's leadership and engagement on infrastructure protection (with the encouragement of the federal government); assure a structure to represent sector members; identify, set an agenda, and initiate a program of sector-wide infrastructure protection activities including:
    - Coordination of a national plan for infrastructure protection for its sector
    - Outreach and awareness to support infrastructure protection plan implementation;
    - Risk assessment methodology and implementation for the sector, including interdependencies

  - Requirements for research and development necessary to meet the special needs of the sector
  - Requirements and overseeing the development of an information sharing mechanism (e.g., ISAC) for the sector, tailored to the special needs of the sector and infrastructure protection
  - Requirements for sector wide guidelines/standards/useful/effective practices on infrastructure protection, training and education and implementation, metrics for success of infrastructure protection activities
  - Identification and communication of obstacles or impediments to an effective infrastructure protection program that contains all elements of above
- Serve as the coordination point for the sector's owners and operators in discussions with other sectors as needed (particularly to identify interdependencies, address common issues, and share effective practices).
- Act as the coordination point of contact for the sector with the federal government at various infrastructure protection meetings, and the strategic communication point back into the sector and its members from the federal government.

The sector coordinator and the sector it coordinates, in cooperation with a designated federal agency and DHS, shall contribute to a sectoral infrastructures and key assets protection plan, a follow-on planning mechanism to the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, by:

- Assessing the vulnerabilities of the sector to cyber or physical attacks
- Recommending actions to reduce and eliminate significant vulnerabilities
- Proposes a system for identifying and preventing attempted major attacks as appropriate
- Developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with DHS (IAIP and Emergency Preparedness and Response Directorates) as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack

Some sectors' diverse interests may make choosing a single sector coordinator challenging. Industry and the sector agency may explore innovative solutions, such as a coordination body or "virtual coordinator" based on existing networked resources, by designating separate sector coordinators to represent key sub-sectors who can in turn, work together to represent the entire sector. The intention is for sector liaisons and coordinators to have a close working relationship and communication.

A sector coordinator with support from the sector liaison, oversees the development of ISACs within its sector and supports its success. In some cases, an ISAC manager may be designated, who is responsible for the day-to-day operations of the ISAC, to work with the sector coordinator or the sector coordinating body with support from DHS and the sector agencies.

An ISAC is an operational mechanism to enable members to share information about vulnerabilities, threats, and incidents (cyber and physical). Presidential documents, such as the *National Strategy for Homeland Security*, continue to encourage information sharing and identify ISACs as an information-sharing model. Many of the ISACs, particularly since the events on September 11, 2001, incorporate more information on physical security.

An ISAC's purpose is to gather, analyze, and disseminate to its members an integrated view of information system and other infrastructure vulnerabilities, threats, and incidents that are relevant to the sector. An ISAC includes the following characteristics:

- 24/7 indications and warnings within the sector
- Information sharing with government and other ISACs as desired (voluntary and non-attributable)
- Receive alerts and warnings of threats and incidents for dissemination to sector from government and other sources
- Receive vulnerabilities or remediation information for dissemination to sector from government and other sources

The information that ISACs commonly work with provide warnings, establish trends in types and severity of attacks, and share threats and solutions among the ISAC membership and other appropriate organizations, including the Federal government. The ISACs will be communicating with DHS' IAIP's 24/7 operating divisions. This information can be included in the gov'rnment's analysis to help inform the public of possible threats and incides.

- * As indicated in the President's National Strategy for Homeland Security issued July 2002.

CRISIS MANAGEMENT COORDINATION TAB 3

<u>Issue 3</u> – Crisis management plans do not exist for each sector and are not tested end-to-end across the sectors.

<u>Recommendation:</u> Encourage and support the development, implementation, and testing of crisis management plans for each sector. Testing should include validation of cross-sector coordination. Assuring the testing and exercising of sector crisis management plans should be under the purview of the sector coordinator(s).

In the private sector, businesses are required to have crisis management processes in place for all critical functions. This includes the development and maintenance of business recovery plans, as well as testing of these plans, on an annual basis. There is a growing realization that these plans need to encompass not only internal processes, but must also consider any dependencies with suppliers and customers

This same crisis management discipline needs to be applied to the nation's critical infrastructures. Each sector needs to have a recovery plan that is clearly defined and articulated, and shared (as appropriate) with other critical sectors who are users or suppliers of the infrastructure.

Recommended Short-Term Actions:
1. Create automated call trees via an automated notification system. Call trees should include sector liaisons, sector coordinators, and ISAC contacts at a minimum.

2. Encourage each sector coordinator to establish a "Virtual Command Center" via an open bridge line to be used during a crisis. This number should be made available to the appropriate contacts in private industry——including the liaisons, coordinators, and ISAC contacts for other critical infrastructures——and used appropriately in a given situation

Recommended Long-Term Actions:
Encourage development of crisis management plans for each sector. They should be tested annually and include validation of cross-sector coordination. Each crisis management plan should clearly define responsibility for testing. Consideration should be given to establishing common terminology, resource management, and communication protocols.

As part of the Study Group's due dilligence, critical infrastructures were invited to present their sector's approach to security and/or crisis management.

THE RAILROAD SECTOR

RAILROAD SECTOR APPROACH TO SECURITY

Prepared for NIAC Task Force on
Cross Sector Interdependencies &
Risk Assessment Guidance

Conference Call

June 11, 2003

Railroads' Importance to the U.S. Economy

Railroads transport:

- 42% of intercity ton-miles
- 64% of coal used for electric power
- 40% of the grain harvest
- 70% of automobiles made in America
- 20% of chemicals, and more of those essential to the public health

Selected Impacts of a Shutdown in Hazmat Traffic: Chlorine

- Used in 98% of all water treatment, 85% of pharmaceuticals, 96% of crop protection.
- In the Oct. 2001 72-hour embargo, L. A. and a few other cities almost ran out and required special shipments.
- Trucks can't pick up the slack, as only 82 nationwide can haul over 20 tons of chlorine.

Other Rail-Dependent Hazmat Traffic Used for:

- Pulp, paper and aluminum manufacturing
- Gasoline oxygenation
- Surgical equipment sterilization
- Aircraft/Highway deicing
- Antifreeze, brake fluids, solvents production
- Residential and commercial heating

Impact of a Total Rail Shutdown

Industry	**Shut down within**:
• **Plastics**	**4 Days**
• **Automobile**	**1 to 2 Weeks**
• **Paper**	**1 Week (partial)**
• **Coal Mining**	**2 Weeks**
• **Electric Power**	**1 to 2 Months**

Railroad Security Task Force

Five Critical Action Teams:

- Hazardous Materials
- Operations
- Physical Infrastructure
- IT & Communications
- Military Liaison

Over 150 railroad, customer and security personnel.

Risk Assessment

- U.S. Government “Best Practices”
- Assessed risks to:
  - National Economy
  - National Security
  - Population
- Created Security Management Plan

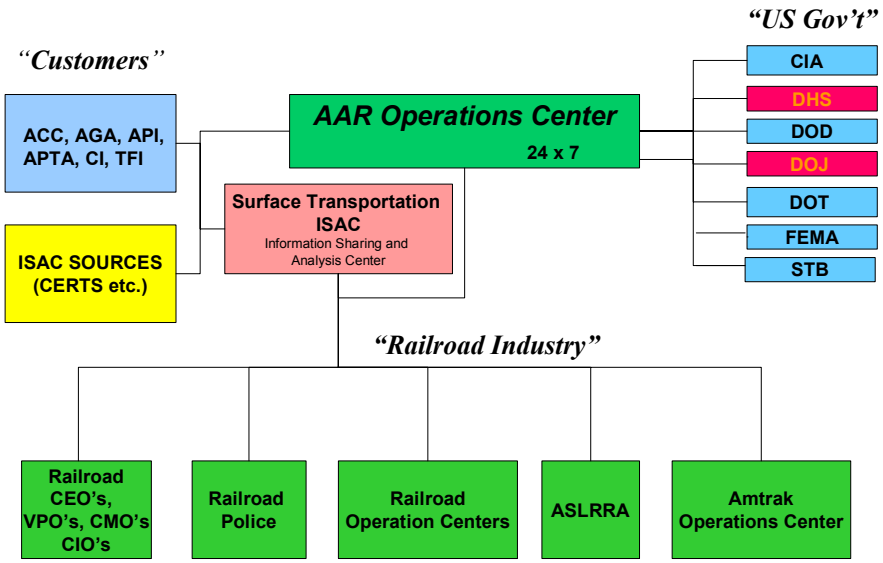
Alert Levels

- Level 1 – New Normal
- Level 2 – Heightened Security
- Level 3 – A Credible Threat of an attack on the US or railroad industry
- Level 4 – A Confirmed Threat of attack against the railroad industry or actual attack in the US

Countermeasures

- At each Alert Level
- For each of 3 functional areas:
  - Operations
  - IT/Communications
  - Railroad police
- All AAR members implement

Railway Alert Network (RAN)



Disaster Recovery

- Backup capabilities needed:
  - Train control systems
  - Critical data communications
- Priority restoration needed:
  - Telecommunications systems
  - Data processing
  - Electricity
  - Diesel fuel

Government Support Requested

- Department of Homeland Security
  - IAIP
  - Transportation Security Administration
  - National Communications System
  - FEMA
- Department of Transportation

North American Electric Reliability Council

Critical Infrastructure Protection

ELECTRICITY SECTOR

18 June 2003

Topics

- Electricity Sector
- NERC
- CIPAG
- ESISAC
- Communications

The Electricity Sector

$$\sum_{C=1}^{6} \times 10 \left(\frac{aGen + bTrans + cLSE + dPSE + eRC + fCA + gGov}{3I} \right)$$

Interconnectedness, Interdependencies, Reliability, Security; Guidelines, Standards

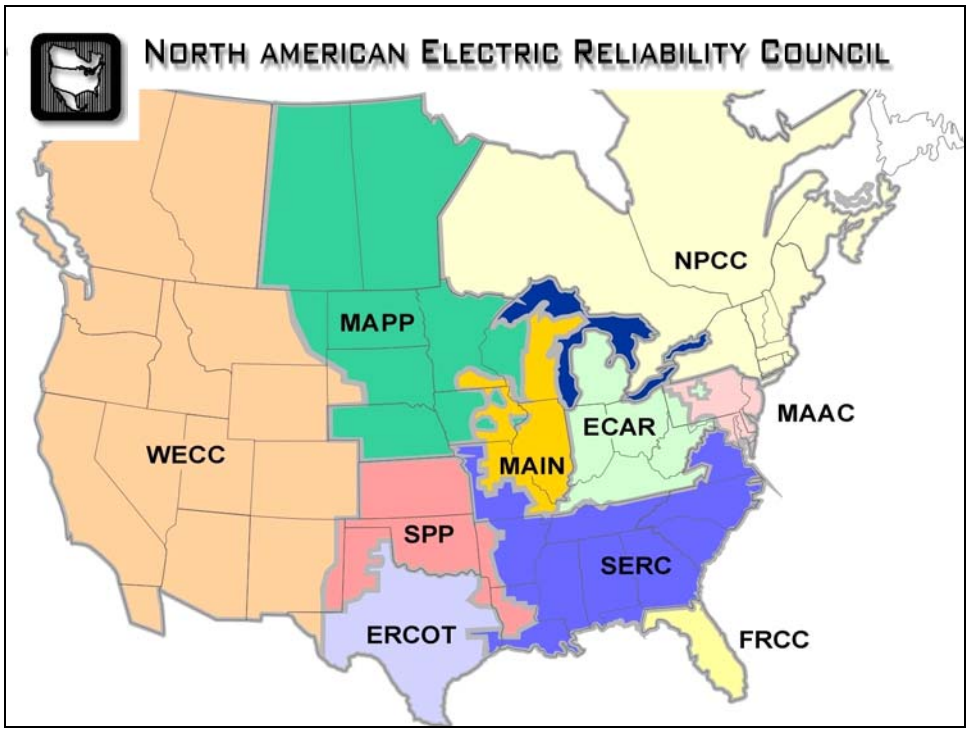
Orgs: NERC, ESISAC, Other ISACs, APPA, CEA, EEI, ELCON, EPRI, EPSA, NEI, NAESB, NRECA

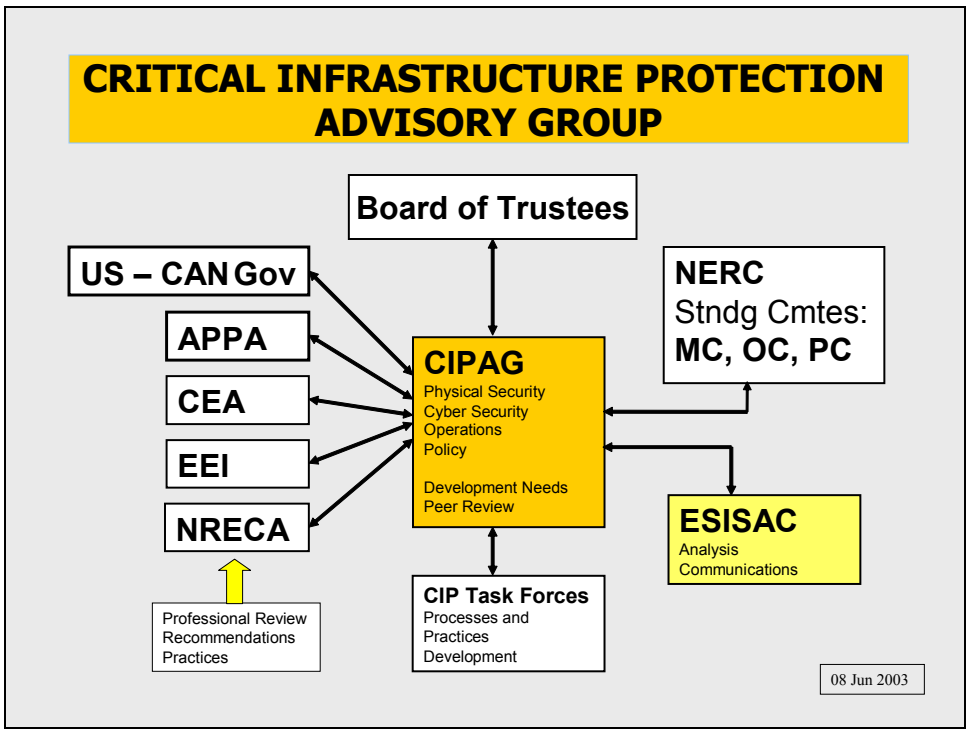
Agencies: DOE, CIAO, DHS, DOD, FERC, NARUC NRC, OCIPEP, RUS, USSS

Definitions and Description

- The equation:
  - Summed over millions of Customers
  - Entity types that comprise the ES
  - Divided by three Interconnections:
    - Eastern
    - Western
    - Texas
- Generation, Transmission, Load Serving Entities, Purchasing-Selling Entities, Reliability Coordinators, Control Areas, Regional Transmission Organizations, Independent System Operators, Regulators (Canada/US: Federal/State/Provincial/Local)

- APPA: American Public Power Association
- CEA: Canadian Electricity Association
- CIAO: Critical Infrastructure Assurance Office
- DOD: Department of Defense
- DOE: Department of Energy
- DHS: Department of Homeland Security
- EEI: Edison Electric Institute
- ELCON: Electricity Consumers Resource Council
- EPRI: Electric Power Research Institute
- EPSA: Electric Power Supply Association
- ES: Electricity Sector
- FERC: Federal Energy Regulatory Commission
- IAIP: Info Analysis, Infrastructure Protection
- ISAC: Information Sharing and Analysis Center
- NAESB: No. Amer. Energy Standards Board
- NARUC: Natl Assoc Reg Utility Commissioners
- NEI: Nuclear Energy Institute
- NERC: North American Electric Reliability Cncl
- NIPC: Natl Infrastructure Protection Center
- NRC: Nuclear Regulatory Commission
- NRECA: Natl Rural Electric Cooperative Assn
- OCIPEP: Office of Critical Infrastructure Protection and Emergency Preparedness
- RUS: Rural Utility Services


NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL
NPCC
MAPP
MAAC
ECAR
WECC
MAIN
SPP
SERC
ERCOT
FRCC


CRITICAL INFRASTRUCTURE PROTECTION ADVISORY GROUP
Board of Trustees
US – CAN Gov
APPA
CEA
EEI
NRECA
CIPAG
Physical Security
Cyber Security
Operations
Policy
Development Needs
Peer Review
NERC
Stndg Cmtes:
MC, OC, PC
ESISAC
Analysis
Communications
CIP Task Forces
Processes and
Practices
Development
Professional Review
Recommendations
Practices
08 Jun 2003

ESISAC Mission

- **Receive** Electricity Sector information for analysis by Government Agencies and the ISAC.
- Provide analytical **support** to the NIPC and other Government Agencies in the interpretation of information relevant to the Electricity Sector.
- Promptly **disseminate** threat indications, analyses, warnings together with interpretations to assist the Electricity Sector in taking protective actions.

Threat Alert Levels


THREAT ALERT SYSTEM
AND PHYSICAL RESPONSE GUIDELINES
FOR THE ELECTRICITY SECTOR

Definitions of Physical Threat Alert Levels

A Model for Developing Organization Specific
Physical Threat Alert Level Response Plans

Version 2.0
October 01, 2002

Developed by
North American Electric Reliability Council (NERC)
Critical Infrastructure Protection Advisory Group

Approved by
NERC Board of Trustees


THREAT ALERT SYSTEM
AND CYBER RESPONSE GUIDELINES
FOR THE ELECTRICITY SECTOR

Definitions of Cyber Threat Alert Levels

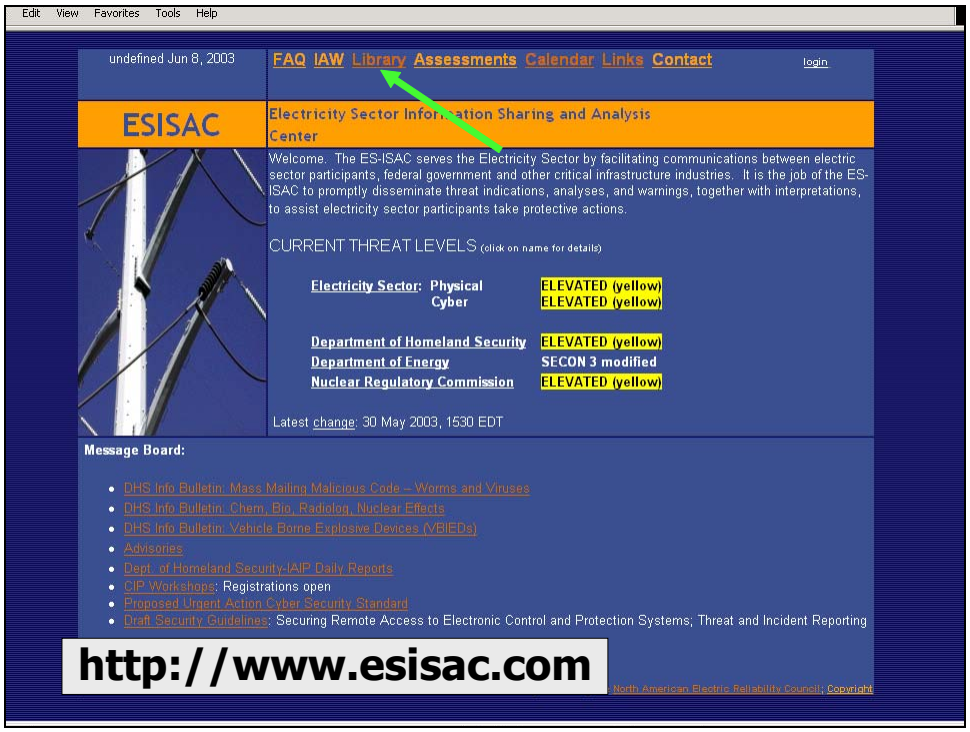
A Model for Developing Organization Specific
Cyber Threat Alert Level Response Plans

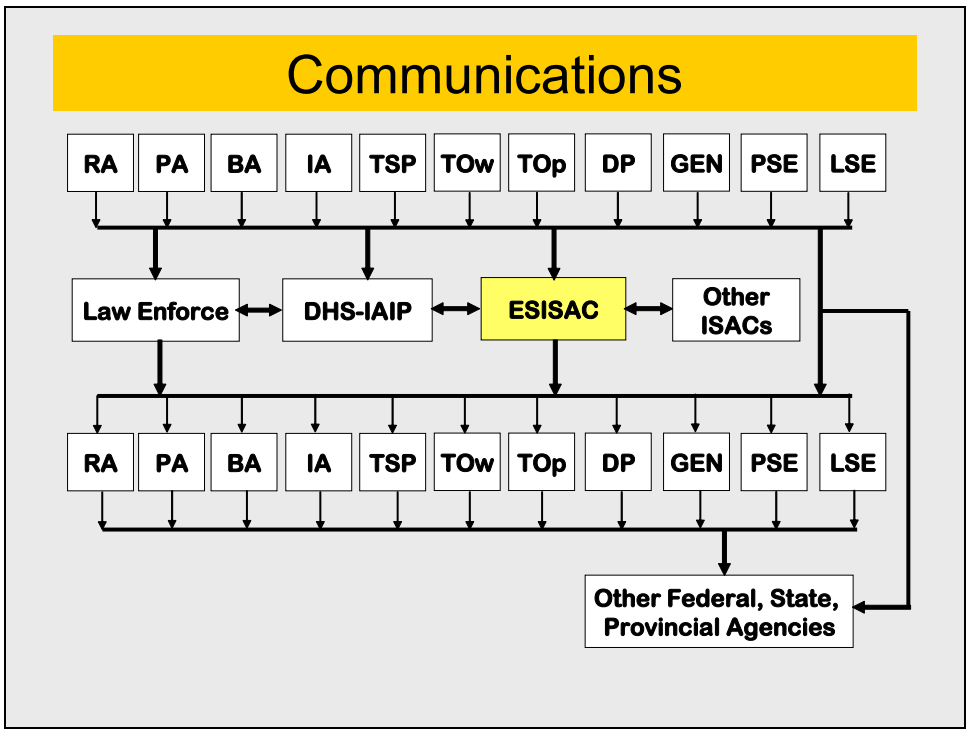
Version 2.0
October 01, 2002

Developed By
North American Electric Reliability Council (NERC)
Critical Infrastructure Protection Advisory Group

Approved by
NERC Board of Trustees

Exercise


Edit View Favorites Tools Help
undefined Jun 8, 2003
FAQ IAW Library Assessments Calendar Links Contact
login
ESISAC
Electricity Sector Information Sharing and Analysis Center
Welcome. The ES-ISAC serves the Electricity Sector by facilitating communications between electric sector participants, federal government and other critical infrastructure industries. It is the job of the ES-ISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions.
CURRENT THREAT LEVELS (click on name for details)
Electricity Sector: Physical ELEVATED (yellow)
Cyber ELEVATED (yellow)
Department of Homeland Security ELEVATED (yellow)
Department of Energy SECON 3 modified
Nuclear Regulatory Commission ELEVATED (yellow)
Latest change: 30 May 2003, 1530 EDT
Message Board:
DHS Info Bulletin: Mass Mailing Malicious Code – Worms and Viruses
DHS Info Bulletin: Chem, Bio, Radiolog, Nuclear Effects
DHS Info Bulletin: Vehicle Borne Explosive Devices (VBIEDs)
Advisories
Dept. of Homeland Security-IAIP Daily Reports
CIP Workshops: Registrations open
Proposed Urgent Action Cyber Security Standard
Draft Security Guidelines: Securing Remote Access to Electronic Control and Protection Systems; Threat and Incident Reporting
http://www.esisac.com
North American Electric Reliability Council; Copyright


Communications
RA
PA
BA
IA
TSP
TOw
TOp
DP
GEN
PSE
LSE
Law Enforce
DHS-IAIP
ESISAC
Other ISACs
RA
PA
BA
IA
TSP
TOw
TOp
DP
GEN
PSE
LSE
Other Federal, State, Provincial Agencies

REPORT INCIDENTS TO

1. **LOCAL LAW ENFORCEMENT**
   Establish and maintain relationship
2. **LOCAL FBI**
   Establish and maintain relationship
3. **DHS-IAIP IAW Program**
   InfraGard; CIPIS; nipc.watch@fbi.gov
   202-323-3204,5,6
   888-585-9078
4. **ESISAC**
   CIPIS
   [https://www.nerc.net/registration/]
   esisac@nerc.com
   609-452-8060 [day]
   609-452-1422 [anytime]

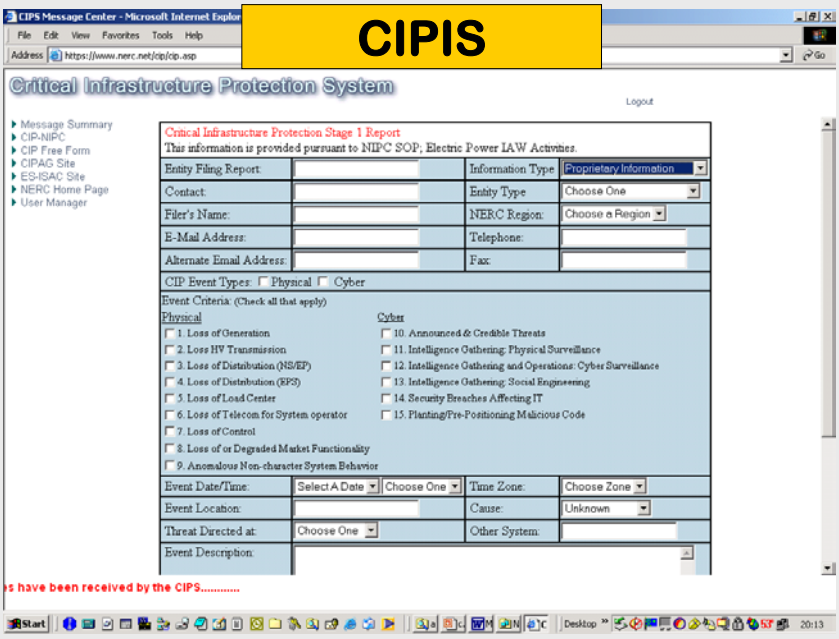
Communication Types

- Incident data for analysis
  - From Electricity Sector (ES) entities
  - To DHS-IAIP and ESISAC
  - To ES entities as determined by inputting entity
- Threat Alerts, Advisories, Warnings, other information
  - To ES entities
    - Sector, Area, Type facility, Specific facility
  - From DHS-IAIP and ESISAC

Communications Mechanisms

- Critical Infrastructure Protection Information System (CIPIS)
- Email listservers
  - Lists with pager and text cell phones included
- Hotline: Reliability Coordinators on shift
- Conference calls
- Specific entity by telephone
- Voice message system (under development)
- Out of band communication (future)

CIPIS



IAW Program Reporting Events

- Loss of Generation
- Loss HV Transmission
- Loss of Distribution (NS/EP)
- Loss of Distribution (EPS)
- Loss of Load Center
- Loss of Telecom for System operator
- Loss of Control
- Loss of or Degraded Market Functionality
- Anomalous Non-character System Behavior
- Announced & Credible Threats
- Intelligence Gathering: Physical Surveillance
- Intelligence Gathering and Operations: Cyber Surveillance
- Intelligence Gathering: Social Engineering
- Security Breaches Affecting IT
- Planting/Pre-Positioning Malicious Code

Other ES Initiatives

- Public Key Infrastructure
- Process Control Systems
- Spare Equipment Project
- Security Standard and Guidelines:
- CIP Workshops:

Security Guidelines

- Overview
- Communications
- Emergency Plans
- Employment Background Screen
- Physical Security
- Threat Response
  - Physical
  - Cyber
- Vulnerability/Risk Assessment
- Continuity of Business Process
- Cyber Access Control
- Cyber IT Firewalls
- Cyber Intrusion Detection
- Cyber Risk Management
- Protecting Sensitive Info
- Securing Remote Access: Process Control Systems
- Incident Reporting
- Cyber Security STANDARD

North American Electric Reliability Council

Meeting The Security Challenge Workshops

26-27 Feb	**Dallas, TX**
13-14 Mar	**Phoenix, AZ**
27-28 Mar	**Seattle, WA**
10-11 Apr	**DC area**
24-25 Apr	**Orlando, FL**
29-30 May	**Denver, CO**
18-19 June	**Chicago, IL**
24-25 July	**Boston, MA**
Sep (date tbd)	**Canada (loc tbd)**

TY

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC)

Mission

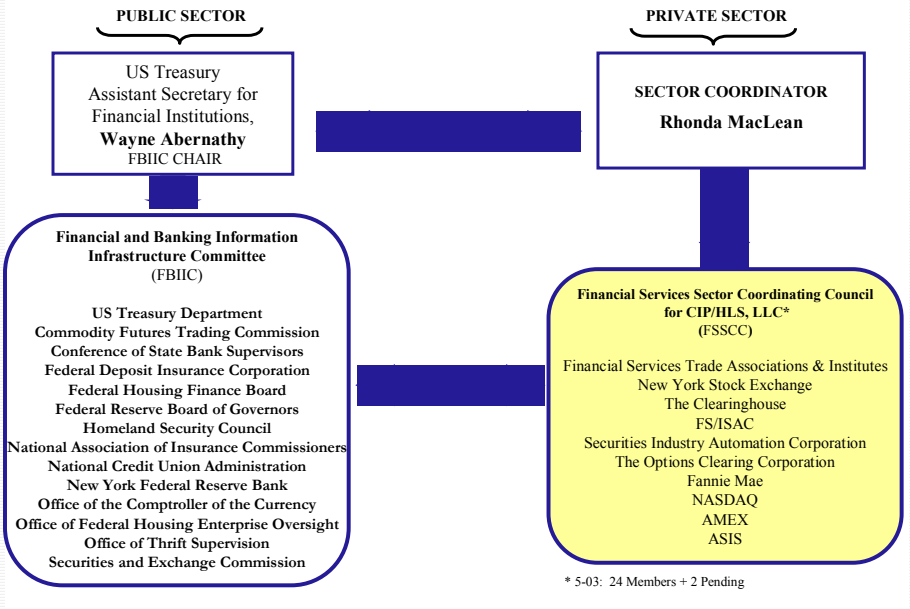
- Foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security.

Objectives

- Provide broad industry representation for CIP/HLS and related matters for the financial services sector and for voluntary sector-wide partnership efforts.
- Foster and promote coordination and cooperation among participating sector constituencies on CIP/HLS related activities and initiatives.
- Identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS

5

Financial Services Cyber and Physical Protection Public-Private Partnership Framework



Members of the FSSCC

- **ABA** – American Bankers Association
- **ACLI** – American Council of Life Insurers
- **ASIS** – American Society for Industrial Security
- **ACB** – America's Community Bankers
- **BAI** – Bank Administration Institute
- **BITS/FSR** – BITS and The Financial Services Roundtable
- **CUNA** – Credit Union National Association
- **Fannie Mae**
- **CBA** – Consumer Bankers Association
- **FS/ISAC** – Financial Services/Information Sharing and Analysis Center
- **FIA** – Futures Industry Association
- **ICBA** – Independent Community Bankers of America
- **ICI** – Investment Company Institute
- **MFA** – Managed Funds Association
- **NASD** – NASD, Inc.
- **NASQ** – NASDAQ Stock Market, Inc
- **NAFQU** – National Association of Federal Credit Unions
- **NACHA** – National Automated Clearinghouse Association
- **SIA** – Securities Industry Association
- **The BMA** – The Bond Market Association
- **The Clearing House**
- **The OCC** – The Options Clearing Corporation

7

One Sector's Current Response: The Financial Services Sector

Incident May Be Reported to:

FSSCC

or

FS/ISAC

or

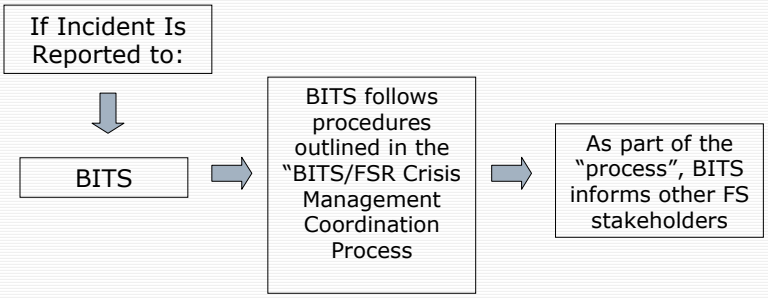
FS Association (i.e., ABA, BITS)

Each would launch their "crisis management coordination" process.

Most processes feed into the others.

8

One FS Association's Response: BITS



9

The BITS/FSR CMC Process

Component	Purpose
Monitoring & Activation	"Always on" and used to determine if the Crisis Management Process should be activated.
Notification	Activates the BITS/FSR Crisis Communicator, establishing guidance for who is contacted and by what means.
Assessment	Assesses the scope and severity of the event to facilitate the development of an action plan and determine the appropriate level of response throughout the crisis.
Response	Guides the discussions and collective actions for managing the event.
Recovery	Guides the discussions and collective actions during the perceived end of the event.
Disengagement	Terminates the recovery and assesses the effectiveness of the process after a crisis is declared to be over.
Information Management	Records and manages all aspects of crisis-related information processes.
Messaging	Disseminates appropriate information to targeted audiences.
Training and Exercising	Audits and exercises procedures on an ongoing basis, as well as trains participants.

10

NATIONAL COMMAND CENTER TAB 4

<u>Issue 4</u> – A National Command Center does not exist as a confluence point for the private sectors during times of crisis.

<u>Recommendation:</u> Establish a virtual command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency situation.

The Homeland Security Operations Center (HSOC):

- Maintains and shares continuous domestic situational awareness
- Conducts initial information assessment and threat monitoring to detect, deter, and prevent terrorist incidents
- Coordinates and monitors homeland security operations

As impressive as this charter is, it does not include the private sector and it is the understanding of the NIAC that inclusion of the private sector will not occur for two years. Therefore, we recommend that until the plan to include the private sector is implemented, HSOC devise a private sector virtual command center and brief the critical infrastructures as appropriate.

GOVERNMENT-SPONSORED EXERCISES_____TAB 5

<u>Issue 5</u> – Government-sponsored exercises (e.g., TOPOFF2) should actively solicit private industry representation.

<u>Recommendation</u>: DHS should sponsor crisis management exercises that include the participation of the critical infrastructures, as soon as possible, and annually thereafter.

In private industry, critical business functions are required to be tested at least on an annual basis. We recommend that regional, cross-sector exercises are held on an annual basis in major U.S. cities.

DEPENDENCY ON THE INTERNET TAB 6

Issue 6 – There is an underestimation of the dependency of the nation's critical infrastructures on the Internet.

Recommendation: Enhance awareness of Internet dependencies.

Most organizations, regardless of sector, tend to underestimate their reliance on the Internet. This underestimation generally comes in two forms: either the organization assumes it still has sufficient fallback processes to return to pre-Internet business models, or it discounts the damage that a critical, non-failure event can have (such as a worm or virus). Many organizations, in making their early transitions to Internet-based models, kept in place legacy processes in the event a fallback was required. Over time, these processes became outdated, personnel were no longer proficient in them, or the support infrastructure was no longer in place to manage them. Internal departments have made strides in adopting new technologies, which may not be visible to upper management. Both factors contribute to a belief at executive levels that the Internet itself is not a critical system. Most faults in critical systems are believed to be failure-oriented (such as the recent blackout across the Northeast). For the Internet, many faults are not failure-oriented—indeed, the most devastating attacks are from worms and viruses that infect systems, sometimes impacting back-end systems such as a bank's ATM network or manufacturing systems. These non-failure faults are generally not considered when assessing Internet reliance.

INTERNET SURVEY QUESTIONS

Organizations should consider the following "Internet Survey Questions" in order to assess their dependence on cyberspace:

1. What revenue based products would be unavailable do to their reliance on the internet?
2. What is the estimate of the revenue that would be lost for a week from the above product not being available?
3. What customer service products would be unavailable?
4. What internal processing supported applications would be broken?
5. What information/marketing tools would be impacted?
6. What regulatory impacts would you see?
7. Are there other impacts?

EXCERPTS FROM THE TESTIMONY OF RICHARD D. PETHIA
Director, CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Before the House Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats?

September 10, 2003

Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from viruses and worms can have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk. Solutions are not simple but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. We can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

RECOMMENDED ACTIONS – WHAT CAN SYSTEM OPERATORS DO?

Adopt security practices: It is critical that organizations, large and small, adopt the use of effective information security risk assessments, management policies, and security practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources, including the CERT/CC. The Internet Security Alliance, for example, has recently published a "Common Sense Guide For Senior Managers" that outlines the security management and technical practices an organization should adopt to improve its security. Guidelines and publications are also available from the National Institute of Standards and Technology, the National Security Agency, and other agencies.

What is often missing today is management commitment: senior management's visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements.

Keep skills and knowledge current. System operators should attend courses that enhance their skills and knowledge, and they should be given the necessary time and support to do so. They need to keep current with attack trends and with tools that help them protect their systems against the attacks. The security problem is dynamic and ever-changing with new attacks and new vulnerabilities appearing daily.

Help educate the users of their systems. System operators must provide security awareness programs to raise users' awareness of security issues, improve their ability to recognize a problem, instruct them on what to do if they identify a problem, and increase their understanding of what they can do to protect their systems,

RECOMMENDED ACTIONS – WHAT CAN TECHNOLOGY VENDORS DO?

The steps available to system operators will help, but will only solve parts or the problem. Technology vendors are in a position to prevent the spread of worms and viruses more effectively. Although some companies have begun moving toward improvement in the security in their products, there is a long way to go. Software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. The CERT/CC continues to see the same types of vulnerabilities in newer versions of products that were in earlier versions.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications. These products are complex and often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of properly enabling the security features they need. While the current practices allow the user to start using the product quickly and reduce the number of calls to the product vendor's service center when a product is released, it results in many Internet-connected systems that are misconfigured from a security standpoint. This opens the door to worms and viruses.

It is critical for technology vendors to produce products that are impervious to worms and viruses in the first place. In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- **Virus-resistant/virus-proof software.** There is nothing intrinsic about computers or software that makes them vulnerable to viruses. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow that code to be executed without constraint on the machine that received it. Unconstrained execution allows program developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, are more recent.
- **Dramatically reducing implementation errors.** Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while the products are in use. In many cases, identical flaws are continually reintroduced into new versions of products. The great majority of these vulnerabilities are caused by low level design or implementation (coding) errors. Vendors need to be proactive, study and learn from past mistakes, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- **High-security default configurations.** With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by

shipping products with "out of the box" configurations that have security options turned on rather than require users to turn them on. The users can change these "default" configurations if desired, but they would have the benefit of starting from a secure base configuration.

RECOMMENDED ACTIONS – WHAT CAN THE GOVERNMENT DO?

The government can help by taking a multi-pronged approach. Actions that I believe should be investigated include the following:

Provide incentives for higher quality/more security products. To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses—clauses that hold vendors more accountable for defects, including security defects, in released products and provide incentives for vendors that supply low defect products and products that are highly resistant to viruses. The lower operating costs that come from use of such products should easily pay for the incentive program.

Also needed in this area are upgraded acquisition processes that put more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, acquisition professionals need to be given training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is essential in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.

Information assurance research. It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

Thus, the government should support a research agenda that seeks new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

More technical specialists. Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

More awareness and training for Internet users. The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one's own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.
- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries. Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

The National Cyber Security Division (NCSD), formed by the Department of Homeland Security in June 2003, is a critical step towards implementation of these recommendations. The mission of NCSD and the design of the organization are well-aligned to successfully coordinate implementation of the recommendations that I have described here. However, implementing a "safer-cyberspace" will require, the NCSD and the entire Federal government to work with state and local governments and the private sector to drive better software practices, higher awareness at all levels, increased research and development activities, and increased training for technical specialists.

COORDINATION IN PLANNING BETWEEN PUBLIC AND PRIVATE SECTORS TAB 7

Issue 7 – Coordination in planning and response between public emergency management (federal, state, and local) and private critical infrastructure is inadequate and/or inconsistent.

Recommendation: Provide a framework for public and private emergency management interaction including national, sector, state, regional, and local levels. This framework should integrate with public and private information sharing models and must account for ISACs and InfraGard, as well as review of significant regional public/private partnerships.

DHS should create a framework for public and private emergency management interaction that includes private companies and critical infrastructure sectors in its scope, as well as geographic and governmental levels of local, regional, state, and I emergency managers.

The Incident Command System (ICS) has been widely adopted as the standard for command, coordination, and communication between diverse government and emergency response entities. At present, the National Incident Management System (NIMS) is the program DHS is currently developing to establish formal incident management protocols throughout the United States, likely encompassing ICS.

While public emergency managers using ICS at the state and local level occasionally address private-sector critical infrastructure issues, this is not consistent and does not adequately account for all infrastructure sectors, nor does it provide uniform structure for interaction with these sectors at all government levels.

If NIMS is intended to replace ICS as the structure for incident management throughout the United States, detailing a critical infrastructure role within NIMS can effectively ensure the public/private partnership in emergency management planning and crisis response at all government levels.

Identification of critical infrastructure as a role within NIMS should include at a minimum: identification of critical infrastructure organizations within the planning area; communication authorities and credentialing of infrastructure company staff for interaction with emergency functions, such as an Emergency Operations Center (EOC) and for access into company property within disaster-impacted areas; and priority designation of resources to aid cross-sector critical infrastructure recovery and reconstitution.

1. Two significant problems hamper effective information sharing and crisis management todayIfederal, state, and city entities have implemented their own information-sharing initiatives. While these initiatives may increase the sharing of information to fight terrorism, they are not well coordinated and consequently risk creating partnerships that may actually limit some participants' access to information and duplicating efforts of some key agencies in each level of government. Moreover, while beneficial to these participants, the initiatives do not necessarily integrate others into a truly national system and may for this reason inadvertently hamper information sharing. A lack of effective integration could increase the

risk that officials will overlook or never even receive information needed to prevent a terrorist attack[7].

2. There seems to be redundancy and potentially competing objectives between DHS and the FBI's InfraGard.[8]

I

In order to aid emergency managers in working with private critical infrastructure companies, DHS should promote a model for the private-sector that is similar in principle to ICS (see Business Incident Coordination System below). In particular, consideration should be given to the designation of a role, a Homeland Security Officer, within a private sector-company as the primary interface with public emergency management entities.

Recommended Short-term Actions:

1. Immediately review the upcoming National Incident Management System to ensure inclusion of privately held critical infrastructures in final version.
2. Ensure there is no duplication of efforts between InfraGard (FBI) and DHS. If conflicting or competing objectives exists, the issue should be escalated for rIon within the federal government.
3. Provide short overview guide to critical infrastructure crisis management for private companies (see *Business Incident Coordination System* in Tab 7) and for governors, including recommendation for designation of Homeland Security Officers for companies.

Recommended Long-Term Actions:

1. Crisis and emergency management require trusted and reliable communication networks, both digital and human. As a result, a public/private emergency management framework must leverage the same networks used to share information about threats and risk mitigation. DHS should develop a national framework for information sharing and emergency management (see *National Crisis Management Partnership* diagram in Tab 7), accounting for and integrating with significant information sharing networks, particularly ISACs and InfraGard.
2. Ensure this model includes a regional component. Significant regional models throughout the United States should be reviewed to develop a single best model, including ChicagoFIRST, Portland, Oregon RAINS, and other large-scale models.
3. DHS should include interaction between public and private emergency management in a guidebook (mentioned above) for critical infrastructure protection and crisis management written for use by critical infrastructure companies and state and local emergency management agencies. The guide m'y be similar to *"A Governor's Guide to Emergency Management Volume Two: Homeland Security"*.[9]

---

[7] Homeland Security – Efforts to Improve Information Sharing Need to Be Strengthened (GAO-03-0760)

[8] InfraGard is a partnership between the FBI and 9,000 private companies through 56 local InfraGard Chapters. Infragard was created to provide a forum for sharing between law enforcement and other local officials and private sector companies.

[9] http://www.nga.org/cda/files/GOVSGUIDEHS2.pdf

BUSINESS INCIDENT COORDINATION SYSTEM (EXAMPLE)

Chris Terzich, Wells Fargo & Company

INTRODUCTION

The principles of the Business Incident Coordination System (BICS) are based on the principles followed by the Incident Command System (ICS) for nearly 30 years to enable first responders from varied entities and functions to work together effectively. During this time, there have been many endorsements of this system, including advocates for its use within the business community. The organizational components of ICS (Command, Operations, Planning, Logistics, and Finance) do not transfer very well to the business environment and ICS has never gained widespread use in business. Some key principles of ICS, however, that are applicable and effective in the business environment include:

- Common Organization and Terminology
- Modular Organization

COMMON ORGANIZATION AND TERMINOLOGY

Private organizations vary greatly in terms of terminology, particularly with regard to internal functions or departments. For example, some organizations call their information technology area IT (Information Technology), while others call it Infrastructure, Systems, DP (Data Processing) or some other term. These terms describe groups that may also fulfill varied functions. In other words, an IT area in one company is not only different in name from another; it differs in function and responsibility as well.

In order to plan and respond effectively, there are certain terms and organizational functions that can be generalized to allow for coordination between businesses and public emergency personnel the following common terms and functions can be used:

1. ***Homeland Security Officer*** – This is the person or function responsible for implementation of BICS within a company. Key functions below may or may not organizationally report to this person. Specific responsibilities of the Homeland Security Officer include:
   - 1.1. Company or enterprise level coordination with HomelanIity functions at the overnmentate and local levels of government
   - 1.2. Designation, if applicable of Regional or Local Homeland Security Liaisons
   - 1.3. Activation and expansion of BICS
2. ***Management*** – There are many levels of management within some companies. During an incident, Management refers to the decision-makers. If a single building is involved, this may be a departmental manager in that building. Management within BICS is responsible for:
   - 2.1. Making decisions, when supported by the process in this document regarding business open or close status
   - 2.2. Communications to employees
   - 2.3. Community support activities (donations to Red Cross, collection of funds, offering of shelter space, etc.)
3. ***Physical Security*** – This is the function responsible for making security plans and/or managing uniformed guards. When an outside guard company provides security guards, this function is the responsibility of the department or direct employee who works with the vendor. Responsibilities of physical security include:

3.1. Liaison with law enforcement
3.2. Sharing of physical security information with BICS function, providing guidance based on level of expertise

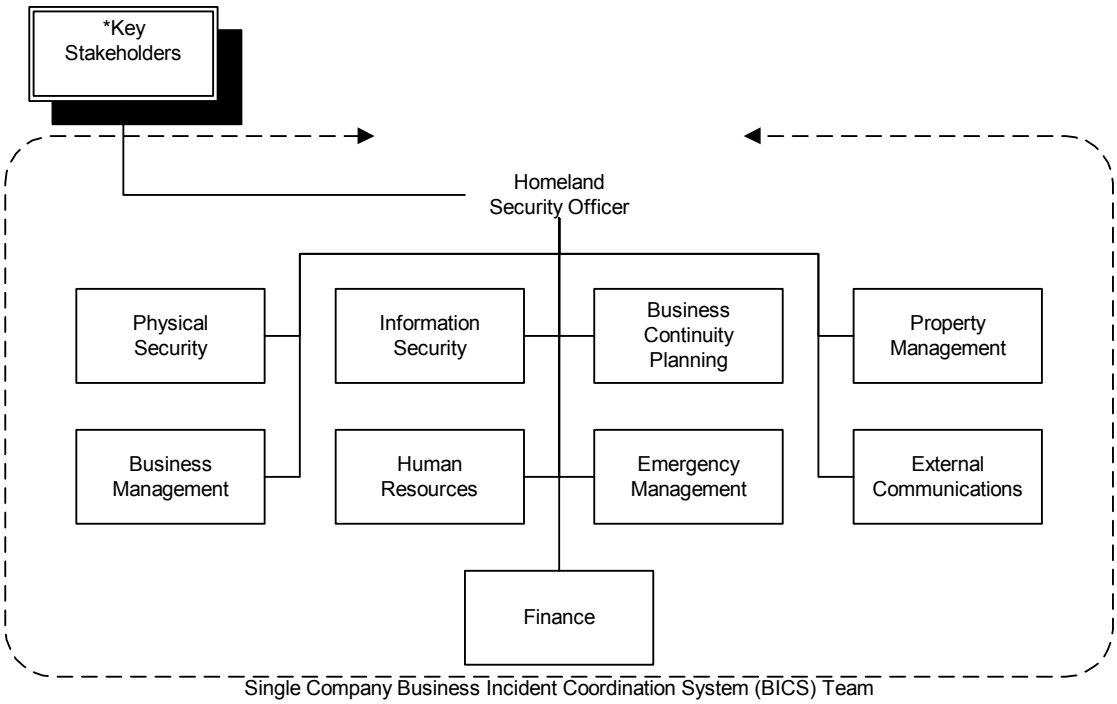
4. ***Information Security*** – Information security is responsible for security of data systems and processes. Responsibilities of Information Security during an incident include:
   4.1. Continuously assess threats and vulnerabilities
   4.2. Implement security controls and remediation
   4.3. Sharing of physical security information with BICS function, providing guidance based on level of expertise
5. ***Human Resources (HR)*** – The human resources function is responsible for support of employees regarding employment issues. During an incident, HR function is responsible for:
   5.1. Trauma support
   5.2. Time away from work
   5.3. Overtime
   5.4. Other staffing issues
   5.5. When these functions are not staffed internally to the company, the HR function is responsible for coordination of external resources
6. ***Property Management*** – Some businesses own their facilities while many others lease workspace. The property management function within BICS is responsible for all company issues related to the property owned or used by the company. Specific responsibilities during an incident include:
   6.1. Working with local officials and the BICS system regarding building safety issues
   6.2. Coordinating and/or conducting damage assessment
   6.3. Property vendor coordination
7. ***Business Continuity Planning (BC or BCP)*** – Sometimes called disaster recovery, business contingency planning or some other variation. This function is responsible for coordination and monitoring of:
   7.1. Interim business actions
   7.2. Movement to alternate site
   7.3. Recovery of business function at alternate site
   7.4. Restoration of work (data or other)
8. ***External Communications*** – Often called Public Relations or PR, the external communications offers a single point of contact for any public or media inquiries of the company. Specific responsibilities include:
   8.1. Fielding on-site public inquiries
   8.2. Fielding of media inquiries
   8.3. Support for BCS preparation of written communications
9. ***Risk Management*** – Risk management is a field that varies significantly from industry to industry and company to company. For the purpose of BICS, the Risk Management function is responsible for:
   9.1. Insurance issues and loss tracking
   9.2. Monitoring of OSHA or other safety regulations
   9.3. Monitoring and administration of Workers' Compensation issues
10. ***Finance*** – The finance area may be responsible for such things as payroll, accounts payable and accounts receivable. In support of BICS, finance is responsible for providing emergency funding of response and employee costs.

MODULAR ORGANIZATION

Webster's defines modular as "*constructed with standardized units or dimensions for flexibility and variety in use*." This was the key to the success of ICS and is the key to success of BICS.

The modular organization of this system starts with the Homeland Security Officer. This person is responsible for the process and for activation and expansion. Unlike ICS, however, this person is not necessarily an incident commander. The concept of the first responder on the scene does not translate well in business. Nonetheless, an organization must clearly define authority lines and ensure either multiple layers of accessible management (i.e., chain of command), or must provide for decisions to be made at the site of an emergency with procedural guidance. As a rule, the more decisions can be made in advance of an emergency, the better the group will function during an emergency. Decisions made in planning should center on process, rather than detailed procedures that will be difficult to access under pressure.

The organizational structure used by BICS develops in a modular fashion, based upon the information initially known about a threat or incident impact. In this diagram, the only role that must be staffed is the Homeland Security Officer. As the complexity increases, more people will fill the roles, ultimately with teams and sub-teams filling each role. Here is a diagram that shows the organization:



* Key Stakeholders represent those who may or may not immediately participate in the Business Incident Coordination System (BICS). In some companies, this may be executive management, the board of directors or simply shareholders, customers and the community.

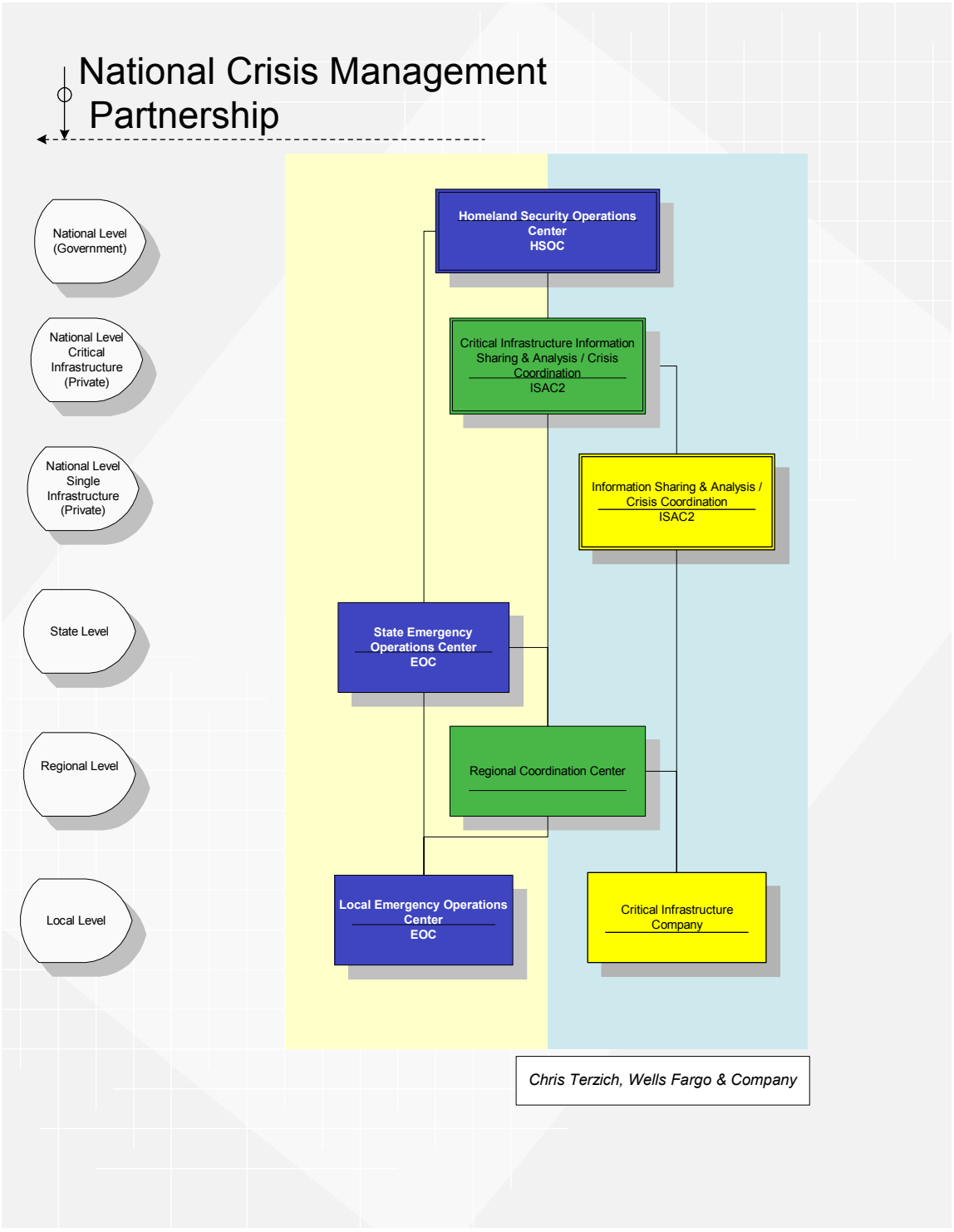
One critical point to make about this structure is that it does not require fulltime, permanent organizational changes within a company. There are many professionals in these various fields discussing the urgent need to align their activities with those in other disciplines. In fact, some advocate similar consolidations of functions. However, the key difference in each perspective is that

the Homeland Security Officer, or senior management role is determined by the perspective of the writer (i.e., if written in a Business Continuity Planning publication, the BCP function should integrate all).

To assume that this improved alignment requires establishment of a Homeland Security Officer as a new executive-level position, reporting to the Chief Executive Officer is a mistake and may even be counterproductive. Establishment of such a position would undoubtedly indicate a company commitment to preparedness. It would also likely accelerate adoption of effective incident management practices. However, all companies are different and the ideal candidate for Homeland Security Officer may be fulfilling one of these roles or a separate role altogether.

Executive management should designate a Homeland Security Officer with periodic reporting on the implementation of this system.

NATIONAL CRISIS MANAGEMENT PARTNERSHIP (EXAMPLE)



LACK OF INCENTIVES TAB 8

<u>Issue 8</u> – There is a lack of incentives that would help defray the additional expense burden resulting from strengthening the resiliency of the critical infrastructures.

<u>Recommendation</u>: Explore the potential for creating tax incentives or other instruments to incent the private sector to enhance the resiliency of the critical infrastructures.

Post 9/11, there is certainly a heightened corporate awareness of the need to strengthen the resiliency and security of the critical infrastructures. The cost burden associated with these corporate investments is substantial. However, it is critical for our nation and our economy that these improvements are made as rapidly as possible. This is especially true for corporate entities considered to be part of our nation's critical infrastructure. A single incident with one of these entities could have catastrophic cascading effects on interdependent organizations and services.

To encourage private-sector investment in strengthening our infrastructures, we recommend that financial incentives be provided to these companies. Without incentives to help defray the additional expense burden, many organizations will be forced into protracted and/or delayed implementations while our nation remains potentially vulnerable.

RESEARCH & DEVELOPMENT AND MODELING CAPABILITIES TAB 9

Issue 9 – Sophisticated modeling capabilities exist at the national laboratories and multiple research and development (R&D) studies on cross-sector interdependencies have been completed.

Recommendation: The national laboratories should focus their interdependency modeling and research on the regions and sectors whose failure would have the highest impact on the economy and national security. The Working Group suggests starting with modeling the telecommunications and energy sectors and the interdependencies among them and the other critical infrastructures. Additionally, existing R&D studies need to be indexed and cross-referenced in such a way as to make these materials accessible to appropriate parties.

It is clear that substantial effort and investment has gone into an equally substantial number of modeling efforts and studies on cross-sector interdependencies. The Study Group reviewed and abstracted 37 studies and received a briefing on the capabilities of the National Infrastructure Simulation and Analysis Center (NISAC). The information resulting from both the modeling efforts and the studies needs to be leveraged by appropriate parties so that the lessons learned can be implemented and built upon before additional efforts are launched.

NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER (NISAC)

Title: A National Infrastructure Simulation and Analysis Center (NISAC): Strategic Leader Education and Formulation of Critical Infrastructure Policies

Centre for Strategic Leadership, US Army War College, Published: August, 2003
Author(s): COL William Wimbish and MAJ Jeffrey Sterling

Executive Summary: With the collapse of the World Trade Center Towers, many national policy makers feared the financial markets would follow, causing a cascading breakdown of other critical infrastructure assets. Fortunately, our worst nightmare failed to materialize, but the need to protect and to better understand our nation's critical assets was unmistakable. The clarion from the 9/11 terrorist's attack calls for strategic leaders to understand the complexity, interdependency, and vulnerability of our infrastructure. The National Infrastructure Simulation and Analysis Center (NISAC) provides an unparalleled modeling, simulations, and analysis capability to assist the military's Senior Service College (SSC) community in educating future strategic leaders about the realities of the Nation's infrastructure system and in researching the effects that new government security policies and actions would have on the nation's critical assets and public and private sector services.

.

MATRIX AND ABSTRACTS OF REPORTS ON CRITICAL INFRASTRUCTURE INTERDEPENDENCIES

Thirty-seven publicly accessible research reports were identified on critical infrastructure interdependencies. The research pertains to the various critical sectors as follows:

- All Sectors 11
- Energy 22
- Water 6
- Telecom 5
- Transportation 3

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations

All sectors	Infrastructures Interdependencies: Overview of Concepts and Terminology	N/A	Lindsey	• Excellent overview of concepts and terminology
				• Read in tandem with PowerPoint presentation – Report #2 below
				• Would like to see entire paper
					• Understanding, analyzing, and sustaining the robustness and resilience of these infrastructures require multiple viewpoints and a broad set of interdisciplinary skills
					• Infrastructure interdependencies can be described in terms of four general categories:
					  • Physical (e.g., the material output of one infrastructure is used by another)
					  • Cyber (e.g., infrastructures utilize electronic information and control systems)
					  • Geographic (e.g., infrastructures are co-located in a common corridor), and
					  • Logical (e.g., infrastructures are linked through financial markets)
					• Physical, cyber, geographic, and logical infrastructure interdependencies transcend

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations

					individual infrastructure sectors (by definition) and generally transcend individual public and private-sector companies
					• Failures affecting the interdependent infrastructures depicted in Fig. 3 can be described in terms of three general categories:
					  • Cascading failure – A disruption in one infrastructure causes a disruption in a second infrastructure
					  • Escalating failure – A disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g., the time for recovery or restoration of an infrastructure increases because another infrastructure is not available)
					  • Common cause failure – A disruption of two or more infrastructures at the same time is the result of a common cause (e.g., natural disaster)
					• An understanding both of backup systems or other mitigation mechanisms that reduce interdependence problems and of the change in interdependencies as a function of outage duration and frequency is necessary
					• The key point is that interdisciplinary expertise and research are needed to address these dimensions. To be successful, this effort will require cooperation and

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					collaboration among infrastructure and interdependency experts from government, industry, academic and research institutes, and the national laboratories. It also will necessitate focused education and awareness efforts to prepare professionals to understand fundamental interdependency concepts and issues and the "system of systems" paradigm.

All sectors	Infrastructure Interdependencies	12/01	Lindsey	• Supporting material for Report 1/A above
				• Different author than Report 1/A – based on the article
				• Lists technical R&D challenges, practical issues in understanding interdependencies, policy research issues and social, business and anthropological research – but stops short of making recommendations for "next steps"
					• Definitions:
					  • Dependency: A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other
					  • Interdependency: A bidirectional relationship between two infrastructures, through which the state of each infrastructure influences or is correlated to the state of the other infrastructure. More generally, two infrastructures are interdependent when each is dependent on the other
					• Interdependency Considerations
					  • Increasing reliance on information technology and telecommunications has increased interdependencies
					  • Interdependencies transcend individual public and private sector companies
					  • Infrastructure linkages vary significantly in

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					scale and complexity – local, regional, national, international • Gaps exist is capability to analyze multiple contingency events involving interdependent infrastructures • Understanding interdependencies requires examining multiple dimensions • Dimensions for describing infrastructure interdependencies • Type of failure • Infrastructure characteristics • State of operation • Types of interdependencies • Environment • Coupling and response behavior
All sectors	Interdependencies in Civil Infrastructure Systems	Winter 01	Lindsey	• The paper focuses on the tension between the need to push civil infrastructure systems to higher levels of efficiency and competitiveness and the need to ensure minimum levels of service, reliability, and security, even under critical conditions • Stresses the need for more attention and study and proposes new frameworks for understanding systems of infrastructure systems	• Information systems can make or break infrastructure • Further efficiencies might be difficult to realize because of trade-offs with induced vulnerabilities • In addition to cyber attacks, infrastructure systems are vulnerable to myriad stresses and failures as a result of everyday interdependencies, insufficiencies and inefficiencies • The vulnerabilities must be understood, predicted, sensed and engineered to meet multiple performance measures • Despite the challenges, modeling systems of

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					infrastructure systems, whether CAS or not, is necessary for optimal life-cycle management of civil infrastructure systems • Although new methods and tools for individual infrastructure system models have been evolving, fewer attempts have been made, and even fewer successes attained, at modeling meta-infrastructure systems • Infrastructure systems, which were engineered to facilitate the competitive flow of people, goods, energy, and information, have expanded far beyond their original design specifications. To meet the exigencies of our greatly changed world, we must rethink and reengineer infrastructure systems life cycles to serve their original purposes under new conditions, such as globalization, deregulation, telecommunications intensity, and increased customer requirements.
All sectors	*Recovering from Disruptions of Interdependent Critical Infrastructures	09/01	Terzich	While infrastructures are complex and dynamic, modeling of relationships and impacts of outages is possible. Wide ranges of variables can impact outcome significantly. This paper elaborates on this and describes work underway at Sandia labs. No conclusions or recommendations	• Infrastructures are complex, dynamic, interdependent and adaptable • Assessment of risk must account for this • Some data and relationships can be quantified and applied in models to explore possible effects of system evolution and events • As the interdependencies increase the complexity and alter system responses, the secondary effects and feedback mechanisms may generate unforeseen consequences or

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					reduce the magnitude of what appear to be considerable risks • Research is underway within the Infrastructure Interdependencies Program at Sandia National Laboratories to develop Dynamic system models for specific applications to evaluate the potential effects of infrastructure disruptions on individual systems
All sectors	*Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems	09/01	Terzich	This PowerPoint builds upon the concepts and terminology outlined in 1A above. An overview is provided for a Monte Carlo Simulation model called CI3 – Critical Infrastructures Interdependencies Integrator. This model applies probabilities to many variables within a system or infrastructure to provide an analysis of the duration of disruption	***Purpose of CI3:*** estimate service restoration time o Impacts of disruptions vary as a function of the outage duration o Estimates of outage duration are important in making decisions about system operations and strategies for mitigating vulnerabilities o Duration of outages is uncertain ***Analyzing and Mitigating Vulnerabilities*** o Requires multiple disciplines: engineers (civil, electrical, industrial, mechanical, systems, etc.), computer scientists, information security professionals, economists, lawyers, regulatory and policy analysts, statisticians, decision analysts o Requires new tools (like CI3) to help better understand system operation and response (e.g., to disruptions) o Requires new research How infrastructures are coupled and how disruptions cascade from one infrastructure to another

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					How interdependencies change as a function of outage duration, frequency, and other factors How backup systems or other mitigation mechanisms can reduce interdependence problems and vulnerabilities
All sectors	Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center, A case Study	11/01	Terzich	This summary report highlights some of the direct and indirect impacts of the New York City terrorist attacks, focusing in particular on infrastructure interdependencies, that is, the physical, cyber, geographic, and logical linkages among our nation's critical infrastructures. Direct physical impacts, as well as the subsequent cascading impacts on other infrastructures (i.e., effects that rippled within and among the critical infrastructures), are briefly described. Interdependencies that exacerbated repair and recovery efforts are also noted.	• Impacts and responses are described by sector • Significant impact was noted in all sectors, whether directly affected by the attacks • Airlines were most significantly impacted directly, through loss of traveler confidence or as a result of additional security measures • Power and telecom were noted as causing cascading failures in other sectors • Estimates to restore irretrievable information technology and communications range from $8 billion to $16 billion • Large Manhattan-based businesses with well-tested, sound disaster recovery plans (or geographically distributed communications and computer networks) continued operations almost without interruption • Security heightened in all sectors, cost and economic impact not fully known The economy suffered immediate effects in the wake of the attacks. For example, the cost of

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					energy declined, markets closed, and airline service was suspended. Longer-term effects, such as layoffs, decline in consumer confidence, and financial losses, continue to fuel a downturn in domestic and global economic activity.
All sectors	*Critical Equipment Functionality: Mitigating Natural Hazards Vulnerability	09/01	Terzich	This paper observes that critical equipment systems (CES) within buildings is often not designed to remain functional during and after a natural disaster (e.g., earthquake). A process is outlined to assess the performance expectations and evaluation of mitigation or redundancy of function.	• With support from the Multidisciplinary Center for Earthquake Engineering, the authors developed a method to assess the seismic reliability of individual pieces of equipment subjected to design-level earthquakes • The ad hoc nature of equipment repair can create additional vulnerabilities • The process is consequence-based, incorporating the importance of individual equipment items in a system and uses rapid visual screening techniques intended for use by people without an engineering background ***Summary of Methodology*** (examples and further explanation within the document) 1. Identify critical systems and components, accounting for redundancy 2. Create critical systems diagram to provide a framework for quantification of relative reliability of systems 3. Complete score sheet to measure individual components 4. An overall system score is then determined

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					The conclusion offered is that CES reliability should equal that of the structural reliability.
All sectors	Science and Technology for National Security	N/A	Watson	Two-page brochure for Argonne National Lab's modeling capabilities. Highlights critical infrastructure protection (CIP) support, especially interdependency vulnerability assessments	• Argonne primarily supports Dept of Energy, but has comprehensive understanding of cascading cross-sector effects and dependencies. • Argonne's Infrastructure Assurance Center leverages the entire lab. Program includes : o Vulnerability assessments—physical, operational, cyber, interdependency aspects ; cascading effects of disruptions; improved technologies for preventing and recovering from events o Infrastructure outreach—increase awareness among CI owners/operators o Community critical infrastructure protection program—work with local communities to develop plans and procedures for municipalities to prevent or recover from major disruptions in energy infrastructure • Work to date: o WTC lessons learned study o Support for Utah Olympic Games o Guidelines for electric power disruption (w/City of Chicago, Commonwealth Edison, 270 surrounding municipalities) • Models: o Emergency Response Synchronization Matrix o Integrated Performance Evaluation

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					System ○ Emergency Planner for Special Populations ○ Electric Power Infrastructure Analysis Tools ○ Natural Gas Infrastructure Analysis Tools ○ Petroleum Infrastructure Analysis Tools ○ Water Infrastructure Analysis Tools ○ Military Logistics Infrastructure Analysis Tools ○ Infrastructure Interdependencies Analysis Tools Agent-Based Simulation of Terrorist Networks
All sectors	Information Infrastructure Interdependencies: Systemic Risk Issues	06-07 2002	Watson	• Powerpoint presentation by Joint Research Centre of the European Commission • Referenced previous studies on infrastructure interdependencies; outlined the problem • Highlighted difficulties posed by complexity, lack of consistent definitions, immaturity of research, poor understanding of dependencies Recommended risk management approach, involving cross-sector public-private collaboration; part of	• EC captures security and critical infrastructure protection within umbrella of "dependability." • Dependability includes: ○ Integrity ○ Confidentiality ○ Availability ○ Privacy ○ Accountability ○ Safety • Report highlighted dependence on information and information systems • Recommendations included comprehensive, interdisciplinary R&D (on dependability, risk, modeling/simulation; legal, socio-economic and policy aspects)

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				EC Framework Program 6 (FWP6)	
All sectors	Protecting Critical Infrastructures and Key Assets	N/A	Watson	• This is an 8-page extract from the National Strategy for Homeland Security. • Written prior to formation of DHS, this document outlines goals and objectives for protecting critical infrastructures and key assets. Recommendations are now being implemented by DHS, but many programs are still in their infancy.	• The document outlines rationale to protect critical infrastructures and key assets, defines critical infrastructures, assigns lead agency responsibilities, and outlines key DHS responsibilities. • It highlights the need for public-private and international collaboration. • Major goals and objectives: o Unify America's infrastructure protection effort in the Department of Homeland Security. o Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets. (This is the most challenging goal and the one that is most relevant to this NIAC Working Group's efforts.) DHS "would build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets across critical infrastructure sectors. The Department would thus have a crucial capability that does not exist in our government today: the ability to continuously evaluate threat information against our current vulnerabilities, inform the President, issue warnings, and effect action accordingly" o Enable effective partnership with state

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					and local governments and the private sector o Develop a national infrastructure protection plan o Securing cyberspace o Harness the best analytic and modeling tools to develop effective protective solutions. (Part of this is assessing criticality—not all bridges are critical to the nation, but may be critical to a municipality) o Guard America's critical infrastructure and key assets against "inside" threats o Partner with the international community to protect our transnational infrastructure
All sectors	National Infrastructures as Complex Interactive Networks	'00	Vismor	This document provides the program framework for the Complex Interactive Network/Systems Initiative that was approved in 1998 and started in 1999. It would be good to get an update on where this 5 year project stands.	Many of our nation's infrastructures are complex, networked grids, in which no single entity has control. In addition, traditional mathematical modeling methodologies can not accommodate this level of complexity. The Complex Interactive Network/ Systems Initiative is a five year, $30 million project which was begun in 1999, sponsored by EPRI and DoD, to help develop modeling capabilities for these complex networks. An example related to the August 1996 blackout which resulted in $1.5 billion of damage, could have been avoided by shedding .4 % of capacity for thirty minutes. The objectives of this research is to develop tools and techniques to enable this complex networks to self-stabilize, self-optimize, and self-heal. This will be done

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					through: • Modeling – Understand the true dynamics. • Measurement – Knowing what is happening. • Management – Deciding what to do. By emphasizing mathematical foundations, the project is leading towards a concept of self-healing via systems that are automatically reconfigurable in the event of material failures, threats, or other destabilizing forces.
Transportation	*Improving the disaster Resiliency of Transportation Systems	09/01	Vismor	This document reviews the status of disaster risk mitigation for transportation systems. It also discusses what needs to be done to improve the disaster resiliency of transportation systems.	Because they spread over wide area and are made up of a large number of components subject to failure, transportation systems are very vulnerable to a range of disasters. Today, the knowledge and technology exist to implement effective disaster mitigation practices. A number of obstacles prevent that knowledge and that technology to be used in practice. Lack of information, lack of training, lack of funding, lack of legislation, and lack of enforcement are the most common of these obstacles. The author recommends the following next steps: • Develop a simulation game that would focus on the resilience of transportation systems to disasters • Create a shared library of documented model case studies of successful mitigation initiatives • Create a shared library of studies of impact on transportation systems after windstorms,

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					floods, earthquakes, and other disasters • Set up a Clearinghouse of information and resources on disaster mitigation for transportation systems • Set up a database of specialists in disaster mitigation for transportation systems
Water	Analyzing Water/Wastewater Infrastructure Interdependencies	N/A	Van DeHei	Paper describes four categories of infrastructure interdependencies (physical, cyber, geographic and logical) as they apply to water/wastewater infrastructure. Also discusses the challenges of analyzing water/wastewater infrastructure because of dimensions of infrastructure interdependency that create spatial, temporal, and system representation complexities. A model developed by Argonne National Laboratory to look at impacts of interdependencies on infrastructure repair is also briefly addressed.	• Scale and complexity of interdependencies are not readily understood, so dimensions for describing them are identified: o Type of failure o Infrastructure characteristics o State of Operation o Types of Interdependence o Infrastructure Environment • Argonne National Laboratory has developed a tool to estimate the time and/or cost to restore infrastructure systems, components or networks of systems, called the "Critical Infrastructure Interdependencies Integrator (CI3)", which uses a Monte Carlo simulation. o CI^3 was developed specifically to estimate outage times while considering failures in other infrastructures, as well as the dependencies of water on other systems. Recommendations: additional research needed to better understand linkages to other infrastructures and applying uncertainty

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					techniques.
Water Energy	Blue Cascades Table top Exercise Pacific North-West Economic Region	09/02	Vismor	The Blue Cascades tabletop exercise brought together 70 private and public organizations in the Pacific Northwest with the goal of developing a cooperative preparedness strategy using a risk based approach to enhance the security of critical systems in the region.	Findings: • There was minimal coordination of activities, and little or no understanding of other organizations' interests, response plans or restoration priorities. • No region-wide strategy • Range of services that federal civilian and defense agencies could provide during regional emergencies was not clear. Information was lacking on how regional national defense with significant dependencies on the commercial infrastructure would coordinate with these infrastructures. • There are no dedicated communication channels for infrastructure stakeholders to use to report information to federal, state and local governments. • Roles and missions of the various government authorities at all levels in a large scale regional disruption were unclear. Recommendations: • Improve understanding of regional interdependencies by undertaking region wide identification of what assets are most critical, conducting physical and cyber vulnerability assessments, and identifying/assessing interdependencies.

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					• State and local governments should review, with private sector input, emergency response plans and mutual aid agreements to assure that interdependency related challenges are addressed. • Develop a secure, regional clearing house for interdependencies issues and related preparedness information. • Work with appropriate government organizations to put in place a common, public-private sector, continent wide alert system. Delineate roles and responsibilities of government authorities in regional disruptions.
Energy	Power-Grid Independence Means Better Homeland Security	01/03	Vismor	Paper expounds the virtues of Distributed Generation of electricity versus traditional utility power backed up by generators.	• Distributed Generation (DG) eliminates dependency on conventional power transmission and distribution systems. • Places power at the point of use, in contrast to the electricity gric, which is hundreds of miles of power lines, open to attack and less efficient than the short-wire solution. • Multiple, small systems are less attractive targets. • Traditional back up power devices are dated technology and run a 67% chance of failure in their lifetime.
Water	Technologies, Capabilities, and Expertise for Water and Wastewater	03/03	Van DeHei	This two page paper is a summary of the technologies, capabilities and expertise of Argonne National Lab in this area.	List includes a summary of studies and vulnerability assessments conducted, cost estimates for expanding pipeline structures or implementing redundancies, etc. All items are water/wastewater specific. Mentions

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
	Infrastructures				development of CI3, and RESRAD (radiological exposure model)
Water Transportation Energy	The impact of water, power, and transportation infrastructure failure on the scale of relief operations following a catastrophic natural disaster	09/01	Holmes	PowerPoint presentation delivered at George Washington University – Institute for Crisis, Disaster, and Risk Management on **September 11, 2001.** Study of response programs efforts to estimate displacement and duration of individuals after natural disasters. Specific study of earth quakes in San Francisco. No published papers were found to support the conclusions. One can only infer what was discussed from the PowerPoint slides.	• Traditional response programs are based on risk assessments which rely upon estimates of structural damage to the homes and buildings. • Damage to water, power, and transportation infrastructure can make it impossible for people to support themselves in relatively undamaged homes. • Prediction of infrastructure damage and recovery time is essential to effective response planning • Interdependencies/coupling of infrastructure not well understood • Large uncertainties exist in prediction of damage and prediction of recovery times for infrastructure • Recommends additional research with an objective to identify alternatives for ensuring survival/restoration of critical infrastructure
Water	US House Of Representatives Committee on Transportation and Infrastructure Subcommittee on Water Resources and the	10/01	Vismor	Statement delivered by Jeffrey J. Danneels, Department Manager of the Security Systems and Technology Center at Sandia National Labs. Very good document that clearly describes the necessary steps	A phased approach to improve water infrastructure security is suggested: Near Term: • Threat definition • Information protection • Short-term risk reduction Intermediate Term:

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
	Environment "Terrorism: Are America's Water Resources and Environment at Risk?"			to address issues related to terrorism, as well as the strain of increased capacity demands on our aging water infrastructure.	• Real-time monitoring • Redundancy • Back-up systems and spares • SCADA improvements • Security technologies Long Term: • Alternative solutions • Reducing consequences • Advanced treatment technologies • Distributed treatment • New drinking water safety and security standards • Critical assets • Education
Energy	*A Method for The Study of Cascading Effects within Lifeline Networks	09/01	Vismor	Describes an innovative approach to study the interactions between the critical infrastructure networks in order to establish risk assessment and management methods, and to understand their cascading effects. Includes a case study of a hydroelectric power generation network and an electrical power transportation network.	Outlines a methodology to define, characterize, and assess the transfer of vulnerability between lifeline networks. This methodology is based on three specific steps: 1. Assessment of the initial vulnerability and characterize its potential consequences 2. Transfer these potential consequences to the other networks through cascading effects 3. The transferred consequences are identified as vulnerabilities This methodology is carried out on consequence studies, rather than the usual scenario approached, in order to evaluate all situations.

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
Energy	*Outage Management Systems: Surviving the Implementation	09/01	Hurt	• Electric utilities are actively installing or are considering installing an Outage Management System (OMS) for their electric distribution operations. This presentation (through a case study – PSE&G in New Jersey) identifies some of the key issues that are critical to ensure successful implementation of the new system. • Other than articulating the value of OMS systems… this case study has little value for our working group.	• The benefits PSE&G plans to gain from the new system are improved operations and dispatching less paperwork, better information back to customers, more detail on each outage event, improved storm management, and graphical data display of real time outage status and restoration. • This system will provide the capability to provide customers with real time status of an outage affecting their service and/or provide a call back to them when service is fully restored. • A number of recommendations were offered for any distribution utility planning to or presently implementing an outage management system including: o Plan more time o Allocate sufficient resources o Get the "connected model" right o Plan transition period o Define expectations to executives o Communicate often o Provide intensive training Don't underestimate stakeholder management.
Energy Telecom	*Critical Infrastructures Will remain Vulnerable: Neighborhoods must Fend for Themselves	09/01	Hurt	• Paper looks at the relationship between power, telecom and information systems, that it contends comprise the most critical parts of infrastructure (Willis Ware 1998), and	• Proposes a policy of diversification and decentralization of power, telecom, and information systems to provide a systematic rather than ad hoc investment in backup power and redundant access to telecommunications and information systems by dividing regions into neighborhoods that are made self-sufficient.

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				speculates on how to make the infrastructure more robust and dependable. • Focus is on tolerating outages of relatively short duration, approximately 48 hours; limits scope of a failure to be regional in its effects.	• Contends that self-sufficient neighborhoods, based on local power generation and redundant networks and services, could be achieved with technology changes that are on the horizon. • Besides basic questions of technical feasibility and affordability, the paper raises significant policy questions, including: o Who defines a neighborhood and how is it defined? o What changes in regulatory models are required to implement a self-sufficient neighborhood? o What incentives could lead to self-sustaining implementations of neighborhoods?
Energy Transportation Water	*Analysis of National Infrastructure Networks for Seismic Impacts	09/01	Vismor	Under support from FEMA, analyses were performed to understand the impact of disruption to critical infrastructure from earthquakes, and to assist in the identification and prioritization of mitigation measures and policies.	As a part of this study, an inventory of critical infrastructures was compiled for the conterminous United States. This included highways, railroads, airports, ports, transmission stations, sub-stations, gas pipelines, hospitals, and aquaducts. Scenario earthquakes of various sizes and locations were considered. Technical and detailed analysis and methodology.
Energy	Critical Infrastructures Assurance: Guidelines for Municipal Governments Planning for	12/02	Ellis	This document presents guidelines on actions that can be taken by municipal governments to protect public health and safety before, during and after a disruption to the natural gas	This 162 page document is a comprehensive study completed by the gas companies serving the Chicago Metropolitan area. It reviews the current natural gas systems, and all the necessary steps from pre-planning for a disruption, to restoration and long term preparedness. This would provide an excellent

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
	Natural Gas Disruptions			service.	guide for another region planning a similar exercise.
Energy Telecom	*Documenting Damage, Disruption, Interdependencies, and Emergency Response of Power and Communication Systems after Earthquakes		Condello	Paper outlines the value, objectives, approaches and types of information to be collected in a post-earthquake investigation, identifies impediments to such investigations and identifies potential physical, regulatory and cross-sector issues which may lead to increased vulnerabilities to earthquake events	As a single event, earthquakes have the greatest, and most routine, opportunity to impact numerous lifeline systems (power, communications, water, gas, bridges, emergency service response). As these systems become more inter-related, the need for post-incident documentation of failures becomes more important in order to understand the cascading effects of individual component or system failures and to build the necessary standards or earthquake codes to mitigate these extenuating effects. Paper outlines at high level what is incorporated in a post-incident investigation, the nature of the information to be gathered, the issues associated with gaining that information and the need to broaden the nature of the investigation to ensure that the interdependencies are catalogued for analysis. The author outlines the need to look beyond the power systems (their primary focus) to the impact of earthquakes on other systems (transportation, communications) and recommend broader application of what is currently investigated to these other Sectors. They further recommend that access to, and dissemination of this post-incident information should be improved to develop improved mitigation strategies.
Energy	*Communication	09/01	Vismor	This paper describes different	Power system can become vulnerable in the

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
Telecom	Infrastructure Design for Strategic Power Infrastructure Defense (SPID) System			information technology applications in power system information transmission system design, IT technologies will have significant positive effects on the power system information exchange and lead to enhanced data cataloging and archiving. Reliable and secure access to wide area system data is a key to the implementation of many newer protection and control strategies being developed at this time.	face of possible power system abnormalities. To maintain system reliability becomes a serious concern for the future. This project was launched by EPRI/DoD to understand the origin and nature of catastrophic failures and to develop defense strategies and technologies that will significantly reduce the vulnerability of the power system infrastructure. The approach is characterized by the extensive use of network and real time information from diverse sources, coupled with the development of an evolving dynamic decision event tree. This paper examines the communication issues for the SPID system including information transmission network design and data exchange architecture design. A communication infrastructure design for the SPID system is also proposed. Rather than specifying the detailed network design, the paper provides an overview of the architecture issues.
Energy	*Assessment of the Influence of Regulatory Constraints upon Utility Performance	09/01	Vismor	Paper discusses some key issues concerning the influence of regulatory constraints upon the structural reliability of the power delivery system.	Outlines a framework for performance assessment of the electric utility system and its interactions with other critical lifelines such as water supply and sewage. Results focus on the Pacific Northwest, but method could be adapted to other parts of the U.S.
Energy	Electricity Technical Discussion	05/03	Garcia	Provides an accessible technical overview of how electricity is generated and distributed, and how key interdependencies are involved in electric industry	• The U.S. national grid consists of more than 3,000 power plants, which are fueled by coal, oil, gas, nuclear, hydro and wind. • Hundreds of thousands of computers and software programs, as well as embedded microchips that make up SCADA systems,

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				operations.	automatically operate and monitor key components in the power generation process. • The transmission and distribution system is not heavily dependent on computers. • The highest priority interdependency of the electric industry is voice and data communications. • Although the electric industry owns and operates a majority of its communications equipment, a substantial portion is dependent on local telephone carriers, long distance carriers, satellites, cellular systems, paging systems, networking service providers, Internet service providers, and others. • Data communications provide real-time updates of electric system status to SCADA systems in distribution and bulk electric control centers. Data communications are also used for remote control of devices in the field, such as, circuit breakers, switches, transformer taps, and capacitors. • Large-scale loss of data communications would not likely have an instantaneous impact on electric power production and delivery, because most devices and systems would remain in the last known position. However, after 15-20 minutes, operations could begin to become impaired, as operators would have an incomplete picture

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					of system conditions. Electric system operations could become further impaired within an hour if load conditions are changing rapidly or within a few hours if demand is more stable. The critical path data to be addressed will normally be power flows on key transmission lines, voltages, and Interconnection (grid) frequency. • Thus, voice communications are indispensable for electric system operation. Although loss of externally provided voice systems such as telephones, cellular telephones, and pagers is considered a very unlikely event, electric systems must provide sufficient redundancy to assure continuous voice communications over a geographic area that addresses its critical facilities and interfaces to neighboring systems and regional centers. • The principal mitigation strategy is the use of microwave, long and short wave radios, satellite voice systems, privately owned phone networks, and other systems that provide independent and redundant backups. • Electric systems also have dependencies with fuel supplies, although these dependencies do not appear as critical as those related to telecommunications.
Energy	An Agent Based Micro-simulation of Critical	04/00	Garcia	This document written by Sandia scientists is academic, technical, and theoretical in	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
	Infrastructure Systems			its construct, and to me has questionable practical application to what I believe we're trying to do (it's also three years old). It assumes the reader is fluent in the authors' lexicon and has some grounding in the research methodology underlying the discussion.	
Energy	An Agent Based Tool for Infrastructure Interdependency Policy Analysis	09/00	Vismor	Powerpoint presentation from Argonne Labs which explains the use of an agent based software tool to model the interdependencies between the electric power and natural gas sectors.	Electric generators that use natural gas as a fuel source are rapidly gaining market share over coal and nuclear sources. This is creating a new dependency on gas by the electric sector. The modeling tool enables different market and economic assumptions to be factored into the analysis.
Energy	An Approach to the Understanding of Interdependencies	09/02	Vismor	Focuses on the interdependency of the power and communication infrastructures and their dependence on systems (and the internet). In 1997, NSTAC provided a report titled "Electric Power Risk Assessment" and stated that the security of electric power control networks represents a significant emerging risk to the electric power grid. Provides some suggested ways to deal with and model	Critical data is exchanged among power systems that make use of open systems such as the internet. The protection of internal networks and systems is not sufficient. This must be expanded to open systems such as the internet. The paper suggests the following approach: 1. Apply the proposed categories of link types and interaction layers, and identify the different interdependency channels that could be activated. 2. Use the existing dependability assessments of the singular systems and of the system of systems for determining the failure modes that

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				"systems of systems" as opposed to single systems.	could violate the dependability requirements provoking SOS level malfunctions. 3. Interrelate the information of interdependency channels and top events, and determine reasonable interrelationships. 4. Evaluate each of these conceivable associations. Investigate the feasibility of complementary reliability and security measures.
Energy	Aspen-EE: An Agent Based Model of Infrastructure Interdependency	12/00	Vismor		Reviews a model developed by Sandia Labs using a micro-simulation model, which is an agent based model.
Energy	Critical Infrastructures: Interdisciplinary Research and Education Challenges	12/01	Hurt	Presentation explores the importance of investment in both research & development and education programs in Electric Power industry. The challenges of investment both are also highlighted.	• Measuring the cascading, Dependencies, Interactions of large scale networks: o Too complex for single central entity to evaluate, monitor, and manage in real time. o Too complex for conventional mathematical methodologies. o Multi-layered, multi-resolutional intertwined networks. • Trends- o Information technology allows us to create systems with bewildering complexity. o The need for a new science for interdependent networks remains. • Electricity infrastructure underlies every

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					aspect of our economy society. Possibly the largest machine in the world. • Demand is out pacing investment in R & D and infrastructure. • Deregulation is putting pressure on inter-regional infrastructures. • Power interruptions & inadequate quality cause economic losses to the nation conservatively estimated to be over $100 Billion/year. • EPRI/DoD Complex Interactive Networks Initiative – Goal to develop tools that enable secure, robust and reliable operation of interdependent critical infrastructures with distributed intelligence and self-healing abilities. • The size and complexity of our infrastructures make understanding them a cooperative effort among disciplines. • Need to establish education centers that cut across department boundaries and create bridges between departments and disciplines – new courses, seminars etc. • R & D challenges – o Need to develop a theoretical framework, modeling and simulation tools for interdependencies and their fundamental characteristics. Need for integrated assessment, monitoring, and early warning

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
Energy Telecom	Distribution System Disruption and Recovery for Natural Hazards	09/02	Condello	Document outlines methodologies to represent the disruption and recovery of an urban distribution system under earthquake and winter storm conditions. Intent is to ultimately build a methodology that can represent various outage scenarios so that analyses on which types of structural components in distribution or transmission systems perform poorly during various events and why.	Authors found that traditional analysis methods (restoration rate) do not adequately represent both earthquake and winter storm scenarios. Rather, utilizing an "outage duration" method of analysis based on empirical data might prove to be a better method for characterizing recovery efforts. Predictive models based upon these methods are currently underway and further measurements and analysis of additional empirical data across more locales should provide a more accurate characterization of damage, recovery and restoration to utility lifelines under a variety of hazardous conditions.
Energy Telecom	Managing Disruptions to Critical interdependent Infrastructures in the Context of the 2001 World Trade Center Attack	11/02	Vismor		This research is intended to improve understanding of and support for the management of critical infrastructure interdependencies following large-scale, disruptive disasters. The particular focus of this work is on developing techniques that can be used to mitigate against or respond to events that have the capability of impacting interdependent infrastructure systems.
Energy	Natural Gas Security Issues Related to Electric Power Systems	11/01	Vismor	Presented by Argonne National Labs; illustrates the interdependencies between the electric and natural gas sectors.	Key Recommendations: Companies should not only conduct vulnerability assessments of their own systems and operations, but also of their partners. Industry and government should advocate the development, adoption, and implementation of global IT processes to reduce vulnerabilities of cyber and other electronic systems.

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
					Industries should enhance their response and recovery plans, including participation in regional response and recovery planning to deal with disruptions to physical and cyber infrastructures.
Energy	Simulating Energy Markets and Infrastructure Interdependencies with Agent Based Models	N/A	Leffler	In this very interesting paper the authors present the concept of Agent-Based Simulation (ABS) as applied to not only one enormously complex physical infrastructure (Electricity), but two such systems (the other: Natural Gas) including the interdependencies between them. There are two distinct and related analyses. One involves the physics of the infrastructures; the other relates to the human decision-making that impacts the physics. Speaking for the electricity system, the capability to model and simulate the state physics of the system is well-known and applied, in real-time on individual system and regional bases. The capability	The following recommendations are offered for consideration: 1. The concepts presented in the paper are very interesting and certainly deserve our discussion. This must be with industry and modeling experts. 2. If we move forward with this additional interdependency metric (human actors), we must understand it well. 3. To commence the interdependency modeling of the systems, we must find the experts in the industries with in-depth experience in the industry and modeling knowledge. These persons must be dedicated to the task; this is not the work of a committee.

[10] "Agent Based Simulation in Integrated Assessment Resources Management", Claudia Pahl-Wostl.

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				to model on an interconnection basis exists and has been applied to the Texas Interconnection. The Eastern and Western Interconnections can be modeled in their entirety using the recently developed common information modeling standard of the International Electrotechnical Commission (IEC). A next step in real-time physics modeling of the electricity system is stability and voltage dynamics. This is done now, in a pseudo real-time manner. For example, the electric systems now study in real-time the impact of a variety of transmission and generation "outages" on the loading of the system with respect to its limits. The dynamic analysis is generally done off-line with steady state limits utilized as proxy for dynamic effects. A next step is further application of the on-line dynamic analysis tools.	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				This abstract of the paper does not address the current state of physics modeling of the natural gas system. We can envision interaction analyses between the physics of the two systems. For example, consider the immediate and total outage of all natural gas high pressure pipelines supplying a major multi-unit electric generation station. The station might likely shutdown within seconds due to lack of on-site natural gas storage and the time required to switch to alternate fuels. The total loss of generation may result in a dynamic stability condition resulting in partial electric grid separation. The grid may supply electric energy to a natural gas compressor at some other pipeline station. Recognition to electric supply restoration time, availability of backup power at the compressor station, natural gas line pack and timing for	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				its decay would be included in the interdependency analysis, just considering the physics. Agent based modeling provides "autonomous software systems that are intended to describe the behavior of observed social entities (e.g. individuals, organizations, governmental agencies). An enormous advantage of agent based modeling is the ability to assess the plausibility of the behavior of agents, the ways in which the agents interact and the consequences of that behavior and interaction."[10] The proposed agent-based analysis is of human decision-making processes as a part of the overall operation of the infrastructures. In other words, first, how human decision-making would impact either the electric or natural gas systems' operation given a variety of economic and other stimuli. Then, how	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				would these human decisions interact between the two systems. Then, carry this to the next step to analyze the human decision-making and system physics interacting. For one example of the human impact, analyzing just the electric system, decisions are made in various timeframes regarding electric capacity reserves (as the paper describes). To simplify this example, consider that existing NERC policy regarding reserves for a variety of conditions is fully met. Now, a major generator is lost due to mechanical failure. The policy calls for restitution of reserve capacity to meet the next possible loss of generation, within a prescribed time period. Variabilities include electrical demand in the short timeframe, supply availability to fulfill the reserve requirement (to meet the probabilities associated with demand variability and	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				generation outages), costs of supply, means to recover these costs, obligation to supply demand. The ABS accounts for the human decision-making that will impact the actual reserve posture. In today's electricity structure there are many independent organizations involved in the overall decision-making. The agents would provide probabilistic modeling of these behaviors. This then would feed back to the physics model to provide an overall reliability assessment. Other matters to consider in the agent models include: 1. Accuracy of data (real-time and projected) used in decision-making (e.g. transmission loading impacts on electric transaction arrangements). 2. Errors and mistakes in human decision-making (e.g. contract to electronic tag	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				transcription error). 3. Time to effectively respond to the system physics (e.g. planning tomorrow's reserves vs responding to an instant emergency). 4. Communications among decision-makers (e.g. consider loss of communications and the further interdependencies of both electricity and natural gas on telecommunications). 5. Agent unpredictability (e.g. humans not following predicted or probabilistic patterns due to a variety of outside stimuli). One matter of issue is the graph in Fig-7 regarding unserved energy (presumably electric) and natural gas as a percent of fuel used in electric generation. Either the graph is insufficiently described, in error, or I don't understand the	

Sector	Report Title	Date	Reviewer	Abstract	Key Points/ Recommendations
				representation.	
Energy	Energy Security	04/03	Vismor	This research was funded by DOE.	Report concentrates on the vulnerabilities of the electric system, natural gas, and petroleum, and their dependencies on other critical infrastructures in a post 9/11 era.

* The discussions were presented in Alexandria, Virginia during a Workshop on "Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures" on September 10-11, 2001. http://www.ari.vt.edu/workshop/papers.htm

RANKING OF INTERDEPENDENCIES BY CRITICAL INFRASTRUCTURE SECTOR REPRESENTATIVES

The WorkingGroup participants were asked to rank the sectors upon which they are most dependent – and the sectors they felt were most dependent upon the critical infrastructure they represent.

Sector	Respondent	First	Second	Third	Most Dependent on this sector:
Agriculture					
Food					
Water	Diane VanDe Hei (amwa)	Electricity	Surface Transportation	Chemical	Emergency Response Public Health; Electric
Public Health					
Government					
Defense Industrial Base					
Information & Telecommunications					
Telecom	David Kanupke (usta)	Electricity	Transportation	IT	All
Telecom	Kathryn Condello (ctia)	Telecom (Intra-sector)	Electricity	Transportation (Roads)	Public Safety/Continuity of Government; Financial Services
IT	Ken Watson (Cisco)	Telecom	Electric	Transportation	Telecom; All
Energy	Lou Leffler (nerc)	Gas	Telecom	Water	Water; Gas; All
Oil and Natural Gas	Bobby Gilham (Conocophillips)	IT and Telecommunications	Electricity	Transportation	
Transportation	Rich Holmes (Union Pacific)	Electricity	Telecom	Diesel/Oil and Gas	Electricity (transportation of coal); Water (Chlorine), Military Shipments
Banking and Finance	Vismor (Mellon)/Callahan BoA	Electricity	Telecom	Transportation	Food; All
Banking and Finance	Meckler (Wells Fargo)	Telecom	Transportation	Banking and Finance	Banking and Finance; All
Chemical Industry & Hazardous Materials					
Postal & Shipping					
National Monuments & Icons					
Education					
Results		Electricity = 4	Electricity= 3	Transportation = 4	
		Telecom = 3	Telecom = 3	Water = 1	
		Gas = 1	Transportation = 2	Chemical = 1	
				IT = 1	
				Diesel = 1	
				Banking and Finance = 1	