

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

SECTOR PARTNERSHIP MODEL IMPLEMENTATION

**FINAL REPORT AND
RECOMMENDATIONS
BY THE COUNCIL**

October 11, 2005

**MARTIN G. MCGUINN
WORKING GROUP CO-CHAIR
CHAIRMAN, PRESIDENT & CEO
MELLON FINANCIAL CORPORATION**

**MARILYN WARE
WORKING GROUP CO-CHAIR
CHAIRMAN EMERITA
AMERICAN WATER**

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	3
-------------------------------	---

EXECUTIVE SUMMARY

• INTRODUCTION	5
• APPROACH AND METHODOLOGY	7
• CONCLUSIONS AND RECOMMENDATIONS	8
• CONCLUSION	18

APPENDICES

1. PROPOSED SECTOR PARTNERSHIP MODEL.....	19
2. GOVERNANCE AND REPRESENTATION	20
3. RECOMMENDED SECTOR PARTNERSHIP MODEL	25
4. SAMPLE GCC CHARTER	26
5. SAMPLE SCC CHARTER	31
6. SCC PURPOSE AND FUNCTIONS.....	38
7. DEFINITIONS	41
8. FACA FACT SHEET	44
9. PCIS LETTER, 6/23/05	46

Acknowledgements

Mr. McGuinn and Ms. Ware wish to acknowledge the efforts of the entire Working Group and the study groups (listed below) and extend their deepest appreciation to all who have offered their time and advice to support this effort.

Working Group Members

Alfred R. Berkeley III, Chairman and CEO, Pipeline Trading Systems, LLC
 John T. Chambers, President and CEO, Cisco Systems, Inc.
 Richard K. Davidson, Chairman, President and CEO, Union Pacific Corporation
 Chief Rebecca F. Denlinger, Cobb County Georgia Fire and Emergency Services
 Thomas E. Noonan, Chairman, President, and CEO, Internet Security Systems
 Erle A. Nye, Chairman Emeritus, TXU Corporation
 John W. Thompson, Chairman and CEO, Symantec Corporation

Integrated Study Group Members

Representatives for NIAC Members

Susan Vismor, Mellon Financial Corporation
 Bruce Larson, American Water
 Pete Allor, Internet Security Systems
 Rob Clyde, Symantec
 Rick Holmes, Union Pacific Corporation
 Bill Muston, TXU Corporation
 Stu Shannonhouse, Cobb County
 Ken Watson, Cisco Systems Inc.

Representatives from Sector Coordinating Councils

Dan Bart, Communications Lead, Telecommunications Industry Association
 Stuart Brindley, Electric SCC Chair, Independent Electricity System Operator
 Guy Copeland, Information Technology Lead, Computer Sciences Corporation
 Clay Detlefsen, Food and Agriculture SCC Co-Chair, International Dairy Foods Association
 Don Donahue, Financial Services SCC Chair, Depository Trust and Clearing Corporation
 Gary Forman, Oil and Natural Gas SCC Vice Chair, Columbia Gas
 Al Hancock, Dams SCC Vice-Chair, Xcel Energy Corporation
 Zane Hill, Postal and Shipping SCC Chair, US Postal Inspection Service
 Andrew Howell, Transportation Lead, U.S. Chamber of Commerce
 Patrick Laird, Electric SCC Vice Chair, Exelon Corporation
 Lyman Shaffer, Dams SCC Chair, Pacific Gas and Electric Company
 Lynn Stovall, Water SCC Chair, Greenville, SC Municipal District
 Beth Turner, Chemical SCC Chair, DuPont
 Mike Wallace, Nuclear SCC Chair, Constellation Energy
 Gary Weber, Food and Agriculture SCC Co-Chair, National Cattlemen's Beef Association
 Rick Williams, Oil and Natural Gas SCC Chair, Exxon Mobil

Sector Specific Study Groups

Food and Agriculture

Electric

Oil and Natural Gas

Chemical

Nuclear

Postal and Shipping

Financial Services

Emergency Services

Dams

Information Technology

Communications

Water

Transportation

Executive Summary

Introduction:

Integrated partnerships between Federal, State, and local governments and the private sector must be established in order to accomplish effective planning and preparedness as well as timely response and recovery to terrorist attacks and natural disasters. Any attack or major natural disaster affecting the 17 critical infrastructures and key resources (CI/KR) would greatly disrupt our nation's way of life and have a rippling effect throughout the country. The homeland security goals to avoid and respond to such events are set forth in Homeland Security Presidential Directives 5, 7, 8 and 9 and, if they are to be achievable, require an inclusive partnership framework.

The Sector Partnership Model intends to establish the framework for an unprecedented level of public-private cooperation necessary to secure these assets. The model has its foundation in previous National Infrastructure Advisory Council (NIAC) recommendations. In April 2003, the NIAC examined the topic of how to coordinate crisis event management among the critical infrastructures. The NIAC concluded that cross-sector protection, response and crisis planning and management coordination is fundamental to the rapid restoration of critical infrastructures. These findings and recommendations were a foundation for the Sector Partnership Model.

The NIAC was asked by Department of Homeland Security (DHS) to assess the validity of the partnership model for Critical Infrastructure Protection (CIP) proposed in the Interim National Infrastructure Protection Plan (I-NIPP), which was released in February 2005. This plan outlined how DHS in cooperation with State and local governments and the private sector would develop and implement the national effort to protect infrastructures across all sectors. As stated in the I-NIPP, "protecting our Nation's critical infrastructure and key resources is vital to our national security, economic vitality and way of life." Ultimately, DHS is responsible for the success of the CIP program. However, implementation requires an integrated process among all key stakeholders, including Federal, State, and local governments, as well as the private sector, if the United States is to meet strategic, operational and implementation goals.

The conceptual framework of the Sector Partnership Model as presented in the I-NIPP encourages the identification of Sector Coordinating Councils (SCCs) and formation of Government Coordinating Councils (GCCs). Moreover, the model envisions these councils as the mechanisms for coordination and information exchange in matters relating to critical infrastructure protection across the 17 critical sectors and key resources.

- SCCs serve as the government's principal point of entry into each sector for developing the entire range of infrastructure protection activities and issues. Each SCC is self-organized, self-run, self-governed, and responsible for generating participation of the owners and operators within a sector.

- GCCs are the complementary government counterpart for each sector, formed to achieve inter-agency coordination. The GCC coordinates governmental roles with respect to critical infrastructure strategies, policy, programs, and communications across government organizations.

The model also consists of cross-sector councils for both the private sector and the government.

For implementation of the model to be effective, public and private sector stakeholders must have adequate and legitimate opportunities for meaningful participation. The coordinating councils will serve as resources to provide advice, information, and recommendations on issues associated with CIP, including the NIPP, Sector Specific Plans (SSPs), and the National Response Plan (NRP). Preparedness and response requires continuous and open dialogue among the public and private partners in this framework.

For the Sector Partnership Model to succeed there needs to be a clear definition of roles and responsibilities. Each partner, as an independent organizational entity, has sovereignty of its own and brings unique capabilities to the table. The model generates true value when all partners work together effectively and efficiently. The partnership needs to be rooted in robust collaboration between government and the sectors as well as between the sectors. Given that the private sector owns 85 percent of the critical infrastructure, DHS and other Sector Specific Agencies must embrace the integral role of the owners and operators in this critical endeavor to protect our nation's critical infrastructure and meet the challenges of large-scale disaster preparation, response and recovery. The significant emergency response challenges spawned by the recent Gulf Coast disasters provide exceptional clarity to the urgent need for effective coordination and collaboration among all partners in this framework. The sobering scope and widespread impact of Hurricanes Katrina and Rita among multiple sectors demonstrate the need for joint action and fully integrated partnerships. The government and the private sector must attend to unfinished business, complete the important tasks already undertaken, strengthen what works, and take bold action. Together, with renewed emphasis and increased urgency, a more capable national protection and preparedness enterprise can be firmly established through the Sector Partnership Model.

Approach and Methodology:

DHS requested that the NIAC develop advice and recommendations for the structure, function, and implementation of the model as proposed in the I-NIPP. (*See Appendix 1 Proposed Sector Partnership Model*)

Specifically, DHS asked the NIAC to focus on providing four core deliverables:

1. Sector Partnership Model Structure

- Review conceptual structure
- Identify and validate composition and representation

2. Roles and Responsibilities within the Model

- Review elements of a “charter” (for overall structure and sub-elements)
- Define purpose and rules of engagement

3. Potential Operational Frameworks for the Model

- Assess legal components of possible operational frameworks
- Identify and review options: Federal Advisory Committee Act (FACA)/non-FACA
- Review authorities and core requirements to implement

4. Processes to Support the Model

- Highlight key processes to support true “partnership”
- Define principles of operations

The NIAC invited all existing SCCs or their equivalents to participate in this study, including the Sector Chairs and the members. Each of the 17 CI/KR sectors has a unique set of challenges and requirements, making it imperative for the Sector Partnership Model to be flexible enough to meet these diverse needs. The NIAC wished to incorporate these distinct perspectives as much as possible. In the end, 12 different sectors gave input to this report. The NIAC is very grateful for the level of effort participants invested in the process. This broad private sector involvement ensures that the perspectives, experiences, and lessons learned across the sector spectrum have had a chance to influence the implementation of the model.

Conclusions and Recommendations:

Deliverable #1— Validate Conceptual Structure

Conclusions: The conceptual structure of the Sector Partnership Model was found acceptable with the following considerations and recommendations:

Recommendation: Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) should comprise the base level of the model.

- The Council believes the formation of 17 individual SCCs and GCCs for each of the Critical Infrastructure/Key Resources is a logical approach to coordinate across the sectors and between government and industry. The SCC Chairs have reported that this structure is already in place for many sectors and is currently working.

Recommendation: There was consensus regarding the second level of the model—the Private Sector and Government Cross-Sector Councils. The Partnership for Critical Infrastructure Protection (PCIS) should assume the role of the Private Cross-Sector Council.

- The I-NIPP states that the leadership of the SCCs may voluntarily form a high-level Private Sector Cross-Sector Council to address common and cross-sector interdependency issues. The Council identified the Partnership for Critical Infrastructure Security, Inc. (PCIS) as an ideal candidate to function as the Private Sector Cross-Sector Council. The mission of PCIS is to coordinate cross-sector initiatives in support of public and private efforts to promote the assured and reliable provision of critical infrastructure services in the face of emerging risks to economic and national security. Formed in 1999, the PCIS is currently functioning in a similar role to the one envisioned in the I-NIPP for the Private Sector Cross-Sector Council.

PCIS intends to have the SCCs as members, with each SCC represented by its chair, co-chair, or other appointed individuals from the sector. The PCIS also has a three-member executive board. Elected annually, the board mostly functions for administrative purposes. While its board can speak on behalf of its members, the whole group takes formal action on all substantive issues and tasks. Currently, 14 of the 17 CI/KR identified by HSPD-7 are represented on PCIS.

The NIAC recommends that DHS recognize PCIS as the Private Sector Cross-Sector Council. Once recognized, PCIS would become the body where the Secretary of Homeland Security could address all sectors at once. PCIS should continue to strive for full representation of all CI/KR (excluding National Monuments and Icons and Government Facilities, which will not have a SCC).

Recommendation: PCIS must have a government counterpart, the Government Cross-Sector Council, consisting of the GCC Chairs.

- As a counterpart to the SCCs, the GCCs will form a Government Cross-Sector Council comprised of leaders from each Sector Specific Agency, presumably the chairs of each GCC. This high-level Government Cross-Sector Council will address interdependency and policy issues. The Council believes this level of the partnership model is extremely important for cross-sector coordination.

Recommendation: The Government Cross-Sector Council must engage state Homeland Security Advisors (HSAs) in the model.

- The linkage from National Level Preparedness to State and Local Preparedness will be through the engagement of the State Homeland Security Advisors.

Recommendation: The office of the Under Secretary of Preparedness should be included to show information flow between that office and both cross-sector councils with no connotation of subordination; any directional arrows must be removed, since they imply subordination.

Recommendation: DHS should eliminate the top level of the organization (the NIPP Leadership Council), given that its work is redundant.

- The NIAC recognizes the continuing ambiguity surrounding the top level of the model, the NIPP Leadership Council. To date, DHS has never clearly articulated the membership and functions of the proposed Leadership Council. Moreover, the Council believes all necessary cross-sector coordination can occur both efficiently and effectively through bilateral interactions between the Private Sector Cross-Sector Council and the Government Cross-Sector Council. The Council did not find any practical reason to add another layer to the partnership model. Therefore, the NIAC recommends eliminating the Leadership Council as the top tier of the Sector Partnership Model.

Deliverable #1 – Validate Model Composition and Representation

Recommendation: DHS should recognize all SCCs equally and should recognize them in the manner in which they have chosen to organize themselves. SCCs should constitute themselves in a way that provides for appropriate governance and representation of the whole sector.

- To date, SCCs have organized themselves in different ways, with varying composition:
 - Only owners/operators
 - All trade associations

- Blend of owners/operators and trade associations—sometimes with trade associations as members and an owner/operator as the chair

Questions related to the role of sector trade associations and their participation in the leadership of the SCCs were a source of disagreement. Eventually, discussion of this issue led to consensus that:

- Owners and operators from the sector must be integral in the formation of each sector's SCC and in the SCC itself;
- The SCCs must be autonomous and should develop governance processes and roles appropriate to the sector; and
- Involvement of sector trade associations in the SCCs may be very valuable in achieving effective outreach and gaining buy-in from the sector.

(See Appendix 2 Governance and Representation)

Recommendation: If DHS or another government agency has a request of an SCC, that agency should coordinate with the Sector Specific Agency, as it is the principal focal point for coordination with that SCC and sector.

- The group also discussed the role of the Sector-Specific Agencies (SSAs) in interacting with their designated SCCs. Inefficiencies occur when different government authorities make duplicative requests of sectors without the participation of the SSAs. The Council agreed that, for those sectors with designated SSAs, the lead agency should be the principal point of contact between the SCC and the government on Homeland Security-related issues. For those sectors where a particular DHS division or office serves as the “sector-specific point of contact,” that division or office should fulfill a similar role. The Council believes this will ensure that interactions between SCCs and government will maintain complete alignment toward common goals.

(See Appendix 3 Recommended Partnership Model)

Deliverable #2 – Roles and Responsibilities

The NIAC defined, reviewed and generally accepted the roles and responsibilities of GCCs and SCCs. The list, though, is by no means definitive. As critical infrastructure protection evolves, the functions of the coordinating councils will mature along with it. Moreover, the Council understands that sectors are not identical and agrees that not all functions may be applicable to all sectors.

According to the NIAC's findings, there are several key characteristics of GCCs, including:

- serving as a counterpart to SCCs by providing interagency coordination among all Federal, State, local and tribal entities tasked with homeland security roles for the sector;
- providing coordinated communication, issues development and implementation among government entities;
- coordinating and supporting the efforts of SCCs to plan, implement, and execute sector-wide security; and
- leveraging complementary resources within government and between government and industry

When a GCC is established, the members develop a charter or other governance document that serves as a set of informal rules of engagement for the council by delineating its individual objective, scope of activity, membership, roles and responsibilities, and standard operating procedures. Varying slightly depending on the particular characteristics of the sector, each charter clearly states that the council cannot supersede any responsibility a member may have by law or executive order. GCC membership consists of key representatives from Federal, State, local, and tribal governments with direct control of sector security. The GCC charters also indicate that members should be director-level, or should have equivalent decision-making ability. *Ad hoc* or *ex officio* members are often invited to meet expertise requirements. (See Appendix 4 Sample GCC Charter)

As part of its review process, the NIAC requested that the SCCs share their charters with the NIAC Working Group. (See Appendix 5 Sample SCC Charter). The Council also asked that DHS specifically define the roles and responsibilities the government would like SCCs to support regarding CIP and response. In reply, DHS provided definitions and examples of each function's responsibilities, including:

- representing a primary point of entry for government into the sector to address the entire range of infrastructure protection activities and issues;
- serving as a focal point for communication and coordination between owners, operators, and the government during response and recovery;
- identifying, implementing, and supporting the information-sharing capabilities and mechanisms most appropriate for the sector;
- facilitating inclusive organization and coordination of the sector's policy development, infrastructure protection planning, and implementation activities;
- advising on the integration of state, local, and regional planning initiatives with Federal initiatives, such as the state and local role in SSPs, the NIPP, and the NRP; and
- providing input to the Federal government on research and development efforts.

(For a complete list of functions and analyses, see Appendices 6 & 7 SCC Purpose and Functions and Definitions)

The NIAC determined that the intended functions of the SCCs and the PCIS could constitute giving advice to the government, which was a deciding factor in determining a recommended operational framework.

Deliverable #3 – Assess Operational Framework Options

Recommendation: The NIAC recommends that the operational framework for the Sector Partnership Model be based on an unconditional exemption pursuant to Section 871 of the Homeland Security Act of 2002. The exemption authorizes the establishment of advisory committees as the Secretary may deem necessary and provides that an advisory committee established under this section can be exempt from FACA.

All SCCs and the PCIS should be self-organized, recognized as advisory committees on critical infrastructure protection and response/recovery matters and be exempt from all requirements of FACA:

- **The necessary information sharing and advice from the sectors would otherwise be hampered by legal uncertainty.**
- **Protection is needed against the risk of disclosure of critical vulnerabilities**
- **Communication between GCCs and SCCs will need to occur on an ad hoc basis, often at a moment's notice or in response to an emergency.**

The study group spent a considerable amount of time analyzing deliverable 3. The potential legal implications of various organizational structures within the model were extensively explored and debated. Effective critical infrastructure protection requires the ability to have real time, continuous communications and open dialogue among the public and private partners in the model. The granting of the 871 exemption will establish a known and understood framework that facilitates the flow of advice and information concerning critical infrastructure protection. Not doing so would inhibit information sharing, risk publicly disclosing vulnerabilities, and suppress ad hoc communication during emergencies.

Whenever government and the private sector interact, stakeholders must consider the legal and regulatory issues inevitably involved. Even though SCCs are independent of government and not subject to government regulation, laws do apply to their interaction with government, as in the activities of the Sector Partnership Model. The NIAC recommends a framework that mitigates any legislative or regulatory concerns and impediments. It is imperative for the government and private sector to work together effectively to provide for the protection of critical infrastructures, and protect the information shared between the government and the private sector during these efforts.

To reach these recommendations, the NIAC first identified and analyzed four possible options, referred to as “scenarios,” for an operational framework to implement the Sector Partnership Model. The scenarios are each described below.

Scenario 1 – FACA Structure

While not explicit in the I-NIPP, the structure appears to contemplate that SCCs and the Private Cross-Sector Council would be subcommittees of a parent advisory committee, the NIPP Senior Leadership Council. The subcommittees would not be subject to FACA or to General Service Administration (GSA) regulations implementing FACA provided they do not offer advice or recommendations directly to, and are not managed or controlled by, federal officials. Additionally, the parent advisory committee could not merely "rubber stamp" any recommendations and advice offered by a SCC or Private Cross-Sector Council. In such a case, the subcommittees also would not be subject to FACA's restriction on the performance of non-advisory functions. If a SCC offered advice or recommendations directly to GCCs, or if the Private Sector Cross-Sector Council provided advice or recommendations directly to the Government Cross-Sector Council, this could be subject to FACA and therefore to its various requirements such as advance notice of meetings, open meetings, and public disclosure of detailed minutes and other documents. (*See Appendix 8 FACA Fact Sheet*)

Scenario 2 – Operational Committees

GSA regulations implementing FACA distinguish between "advisory" committees and "operational" (or "non-advisory") committees. "Operational" committees, as defined by GSA, are those committees "established to perform primarily operational as opposed to advisory functions." GSA's regulations permit primarily "operational" committees to advise the government without becoming subject to FACA. It is the responsibility of the administering agency to determine whether a committee is primarily operational. However, a committee designated operational may become subject to FACA if, later, it becomes primarily advisory in nature.

Scenario 3 – Neither Established nor Utilized

The FACA regulations apply to committees established or utilized by one or more federal agencies. An entity neither "established" nor "utilized" by the government is not subject to FACA. GSA regulations state an agency may use the following factors to determine whether a group is "utilized": (a) Does the agency manage or control the group's membership or otherwise determine its composition? (b) Does the agency manage or control the group's agenda? (c) Does the agency fund the group's activities? Answering yes to any or all of these questions does not automatically mean the group is "utilized," but GSA advises that, "An agency may need to reconsider the status of a group under the Act if the relationship in question essentially is indistinguishable from an advisory committee established by the agency." (App. A to Subpart A, Item I.) However, the term "established" is not defined in FACA or GSA regulations (examples are given of when a committee is not "established").

Scenario 4 – FACA Exemption

Section 871 of the Homeland Security Act of 2002 provides that, "The Secretary may establish, appoint members of, and use the services of, advisory committees, as the Secretary may deem necessary. An advisory committee established under this section may be exempted by the Secretary from [the FACA], but the Secretary shall publish

notice in the Federal Register announcing the establishment of such a committee and identifying its purpose and membership." The exemption authority has never been exercised.

In order to reach consensus on a framework for the Sector Partnership Model, the NIAC identified the pros and cons as well as the risks associated with each scenario. An analysis of the data produced the following results:

Scenario 1 – FACA Structure

- Most owners and operators were very uncomfortable with this scenario, so much so that they predicted sector participation in the partnership would effectively end if this option were implemented.
- Many SCCs are strongly opposed to any structure allowing another body to overrule and change their recommendations. If SCCs were working groups of a FACA entity, it would be a “lose-lose” situation. If SCCs submit advice and recommendations up through the higher advisory committee to avoid FACA regulations, they risk having their recommendations changed. They also would be reporting to a higher-level entity that could include representation from their SSAs and regulators. However, if the SCCs are deemed to be entities directly subject to FACA, they would have to follow all requirements of FACA, including those pertaining to open meetings and public disclosure of minutes and other documents. In such a situation, the risk of information disclosure is so great that the owners and operators would likely not disclose vulnerabilities or engage in a candid dialogue with government. Additionally, cross-sector sharing of incidents would end while the actual exchange of information would be incredibly slowed, hindering stakeholders’ ability to react quickly.

Scenario 2 – Operational Committees

- GSA regulations concerning this scenario are ambiguous.
- There is ample ambiguity around those functions deemed operational and those deemed advisory.
- There is a very real risk that any particular SCC could be considered operational today, but advisory (and subject to FACA) tomorrow.
- A potential exists for legal challenges and extended court battles over whether SCCs are operational or advisory.
- DHS has said it would like to go to the SCCs for advice on an annual basis, particularly on obtaining input to national plans, which could be perceived as contradicting a conclusion that the SCCs are operationally focused.

Scenario 3 – Neither Established nor Utilized

- Again, this scenario poses the risk of complicated legal interpretations and protracted court battles.
- This scenario might prejudice future instances when it may be helpful or necessary for the government to provide some type of funding to the SCCs.

- An argument that the Private Sector Cross-Sector Council and the SCCs were not "established" by the government might be weakened because the government has proposed their identification in the I-NIPP (though PCIS and many of the SCCs were in existence prior to release of the I-NIPP). Moreover, a court could perceive that DHS had persuaded the private sector to create the councils in such a way to evade FACA.
- Variations in the factual circumstances of the various SCCs result in some SCCs having a stronger legal case than others under this scenario.

Scenario 4 – FACA Exemption

- Most of the participants involved in this study believe the partnership model will work most effectively under the fourth scenario, which provides the most efficient method to share information. It allows SCCs and GCCs to communicate directly with each other and provides for a protected relationship between industry and its regulating agencies when addressing CIP. Interactions between the government and private sector will increase, and the flow of information will be much more efficient.
- SCCs are more comfortable with this scenario and therefore much more likely to participate.
- There is much less legal ambiguity surrounding Section 871 than exists with other scenarios. Determining whether a council is "advisory" or "operational" or whether it is "established" or "utilized" by the government is really a case-by-case, issue-by-issue question. Moreover, such distinctions can change over time. An effective partnership will not be able to function in the face of so much ongoing risk of litigation and uncertain result. An exemption would clarify that and avoid a future change in the classification of the councils.
- Many believe this scenario promotes equity in the partnership and bolsters cooperation among all stakeholders.

After analyzing the data, the NIAC agreed to accept Scenario Four, a FACA exemption under Section 871, as the framework by which to implement the Sector Partnership Model. Based upon the amount of negative response to it, Scenario One was quickly eliminated. While favorable to some participants, Scenarios Two and Three were weighed down with litigation risks and grey areas subject to different legal interpretations. Moreover, the NIAC acknowledged it was advisable to have only one answer applicable to all sectors. Thus, the Council reached consensus that Scenario Four was the most viable option.

A FACA exemption is essential for the short- and long-term success of the Sector Partnership Model. For private sector owners and operators to participate actively in this system, they must have confidence that the proprietary, sensitive or personal information they have voluntarily shared during the course of an open and honest dialogue will not be subject to public disclosure. Most private-sector stakeholders are, by nature, risk averse in their relationships with government, so it is critical that the value received by taking part in the model outweighs the risk. Without robust and active participation from the

private sector, DHS cannot accomplish its CIP and information sharing goals, key components of infrastructure protection and homeland security.

The NIAC fully appreciates the challenges that the Secretary will face by using his authority for the Section 871 exemption. The Council recognizes there will be obstacles in spite of the clear legislation giving the Secretary this authority. It will require strong leadership and courage. The NIAC and the private-sector representatives on the Study Groups determined that there was no better solution under current law and that they would support the Secretary in this decision.

Deliverable #4 – Key Processes and Principles

Recommendation: The NIAC identified the following key processes and principles to support a true partnership:

- Stakeholders develop a true partnership based on a collaboration of equals in which all partners bring value.
- SCCs are self-formed entities. The private sector is responsible for group formation, membership, and governance.
- The SSA acts as the government lead for coordinating with the sector. All government agencies should recognize the role of the SSA, and use it as their means to interface with the SCCs. Sectors having a DHS office as their SSA will use that DHS office as their government interface.
- Government communication to the sectors should occur primarily through the established SCCs, supported as necessary by the councils' designated information sharing and analysis mechanisms. Exceptions do exist, such as when dealing with threat-based information that needs to reach the affected owners and operators as quickly as possible.
- All participants in the partnership model must fully engage in the ongoing development, implementation, and improvement of national plans, including the NIPP, SSPs, NRP and the National Incident Management System (NIMS). This encompasses:
 - Sector-wide planning
 - Development of sector best practices
 - Sector-wide dissemination of programs and plans
 - Cross-sector coordination
 - Facilitation of response and recovery
- Given that disasters happen at a regional level rather than a national level, it is important to ensure the model synchronizes activities down to the regional level.
- The Protected Critical Infrastructure Information (PCII) Program and the Homeland Security Information Network for Critical Sectors (HSIN-CS) are tools to facilitate information sharing, given the following:
 - Recognize the concept of “originator control” for all information submitted by the private sector as PCII, which would allow the submitter to limit how the information is used.

- When requesting information, the government must clarify why it needs the information, and it must explain how it intends to use it.
- All voluntary private-sector responses to a government data call should be deemed PCII.
- Legal protections must ensure that information voluntarily submitted as PCII will not be used for existing or additional regulation or government mandates.
- PCII protection must be extended to CIP information voluntarily submitted by industry to agencies other than DHS; time is of the essence when dealing with threat information.
- When housed on HSIN-CS, all information provided by the private sector should remain the property of the private sector and thus not be subject to disclosure under FOIA.
- The HSIN-CS portal should include a clearly delineated, simple mechanism for submitting information as PCII.

Other Recommendations:

The NIAC believes previous NIAC recommendations, for example those delivered on October 14, 2003, are relevant to this report as well, and ask that DHS continue to work to more fully implement the recommendations below:

- Crisis management plans should exist for each sector and be tested. Testing should include validation of cross-sector coordination. Testing and exercising sector crisis management plans should be under the purview of the sector coordinator.
- Establish a command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency.
- DHS should sponsor crisis management exercises that include the participation of the critical infrastructures, as soon as possible, and annually thereafter.
- Provide a framework for public and private emergency management interaction including national sector, state, regional, and local levels. This framework must account for information sharing mechanisms as well as review of significant public/private partnerships.
- Explore the potential for creating tax incentives or other instruments as incentives to encourage the private sector to enhance the resiliency of the critical infrastructures.
- The national labs 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. Start with modeling the telecommunications and energy sectors and the interdependencies among them and other critical infrastructures.

Conclusion:

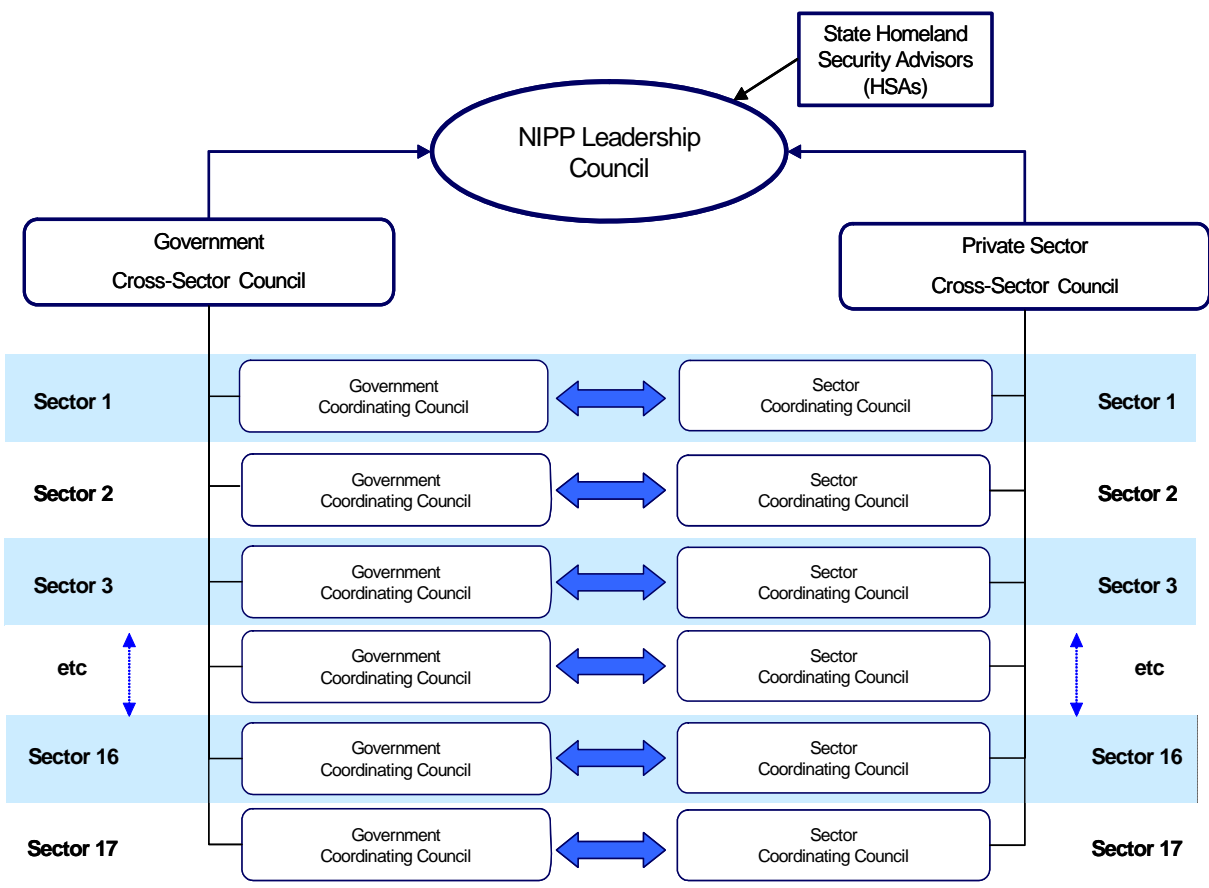
The public-private partnership is vital to the protection of our nation's critical infrastructure as well as the ability of the United States to respond to disasters. A true partnership is possible only if we establish the sovereignty and equality of all stakeholders. Hurricanes Katrina and Rita have pointedly demonstrated how critical it is to integrate infrastructure providers into the national preparedness and response effort. To strengthen this partnership, we must further integrate and embed it into all our national CIP plans, and the framework for engagement must be flexible enough to meet all current and future challenges.

It is imperative that:

- The partnership model be implemented immediately and that the HSA Section 871 exemption is granted across the partnership framework;
- National plans for infrastructure preparedness and response be reviewed to ensure adequate integration of all partnership stakeholders;
- Information sharing strategies and processes be reviewed to guarantee adequate support of both preparedness and response goals; and
- Lessons learned from Katrina and Rita are integrated into all national and regional plans.

Just as September 11 was this nation's wake-up call for prevention and protection themes of Homeland Security, the aftermaths of Hurricanes Katrina and Rita highlight the need for equally effective and coordinated response and recovery continuums. These recent events only emphasize the urgent need to integrate the Federal, State, local, and private-sector stakeholders into an effective, workable partnership model.

Appendix 1 Proposed Sector Partnership Model in I-NIPP



Appendix 2 Governance and Representation

GOVERNANCE AND REPRESENTATION SECTOR COORDINATING COUNCILS

Background

There is wide recognition that the securing of the nation's critical infrastructures and key resources is a shared responsibility between government and the owners and operators. The owners and operators have a responsibility to their shareholders, customers, and communities in which they provide service and operate to assure reliability and sustainability of their operations, services, and products. The government has responsibility to the public for assuring national and economic security, public safety and public confidence for which the critical infrastructures and key resources represent key pillars. Consequently, the owners and operators and the government each have independent activities and programs for which they have responsibility to implement and execute on their own to achieve their defined, and often complementary, missions.

At the same time, a successful national program requires coordination of programs, complementary skills, knowledge and resources of both the public sector and the owners and operators to assure efficiency and effectiveness in the face of continuing national level threats and disasters. For homeland security, in particular, adversaries tend to be tenacious, persistent and adaptable. Response to this type of threat requires an unprecedented level of cooperation and coordination. The federal government has reorganized itself through the Department of Homeland Security to assure coordination of homeland security programs throughout government. At the same time, owners and operators of most of the critical infrastructure and key resource sectors and their sub-sectors have chosen to organize themselves for intra-sector coordination through coordinating councils independent of government and with their own agendas for encouraging and taking action among their sector members.

The government desires to work with each of the sectors to coordinate programs, both national and local, to assure completeness and sufficiency of development and execution. The development of self-governed councils, representational of the owners and operators of their sectors and willing to take on an agenda of homeland security initiatives, provides for a mutually efficient means for the government to interact with the sector.

Interaction Issues Related to Governance and Representation

When government interacts with private-sector entities on policy matters, it has obligations to assure that its interactions are inclusive, avoiding conflicts of interest and providing equitable access to its resources and capabilities. Clarification is required and process may have to be addressed to assure that these principles can be met by the independent councils in interacting with government, whether they be composed and led by trade associations, individual owners and operators, or a combination. Particular issues have arisen regarding the role of trade associations in the councils.

As stated in the June 23, 2005 letter from the Partnership for Critical Infrastructure Security (PCIS), “Certain sectors participating in PCIS have chosen to have senior trade association officials play key roles in those sectors’ SCCs. We believe this decision should be acceptable provided no trade association is permitted to use its position in an SCC for competitive advantage with respect to other associations or to use that role as leverage in lobbying activities.” Several sector councils also consist mostly of trade associations, which fact leads to the following 3 questions:

- How can the government be assured and perception managed that if a senior trade association representative is selected by the sector as its lead spokesman, that he or she is speaking for the sector and not just the association’s interests? [It was noted by private-sector representatives that the same issue of perception could exist with an individual owner and operator selected as the sector council leader.]
- There are companies, some relatively large, owners of what the US may consider critical infrastructure and key resources, who may not belong to a trade association--- how would their views be represented in the SCCs, and in interactions with government? [The government cannot require an individual company to join a trade association in order to have a channel to interact with government.]
- Owners and operators have to make the investments and they have to respond to crisis along with government in the community where all incidents occur. Consequently, their operational perspective identifying critical assets, assessing their vulnerabilities and following through with mitigation “on the ground” is invaluable to government making decisions on policy and guidelines, and assessing and managing the national risk. How can access to this perspective be addressed uniformly or in different ways across the sectors?

Question 1 falls under the category of governance and questions 2 and 3 fall under the category of representation.

Governance

The sector coordinating councils were organized by the sectors as sovereign entities. They were organized voluntarily, independent of government, with structures and processes unique to each sector’s operations. They were intended to have broad sector representation, and self-governance frameworks that vary depending on the unique structure, culture and operations of each sector. This means that each chooses how it is governed, how representation is accomplished in determining its membership, and the leadership structure appropriate for effective and efficient operations for that sector.

Representatives of the federal government have expressed a preference that when it interacts with a sector that it interacts with an owner and operator, as a lead spokesman, to avoid the perception of giving advantage of access to one trade association over another, and to reduce confusion of the “lobbying” vs. the broader sector leadership role during an interaction. It is important to focus on the desired outcome rather than just the “how” in addressing this issue.

Sector councils range in composition of members consisting of all owners and operators to mostly trade associations to a combination. Many of the councils are chaired by an owner and operator but several have chosen senior trade association representatives as chairs. In doing so, some of these councils have also put in place governance processes that assure checks and balances that mitigate any competitive advantage that one trade association may gain through a leadership role in the council.

A case in point is reflected in how the Food and Agriculture Sector Coordinating Council has addressed this issue through its governance processes, described in a June 16, 2005 email from a chair of that sector's council: "It is undoubtedly true that trade associations were created for lobbying and advocating on behalf of their members, which arguably can be detrimental to non-members or to others within a given industrial sector or sub-sector. As you are aware the Food and Ag Sector Coordinating Council (FASCC) has 7 sub-councils with a total of 21 sub-council members sitting on the actual FASCC. Each of those sub-councils in turn can represent hundreds or even thousands of other entities (including other trade associations and corporations/companies/other). The potential for conflicts among the sub-councils kept the FASCC from electing leadership for a very long time and only recently did the FASCC decide that it was a necessary evil. To minimize the potential that an elected FASCC leader could exercise power and influence, or otherwise act to the detriment of others, we chose to have 3 equal co-chairs and have those chairs serve at the pleasure of the FASCC, subject to removal at any time. In addition, if an issue arises that is in the domain or expertise of a particular sub-council(s), the co-chair is supposed to refer the issue to the appropriate contact at the sub-council level. For example, inasmuch as I traditionally represent the interests of dairy processors (those that make fluid milk products, cheese and ice cream) and not dairy farmers, I would have to refer any farm specific issue to the producer (e.g. farmer) sub-council's leadership. Fortunately to date we have not had any internal conflicts because we understand that we must work together to enhance the safety and security of the food supply from the farm to the table. To everyone's credit I think we have each taken the high road and made sure that we have not acted inappropriately to the detriment of others." In summary, it is in the interest of the other members of the council to maintain vigilance and assure through its governance processes balanced representation by its leadership.

Finally, inclusiveness of the council also contributes to balance. For a diverse sector, trade associations play an invaluable role in assuring broad representation of the sector on the council. As described in the June 23, 2005 PCIS letter, "In fact, many SCCs have multiple trade associations participating in their SCC in an open, inclusive structure thus assuring all segments of the sector have a voice in the decisions of the SCC."

In the case of potential conflicts of interest, it has been recommended that an SCC chair – be it an owner/operator chair or an association chair – must be mindful that at times he or she may have a conflict and, in those instances, would be expected to recuse himself or herself from that role and appoint someone to act on the SCC's behalf on that issue. [This is a very normal process in private-sector Boards.] If the government thinks that

there is a conflict and the SCC chair is not recognizing that, it would be appropriate for the appropriate GCC to raise the issue with the SCC.

Representation

In working with the sector coordinating councils, the government assumes that a “representational” sector coordinating council consists of members who can provide leadership and networks of communication and influence into the sector as a whole, that differing as well as consensus owner and operator views/perspectives can be surfaced, and that it can bring to a public-private interaction sector-specific operational expertise and perspective, when they are needed.

Inclusiveness

Implicit in this assumption is that each council consists of senior enough members of the sector who either personally have the credibility to influence others within their sector or are representatives of institutions within the sector with such credibility. In addition, each sector coordinating council has a process to assure inclusiveness in participation or representation, including those owners and operators who may not belong to trade associations. A member of the working group, who is an attorney, pointed out that blocking access to the sector coordinating councils based on membership status in a trade association could raise significant antitrust issues. Many of the sectors already have processes in place to assure inclusiveness. It is recommended that those councils who have yet to develop such procedures be encouraged to do so.

A private sector member of the study group also suggested that as the Homeland Security Information Network (HSIN) progresses and develops, it will provide a means for appropriate and expanded interaction with government for the entire sector, whether an owner and operator chooses to be a member or not of a sector council or a trade association or Information Sharing and Analysis Center (ISAC). It is recommended that each sector council be encouraged to assure inclusiveness in developing the policy and strategy on establishing its presence on HSIN and encouraging the use of other information sharing mechanisms as appropriate for each sector such as ISACs. HSIN is funded by DHS and provided for each sector’s use through the strategic oversight of the sector councils.

Owner-Operator Perspective

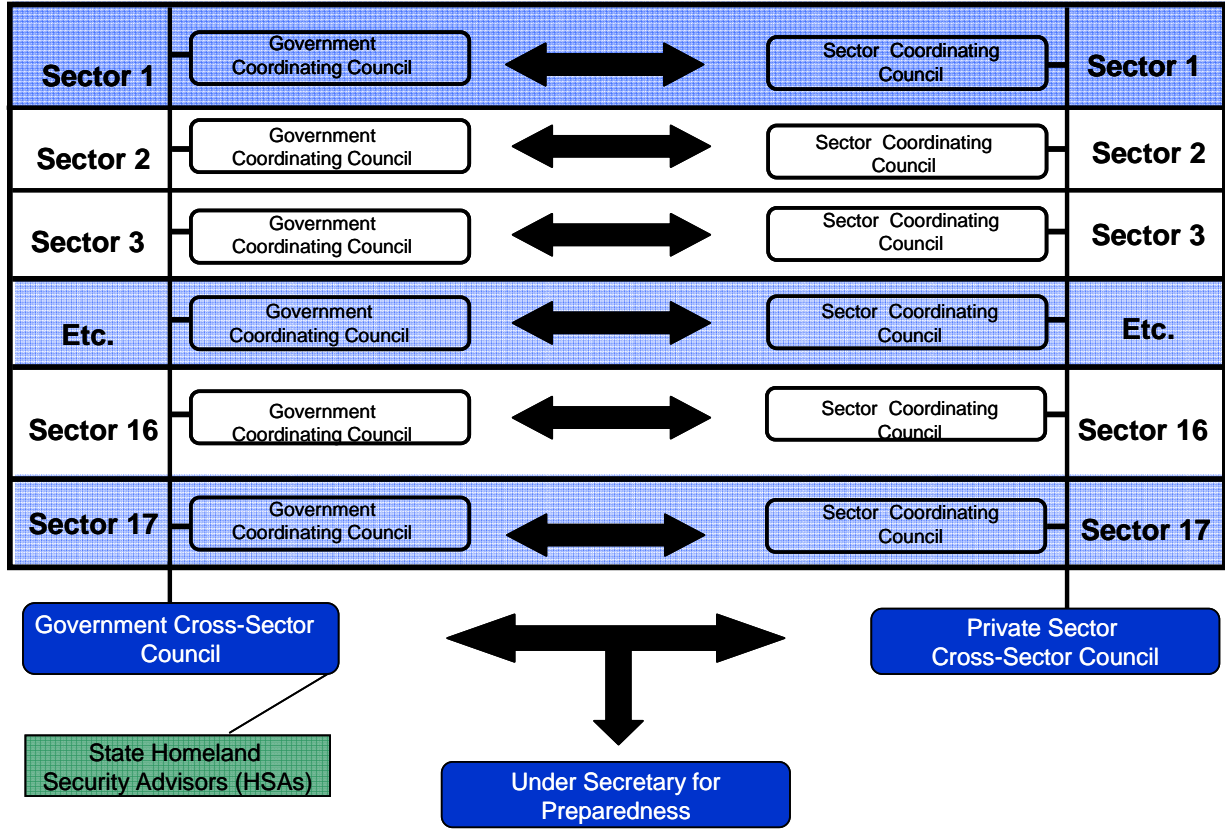
There is agreement among the sector councils on the “owner and operator focus”, including those composed predominantly of trade associations. As stated in the June 23 PCIS letter, “... sector trade associations are formed precisely to provide collective support for the activities of “owners and operators” ... , respond to the wishes of “owners and operators” ... , and must at all times remain aligned with the views of “owners and operators” within the sector.” Many of the sector councils include and are chaired by owners and operators. In either case, it cannot be expected that any council could

include all the expertise and operational perspectives required for all issues that could potentially arise in interactions with the government. However, with inclusive representation and access into their sectors, each council can identify and reach out to the person or entity within the sector appropriate to the need. Consequently, the government's need for access to diverse "owner and operator" perspectives can be satisfied.

Outreach and Sector Education on the SCCs

Private-sector members of the study group pointed out that assuring inclusiveness and willingness of a diverse range of owners and operators to participate in SCC programs and in interactions with government will likely require a coordinated outreach and education activity on the role and function of the SCCs for many of the sectors. Although the SCCs see such an activity as part of their role and responsibility, such an activity may require support from the federal government. The intent of such an initiative tailored for each sector is to identify and connect with companies, trade associations and other entities that thus far are not aware of or not engaged with the SCCs.

Appendix 3 Recommended Sector Partnership Model



Appendix 4 Sample GCC Charter

Food and Agriculture Government Coordinating Council Charter

1. Official Designation

The official designation of this Council is the "Food and Agriculture Sector Government Coordinating Council," herein after referred to as the "GCC."

2. Objective

The objective of the GCC is to provide effective coordination of agriculture and food security strategies and activities, policy, and communication across government and between the government and the sector to support the nation's homeland security mission. In addition, the Council plays a coordination role with the public health and clinical issues resulting from a terrorist act involving the food supply. It acts as the counterpart and partner to the private industry-led Food and Agriculture Sector Coordinating Council to plan, implement and execute sufficient and necessary sector-wide security programs for the nation's Food and Agriculture Critical Infrastructure.

3. Scope of Activity

The GCC will accomplish this objective through the following essential activities:

- **Identifying items that need public-private coordination and communication; and coordination and communication of issues.** The GCC shall bring together diverse federal and state interests to identify and develop collaborative strategies that advance critical infrastructure protection.
- **Identifying needs/gaps in plans, programs, policies, procedures and strategies.**
- **Acknowledging and recognizing successful programs and practices.** The GCC shall facilitate the sharing of experiences, ideas, best practices, and innovative approaches related to critical infrastructure protection. The GCC shall acknowledge and recognize accomplishments that further the objective.
- **Leveraging complementary resources within government and between government and industry.**

4. Membership

The membership will be composed of key representatives and influential leaders on food and agriculture safety/security issues from federal, state and local governments. Official members named to the Council are director-level, or equivalent representatives from:

- Department of Homeland Security
- Department of Agriculture
- Department of Health and Human Services/Food and Drug Administration
- Department of Defense

- Environmental Protection Agency
- Association of State and Territorial Health Officials – two representatives
- National Association of State Departments of Agriculture – two representatives
- National Association of County and City Health Officials – two representatives
- National Assembly of State Chief Livestock Health Officials

The Council reserves the right to invite ad hoc or ex officio membership to meet expertise requirements necessary to fulfill its mission.

The Council recognizes that each member represents a government entity or organization with inherent legal authorities and parameters within which they must operate. At times, these authorities may restrict a member's ability to provide agreement on a decision. These inherent legal authorities must be clearly articulated and understood by the Council as the basis for dissent and the inability to enter into consensus.

5. Roles and Responsibilities

Leadership of the activities and meetings rests with the three main federal agencies: DHS, USDA and FDA. Day-to-day leadership of meetings and activities would rotate among these three, with detail and procedures to be developed. The lead would collect from other members and initiate or bring issues to the GCC for consideration and deliberation. They will monitor and assure initiatives or issues are brought to closure, working with other council members.

There are 12 decision-making members of the GCC. There is one member for five federal agencies (DHS, USDA, FDA, DoD, EPA), two members each from state and local organizations (ASTHO, NACCHO, NASDA), and one member from the state veterinarians.

An alternate is assigned by each member to represent the Council member during his/her absence. The alternate will have decision-making authority as designated by the member as the member deems appropriate for the issues to be presented at a meeting. Each member has the flexibility to have other representation at meetings other than the official alternates, but must clearly designate the representative's decision-making authority prior to the meeting.

The Secretariat, provided by DHS, will provide meeting and organizational support to include: coordination for agenda development, support for agency lead on monitoring and closure of issues and initiatives, administrative support, logistics (travel, meeting room facility), and will establish a communication mechanism for the GCC and with the SCC.

Ex officio members are defined as non-voting participants whose criteria and qualifications for participating will be based upon the ongoing needs for expertise and decisions by the GCC leadership. The purpose of their membership is for the GCC to gain relevant organizational and institutional representation and expertise. Ex officio members may attend all meetings and conference calls. Ex officio membership will be withdrawn, by determination of the Council, as need for ongoing expertise is no longer required.

Subject matter experts are non-voting participants drawn from any organization from which the Council needs expertise on an ad hoc basis.

6. Workgroups

Workgroups are established when substantial investigation, research or other tasks are required which cannot be achieved at a regular GCC session. All products of the workgroups are meant to advise council members on various issues, directions and processes.

7. Principles of Participation

- All members must be working towards the same goal and purpose of improving the nation's agriculture and food system security;
- All members need to participate;
- Discussion and deliberations must recognize and take advantage of each members/organization's strengths, skills, and perspective;
- Result of GCC discussion and deliberations must be a coherent voice made up of each member's contributions;
- Each discussion shall be honest and forthright.

8. Number and Frequency of Meetings

The Council will meet quarterly in Washington, DC, with additionally scheduled meetings and/or conference calls as needed.

ANNEX A

Meeting Management

Standard Operating Procedures

Decision Making

Chapter 2 Quorum

A quorum for decision-making is defined as consisting of at least one representative from each of the three lead federal agencies and three state organizations: DHS, USDA, FDA, ASTHO, NACCHO, NASDA.

Chapter 3 Process

Council members will make decisions through a consultative process, encouraging the exchange of information and points of view, and will strive for consensus. Although any member may disagree with a decision, other members will strive to understand and strive to close the gaps creating the disagreement. Dissension will be recognized and reasons clearly understood by all other members when a member absolutely cannot agree. When there is dissension, the Council may move forward and take action, nevertheless, to fulfill obligations of members of the Council. GCC leaders/members will strive to meet timelines and deliverables even when less than full agreement.

The Council recognizes that each member represents a government entity or organization with inherent legal authorities and parameters within which they must operate. At times, these authorities may restrict a member's ability to provide agreement on a decision. These inherent legal authorities must be clearly articulated and understood by the Council as the basis for dissent and the inability to enter into consensus.

Meeting Support

The Secretariat will:

- 1) Consult with designated lead agency to provide support for developing agenda, maintaining a calendar for GCC and joint council meetings;
- 2) Provide to all members, no later than one week before the meeting, a clear and set agenda with documents and preparatory materials;
- 3) Compile the minutes of each meeting and send to GCC members with the leader concurrence within a week of the meeting for review and concurrence by all the members;
- 4) Develop processes to identify and develop issues to support Council and its leadership;
- 5) Maintain and follow up on the catalogue of GCC topic/issues and work products and their status;
- 6) Develop and implement logistics of meetings, either in person or teleconference;
- 7) Provide other support as needed.

Day to Day Communications

The Secretariat will maintain a list serve of Council members, which any member may use as deemed appropriate.

Meeting Governance

Discussion and deliberations must recognize and take advantage of each member's organization's strengths, skills, and perspective.

- 1) The lead, through the Secretariat, will canvass GCC members prior to the scheduled meeting for priorities and agenda topics;
- 2) The GCC will hold its discussion for set amount of time or upon agreement/closure, bringing in Subject Matter Experts as needed;
- 3) The lead member will ask for GCC agreement for continuation/completion/reconsideration for each agenda topic;
- 4) If substantial work effort is required through workgroups, the lead member will appoint a GCC member to lead the workgroup;
- 5) A minimum of three (3) GCC members must offer subject matter experts to the workgroup.

Leadership

Day-to-day leadership of the GCC will be held by DHS. DHS will designate HHS and USDA, on a rotating basis, to manage meetings using this repeating schedule. DHS will take the lead beginning August 1, 2004-October 31, 2004, followed by FDA November 1-January 31, 2005, USDA February 1, 2005-April 30, 2005, then DHS and so on.

Chapter 4 Establishing Work Groups

The Council establishes work groups:

- 1) To conduct substantial investigation, research and or development when required, which cannot be achieved by a regular session of the Council;

- 2) Which consist of representation to be determined by the scope of the topic;
- 3) By identifying a GCC member to lead to maintain continuity and consistency;
- 4) With specific and clear charge, time limit, and deliverable as part of initiating the work group;
- 5) Supported by the Secretariat as desired.

Ex Officio Membership

The GCC agreed on July 21, 2004 to include the departments of Commerce, Interior and Justice, and the Association of Food and Drug Officials as ex officio members. Their membership is based on the current needs of the Council and may be withdrawn at any time at the determination of the Council.

Appendix 5 Sample SCC Charter

Food and Agriculture Sector Coordinating Council Governance Principles and Operating Procedures

Background, Mission and Purpose

U.S. food and agriculture sector company owners, operators, and trade associations have organized themselves in an alliance to proactively and dramatically foster advances in the way the industry, in partnership with state and federal government agencies, protects the nation's food supply from farm to fork.

The Food and Agriculture Sector Coordinating Council (FASCC) was created by the industry to serve the sector's counter-terrorism and security interests. FASCC was formed using an inclusive and consultative process. The mission of the FASCC is to:

- Facilitate intra-sector communications, set processes for information sharing, and facilitate priority setting regarding sector: strategy and planning; policies and procedures; best management practices; threat communication and analysis; as well as sector protection, response and recovery planning and activities;
- Serve as the primary, policy-level interface with the Department of Homeland Security, and other federal and state agencies on homeland security matters;
- Facilitate communications, plans and activities with other relevant infrastructure sectors, government entities, and others necessary to further secure the nation's food supply and critical infrastructure; and
- Communicate the sector's needs and requests for resources to the government.

In considering new security structures, practices and procedures, the FASCC will seek to combine new security practices with the already existing communication and food safety systems, as well as the science and technology already in place in the food and agriculture industry.

Composition

During the sector organizing process, it was agreed that the FASCC will consist of representatives from Sub-Councils (currently seven). This process and structure is meant to result in the formation of one body (the FASCC) that can accurately represent the scope, breadth, depth, and interdependence of the American food and agriculture sector (i.e., owners, operators, and their associations) on security issues. Taken on their own, each of the initial seven Sub-Councils represents a significant component of the nation's economy and critical food and agriculture infrastructure.

The FASCC is made up of two designates and one alternate identified by each Sub-Council. The three Sub-Council representatives are expected to attend and participate in all FASCC meetings. The two representatives and alternate from each Sub-Council will

be named by a consensus process by the Sub-Council membership and will serve a two-year term on the FASCC. Consecutive or non-consecutive subsequent terms are permitted.

- FASCC members and alternates must, by definition, be employees of owners and operators of the sector or employees of their associations. Consultants, attorneys or other representatives who are not employees of owners and operators of the sector or their associations cannot serve as FASCC members or alternates.
- FASCC Alternates will automatically have decision-making authority when they sit in place of an absent member.
- In the event that a FASCC member cannot, or chooses not to, fulfill the term of their office, the relevant Sub-Council shall appoint a successor to fill the remainder of their term

FASCC Decision Making, Roles and Responsibilities

The FASCC will make decisions using a consensus process rather than majority-rule voting. This is consistent with the approach the sector used to organize itself to ensure inclusion of the diverse segments of the U.S. food and agriculture sector. Consensus is defined by a decision or action that all of the Sub-Councils represented on the FASCC can live with (i.e., choose not to block). Each Sub-Council will have equal voice in decision-making processes and will be allowed one official position in consensus decisions making.

- Council members should collect and convey information effectively, efficiently, and inclusively to their Sub-Councils members; consult as broadly as possible on pending decisions and issues requiring feedback to the government or others outside the Council; and initiate liaison with others who can help serve the security needs of sector members and the interests represented by their Sub-Council. This might include but not be limited to: other critical infrastructure sectors; research and academic institutions; and others.
- Council members should play a leadership role in helping their Sub-Council identify critical needs, problems and opportunities for their own Sub-Council area as well as identify areas for linkage across sub council areas as well as linkage to other critical infrastructure sectors or the government.

The responsibilities of FASCC members are to:

- Represent and communicate the interests of their Sub-Council to the Coordinating Council and the government in sector matters;

- Keep Sub-Council members apprised of key sector, inter-sector, and sector/government activities;
- Bring to bear their best judgment upon FASCC decisions based on their understanding and experience within their Sub-Council business area.

FASCC Meetings

- FASCC meetings will be open to members and alternates as participants and to sub-council members as observers. Leadership of each sub-council will determine those sub-council members that can attend FASCC meetings as observers, which in large part will be driven by the issues to be discussed at the FASCC meeting. Due to the potential size of FASCC meeting audiences as a result of the open policy, sub-council leaders will need to make notice of attendance early to the FASCC Secretariat.
- FASCC will meet on an as needed basis, as decided by the consensus of the Council, but will initially meet in person with conference call-in capability at least once every three months in its first year of operation.
- FASCC decisions can be made only when there is a quorum of participation (defined as at least one of the representatives or the alternate from each of the seven sub-councils). Because the FASCC will make decisions by consensus, it will be possible (though not desirable) to conduct meetings with only one representative of any one Sub-Council. The consensus decision-making process ensures that the protection of the interests of each Sub-Council is respected. This process is based on a presumption that a Sub-Council representative is in appropriate consultation and communication with her/his Sub-Council. Therefore, each Sub-Council must ensure that it has at least one of its three potential participants attending or participating in each session. In the event that none of the three representatives can attend, the sub-council will select an individual to be granted decision-making authority for the sub-council at that particular meeting. FASCC members are expected to prepare for each meeting taking appropriate consultations with the Sub-Council membership.

Principles of Participation in Council Meetings

- All members must be working towards the same goal and purpose of improving the nation's agriculture and food security system.
- All members need to participate by attending meetings, conference calls, and any other such activities whether called by the Sector (industry) or the government.
- Discussion and deliberations must recognize and take advantage of each members/organization's/Sub-Council's strengths, skills, and perspective.

- Results of FASCC discussion and deliberations must be a coherent voice made up of each member's and Sub-Council's contributions.

FASCC Secretariat

The Secretariat function for the FASCC will be provided by the Department of Homeland Security (DHS). The Secretariat will provide meeting and organizational support to include (but not limited to):

- Notifying members and alternates of meetings via email, telephone or both
- Distributing relevant background information prior to each meeting;
- Soliciting agenda topics for FASCC and Joint Council Meetings based on communication with Council members and alternates;
- Informing members and alternates of the agenda items, and particularly decision items likely to be taken up at each Council meeting on a timely basis
- Arranging for meeting locations and support logistics;
- Taking and distributing meeting notes,
- Maintain and following up on a catalogue of FASCC topic/issues and work products and their status
- Ensuring ongoing liaison with the Government Coordinating Council and other external entities.
- Maintaining an updated mailing list for FASCC members and alternates
- Identifying other support as needed and clarifying who should provide that support to the FASCC

Subject Matter Experts

Individual subject matter experts are non-voting participants of the FASCC or any Sub-Council drawn from any organization from which the FASCC or a Sub-Council needs expertise on an ad hoc basis. Subject matter experts may be invited to participate or assist the FASCC or Sub-Council by consensus agreement of the respective body.

Distribution of Material To the Sector

The FASCC will identify or designate material requiring distribution and potential feedback such as reactions to existing or proposed government policies, plans, or activities. Specific guidance will accompany material such as purpose, timeline, nature of feedback desired, format, and means of communication if of a sensitive nature. Because the FASCC is comprised of representatives of each Sub-Council the FASCC will heavily depend upon each Sub-Council to establish clear procedures and protocols for the distribution of information and material and the receipt of feedback, data, or other information.

Communication of Council Decisions and Meeting Summaries

The FASCC will distribute a summary of its meetings and any decisions to the sector via the processes and procedures established by each Sub-Council. Each Sub-Council will convey procedures to the FASCC and the Secretariat so that the means of distribution will be transparent to all within the sector. The FASCC Secretariat will be responsible for: 1) clarifying with the FASCC membership that the meeting summaries and decisions are accurate prior to release for distribution; 2) distributing the final summaries and decision messages to each FASCC member for communication to the Sub-Council members as determined by each Sub-Council's standard procedures and practices.

Requested Meetings, Materials, and Briefings

While not required, briefings, meetings and materials relevant to the interests of the Food and Agriculture Sector generally or which may involve interactive issues between sector Sub-Councils are encouraged to be conducted and conveyed to the FASCC through the Secretariat. Briefings, meetings, and materials uniquely relevant to only one Sub-Council and with no discernable interactive effects to other Sub-Council areas in the sector should be conducted or conveyed at the Sub-Council level. The default should be to err on the possibility of an integrative aspect and hence the primary area of action should be at the FASCC level. When a Sub-Council makes such a request they should notify the FASCC Secretariat.

If the government seeks input of a general nature of interest to the Food and Agriculture Sector it should make the request to the FASCC via the Secretariat. As above, requests unique to a particular Sub-Council should be made to that Sub-Council if there are no discernable interactive or interdependencies to other Sub-Councils, but the FASCC Secretariat should be notified and copied on the communications.

Sector Threat and Response

The FASCC will provide a useful role in ensuring appropriate mechanisms for communicating confidential and sensitive information from the government to the industry via the Sub-Councils, and from the industry to the government, on any actual, threatened or suspected malicious attacks so the information may be analyzed.

Each Sub-Council will be charged with the ability to create, interpret and assess the proper response to a potential threat or attack, as it relates to that Sub-Council's specific area. Further, they will develop the appropriate programs, procedures and processes that will mitigate or reduce the vulnerabilities of their specific areas.

In the area of sector threats and response, the FASCC and Sub-Councils will help in:

1. Detecting potential threats to the food supply infrastructures.

a. Working directly with the Department of Homeland Security, FDA, USDA and other government agencies, the FASCC and Sub-Councils will be able to identify credible threats and craft specific warning messages to the food industry.

2. **Assessing threat information.**

a. Provide information and analysis information that will enable the food industry to report, identify and reduce its vulnerability to malicious attacks.

3. **Providing timely warnings to the critical food supply operators so countermeasures can be developed and implemented**

a. Facilitate the development of “best practices”, recommendations and countermeasures for preventing and recovering from malicious attacks.

FASCC Sub-Councils

Role, Responsibilities, and Principles of Participation

During the sector organizing process sector members stressed the importance and essential nature of building sector coordination from clearly identified sub sector areas called Sub-Councils.

- Each Food and Agriculture Sector Sub-Council will develop definitions regarding the focus of the Sub-Council to assist in identifying the focus and boundaries of its sub-sector areas, and so that members of the sector can clearly identify which Sub-Council or Sub-Councils might involve their business and security interests.
- Each Sub-Council will define its membership, priority issues, and areas of work and activity. Each Sub-Council will need flexibility in prioritizing and identifying its needs, but should examine the general areas of: communications and information sharing; research and development, including prevention, detection; incident management; vulnerability assessments; and recovery.
- Outreach, participation, and membership at the Sub-Council level is intended to be as inclusive as possible of relevant owners and operators and their associations.
- Sub-Councils will articulate their priorities and action items to the FASCC, which then can communicate to the government, other sectors, and other appropriate entities
- Each Sub-Council will determine its own procedures for naming representatives to the council (two from each with one alternate) as well as replacing a member or alternate. In addition, each Sub-Council will take responsibility for naming an ad hoc FASCC representative for any one meeting when none of its named

individuals (i.e., the two members and one alternate) can attend. Sub-Councils should give some consideration to identifying “high risk” food groups, which would be communicated to the FASCC for consideration of additional inclusion in the FASCC.

- Each Sub-Council should establish its own decision making procedures and operating procedures given the nature of the standard business practices and relationships in that part of the food and agriculture sub sector.
- Each Sub-Council might consider the use of subject matter experts, Sub-Council member work groups, and/or advisory work groups to assist in their activities
- Each Sub-Council should establish a procedure for soliciting Sub-Council members’ views on policies, programs, and activities, especially when conveying input to government proposed or existing policies, plans, procedures, and activities.
- Each Sub-Council should establish and maintain Sub-Council membership lists and contact information as well as establish communication procedures for sensitive and non-sensitive information. These should be conveyed to the FASCC and updated on a regular basis.

Other Elements of Sector Participation

Participation in Sub-Councils should be broad and inclusive. All those with a legitimate business interest and the ability to make a meaningful contribution should be encouraged to participate. Participation in multiple Sub-Councils is appropriate whenever legitimate business interests are served.

Sub-Council representation on the FASCC is limited in order to maintain the efficiency of the FASCC and consistency in Sub-Council representation. In identifying members for the FASCC, the following guidelines may be helpful.

1. Two FASCC representatives plus one alternate are appropriate for each functioning Sub-Council.
2. Representatives should be chosen from organizations whose business or whose members mirror the scope of the specific Sub-Council as its members define it.
3. The individuals selected should be full-time employees of their organizations minimizing the chances that any actual or perceived conflicts of interest may develop.
4. While an organization may participate in multiple Sub-Councils, an organization may represent only one of those Sub-Councils on the overall governing council.

Appendix 6 SCC Purpose and Functions (Source: DHS)

SECTOR COORDINATING COUNCILS

PURPOSE & FUNCTIONS

BACKGROUND

For national critical infrastructure protection programs and initiatives to be successful there must be efficient and effective partnerships among DHS, Sector Specific Agencies (SSAs) and other federal agencies, state, local, and tribal entities, and private sector owners and operators.

Effective partnership across all levels of government and between government and private-sector stakeholders fosters greater coordination, communication, and collaboration among stakeholders. This encourages efficient risk management and contributes to the development of comprehensive, coordinated plans of action to prevent, deter and mitigate attacks on critical assets, and rapid response and recovery efforts that limit the consequences of attacks.

In order to effectively carry out the public-private partnership key to critical infrastructure protection, each critical infrastructure sector needs to establish a representative coordinating mechanism to specifically address homeland security issues and to engage with DHS and other government agencies with infrastructure protection responsibilities. There were no existing organizations or bodies that comprehensively represented the owner/operators in most of the individual critical infrastructure sector/key resource areas identified in President's National Strategy for Homeland Security and updated in Homeland Security Presidential Directive 7.

Government Coordinating Councils and private sector-led Sector Coordinating Councils (SCCs) provide a framework for intra-government and public-private cooperation, information sharing and engagement across the entire range of critical infrastructure protection activities.

PURPOSE

The broad purpose of Sector Coordinating Councils is to foster and facilitate the coordination of sector-wide activities and initiatives designed to improve physical and cyber security of the critical infrastructures.

Through SCCs, private-sector owners and operators can efficiently engage DHS and other federal agencies and collaborate to:

- Identify, prioritize, and coordinate the protection of critical infrastructure and key resource sectors

- Facilitate sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices
- Facilitate response and recovery activities and communication following an incident or event

FUNCTIONS

While specific functions may vary across sectors, depending on the unique characteristics of each sector, all Sector Coordinating Councils should, at a minimum, strive to perform the following functions:

- Represent a single point of entry for government into the sector for developing the entire range of infrastructure protection activities and issues
- Assist government in identifying and prioritizing vulnerabilities within the sector
 - Assist in the development of a plan to reduce and/or eliminate significant vulnerabilities
- Serve as an honest broker to facilitate inclusive organization and coordination of the sector's policy development, infrastructure protection planning, and plan implementation activities. Such activities include:
 - Sector-wide planning
 - Development of sector best practices
 - Sector-wide promulgation of programs and plans
 - Input into and implementation of national plans (such as the National Response Plan and National Infrastructure Protection Plan)
 - Research and development
 - Cross-sector coordination
- Identify, implement and support the information-sharing capabilities and mechanisms that are most appropriate for the sector. The core function of these information-sharing capabilities is to deliver alerts, warnings and advisories to their sector
 - Facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents and potential protective measures
- Develop and promote the "business case" to demonstrate to sector peers the value of participation in national infrastructure protection plans and initiatives
- Serve as a focal point for communication and coordination between owners and operators, and with the government during response and recovery
- Provide sector-specific expertise and advice during the response and recovery phase of an incident or event
- Offer sector-wide outreach and education

SCC CRITERIA

Sector Coordinating Councils should meet the following minimum criteria:

- The SCC must be broadly representative of the sector (*see HSPD-7 section, below*), with provisions in its charter to ensure inclusiveness and avenues for redress
- It must be self-organized, self-governed, and have a purpose independent of government
- It should be owner-operator focused, preferably with an owner/operator spokesman
- It should have a homeland security/critical infrastructure protection nexus

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7 (HSPD-7)

HSPD-7 establishes the basis for a national coordinated approach to critical infrastructure protection, including the development of the National Infrastructure Protection Plan as well as the Sector Partnership (GCC-SCC) Model that is codified in the Interim NIPP Base Plan.

HSPD-7 requires DHS to coordinate with the private sector to, “... collaborate with the private sector and continue to support sector-coordinating mechanisms:

- (a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and
- (b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.”

The model for public-private partnership through the Sector Coordinating Councils and Government Coordinating Councils, as well as through higher level Cross-Sector and Leadership Councils has been codified in the National Infrastructure Protection Plan (*see Chapter 5: Roles and Responsibilities, on page 29 of the Interim National Infrastructure Protection Plan*).

Appendix 7 Definitions (Source: DHS)

WORKING DEFINITIONS FOR PUBLIC PRIVATE COOPERATION ON NATIONAL CRITICAL INFRASTRUCTURE PROTECTION

Introduction

Clarity has been requested for terms being discussed by the NIAC's Sector Partnership Model Working Group (SPMWG) that help to define activities that can be taken on by sector coordinating councils, either independently or jointly with government. Of particular interest has been the following terms: facilitate, coordinate, promote, support, focal point. The Webster and the Merriam-Webster dictionaries provide several definitions that are relevant and meaningful to the intent (from the government's perspective) of these activities. This paper provides a selection of those relevant definitions and follows with a section describing how they can be applied to the various categories of activities, through illustrative activity descriptions, which appear to generate the greatest confusion, as indicated by the results of the SCC Charter Checklist results recently received by the study group.

Relevant Dictionary Definitions

- Facilitate
 - To make easier or less difficult
 - Free from difficulty or impediment
 - Lessen labor---aid or assist
- Coordinate
 - To act together in a smooth concerted way
 - To harmonize, characterized by cooperation
 - To bring into a common action, movement or condition
 - Bring into harmonious action
- Promote
 - Contribute to the progress or growth of
- Support
 - Give moral or psychological support or courage to
 - Be behind, approve of
 - Adopt as a belief
 - Argue or speak in defense of
- Focal point
 - A point of convergence

Illustrative Activity Descriptions

Homeland security and critical infrastructure protection require multiple and often concerted action by both owners and operators and the government. The development of self-governed sector coordinating councils, truly representative of the owners and operators of their sectors and willing to take on an agenda of homeland security

initiatives, provides for a mutually efficient means for the government to interact with each sector, if the sector so chooses. Without such a mechanism within a sector, the government would have to continuously identify relevant owners and operators, initiate communication, and build a structure and process for every issue or initiative that required interaction with the sector.

In working with these councils, the government assumes that a “representative” sector coordinating council can provide leadership and networks of communication and influence into the sector as a whole, that differing as well as consensus owner and operator views/perspectives can be surfaced, and that it can bring to a public-private interaction sector-specific operational expertise, when it is needed. The use of the terms “facilitate”, “coordinate”, “support”, and “promote” were intended to reflect this leadership quality and influence. The following activity descriptions is intended to illustrate how these terms may be applied for several of the functions of the sector coordinating councils that the SPMWG is studying.

- Identify and coordinate protection priorities
 - Work with counterparts in government to develop common goals and protection plans, including common goals and agreement on where to invest research and development dollars, and where to apply available government resources to have the greatest mitigation of risk for the sector
 - Develop policy, process and structure, as needed, to harmonize public and private investments, and protection plans and execution
 - Identify obstacles and work with government counterparts in problem solving mode to address
- Facilitate response and recovery activities
 - Identify requirements for a sector’s national response plan and execution
 - Identify and develop policy, structure and process, as needed, unique to each sector, for national response and recovery for the sector, including communication coordination at the leadership and operational levels, and with the government
 - Identify and encourage most appropriate practices for members of the sector
- Single point of entry for government into the sector for CIP activities/issues
 - Initial point of entry to introduce CIP programs, activities or issues
 - Identify and work with government counterparts to determine most appropriate process and structure for or within the sector to work with government to address the program, issue or activity
 - Work with government counterparts to determine priorities of items to be introduced and how to manage potential barrage of requests
 - Work with government counterparts to harmonize government interactions with the sector to reduce duplicative or overlapping interactions and items
- Assist government in identifying and prioritizing vulnerabilities
 - In conjunction with prioritizing protection priorities, identify where research and development and other resources may best be applied to have the greatest return (e.g. SCADA systems) to mitigate risk

- Identify obstacles to such cooperation and work with government counterparts to address in problem solving mode, which could include policy development, legislation, or a unique structure and process to address the particular priority issue
- Identify most appropriate information sharing and analysis mechanisms
 - Determine the policy, strategy, structure and process most beneficial for most of the sector
 - Develop structure and process to work with government counterparts to implement sector policy and strategy for public-private information sharing and analysis
- Promote value of participation in national protection activities
 - Communicate and encourage the application of sector best practices
 - Communicate and educate sector members on national programs planned or in execution or identify sector strategy, structure and process needed to do so
 - Work with government counterparts to develop and implement strategic communication program on national sector and public-private cooperative activities
- Focal point between owners and operators, and with the government during response and recovery
 - As the leadership group for the sector, develop process and structure for coordinating communication on operations during response and recovery, or identify policy, develop strategy, structure and process to achieve same within the sector, including testing the structure and process as needed in conjunction with government counterparts
 - Identify obstacles and work with government counterparts in problem-solving mode to address
- Provide sector-specific expertise and advice during response and recovery phase of an incident or event
 - Develop a structure and process to bring expertise to the table from within the sector as needed by the situation and the issue
 - Coordinate execution of process

Note: These are illustrative activities. Sectors and their operations vary dramatically and consequently the activities the sector councils and their counterparts in government may undertake can vary dramatically.

Appendix 8 FACA Fact Sheet

Federal Advisory Committee Act (FACA)

The Federal Advisory Committee Act (FACA) was enacted in 1972 and designed to enhance public accountability of advisory committees and to reduce wasteful expenditures on advisory committees. The FACA defines an advisory committee as “any committee, board, commission, council, conference, panel, task force or other similar group which is established by statute, or established or utilized by the President or by an agency official, for the purpose of obtaining advice or recommendation.”

The following is a list of the key provisions pertaining to advisory committees that are contained in the FACA, the General Services Administration's implementing regulations (41 CFR Parts 101-6 and 102-3; 66 FR 37728, July 19, 2001), or Management Directive 2300 of the Department of Homeland Security on the subject of Committee Management.

These provisions generally do not apply to subcommittees of an advisory committee that report to the parent advisory committee and not to a Federal official, provided that the Federal government does not manage or control the subcommittee and that the advice and recommendations of the subcommittee are not merely "rubber stamped" by the parent committee.

-
- Notice of establishment of advisory committee to be published in Federal Register 15 days before its charter is filed
 - Waiver of 15 days by GSA allowed for good cause.
 - Sponsoring Federal agency must approve holding of each meeting and prepare and approve the agenda.
 - Notice of meetings must be published in Federal Register 15 days before meetings, summarizing agendas; multiple meetings can be noticed.
 - Exception from notice for national security reasons.
 - Waiver of 15 day requirement by Federal agency under exceptional circumstances.
 - Federal official must be in attendance at meetings, and may adjourn them; may chair a meeting when so directed by head of sponsoring agency.
 - Each meeting to be open to public. Meeting places to be accessible. Interested persons may attend, speak, file statements, subject to reasonable rules adopted by the committee or by the chairperson and the Designated Federal Officer for the

committee (the DHS directive is inconsistent as to which means of adopting rules applies).

Exception when Federal agency makes determination to close meeting under Government in the Sunshine Act, 5 USC 552b(c). Generally, a request to close a meeting should be made 30 days before the meeting.

- Committees may meet by teleconference, but must comply with the requirements for open meetings, such as by having sufficient communication lines for non-members.
- Unless prior Federal agency legal counsel concurrence is obtained, advisory committees may not receive, compile or discuss data or reports concerning matters that would be exempt from disclosure under FOIA exemptions (b)(4) and (6), which deal, respectively, with records that are trade secrets and commercial or financial information and records, the release of which would constitute a clearly unwarranted invasion of personal privacy, and with personal information whose release would be a violation of privacy.
- Voting by email not allowed, and mail ballots may be used only for issues discussed in a public meeting or a meeting properly closed to the public.
- Detailed minutes of meetings required, including a complete description of matters discussed and conclusions reached, and copies of all reports received, issued or approved. Accuracy of minutes to be certified by committee chairman.
- Records, reports, transcripts, minutes, appendices, working papers, drafts, studies, agenda, or other documents prepared by or made available to committee to be available for public inspection and copying
- Sponsoring Federal agency to provide support services.
- Sponsoring Federal agency must approve the creation and operation of subcommittees.
- Advisory committee created for term of two years, subject to renewal.

Appendix 9 PCIS Letter



June 23, 2005
Ms. Susan M. Vismor
Sector Partnership Model Integrated Study Group
National Infrastructure Advisory Council
c/o Mellon Financial Corporation
3 Mellon Center -- Suite 4100 (143-4100)
Pittsburgh, PA 15259

Dear Susan,

The Partnership for Critical Infrastructure Security, Inc. (“PCIS”) thanks you and the National Infrastructure Advisory Council (NIAC) for the opportunity to provide comments on establishing an effective sector partnership model for the private sector and government to work together.

The PCIS has been actively involved in encouraging and participating in a productive public/private partnership with the Federal government over the past five years and applauds efforts to make the relationship even more effective. PCIS was formed in 2000 to work on cyber and physical cross-sector critical infrastructure protection and interdependency issues of concern to the private sector. After September 11th, the mission of the PCIS became even more significant and pressing: improve the security and safety of the nation’s critical infrastructures by enabling critical infrastructure sectors to work among themselves as well as work in partnership with the Federal government. PCIS acknowledges that the private sector, which owns and operates the vast majority of the critical infrastructures and key assets, plays a key role in protecting this nation’s infrastructures and can provide a great deal of assistance to the government at all levels with respect to the government’s responsibility to protect the people, property, and economic prosperity of the country.

Regarding the interactions between the private sector and government, much of the work to date has focused on the process by which DHS and other agencies and the

private sector can work together. The time has come to focus on tackling specific issues that will directly contribute to the common mission. Essentially, the most effective model for a partnership is one that produces results. We feel that mechanisms such as Sector Coordinating Councils do have the ability to effectively work with their government counterparts provided both sides keep certain guidelines in mind.

At a PCIS meeting held on June 14th, one of the topics the group addressed was developing a number of priorities, requests, and methods to address current and pressing issues for an effective public-private partnership – with respect to process, structure and substantive issues.

PCIS believes that the actions for improving the partnership fall under three categories:

- Resolving structural issues regarding the sector coordinating mechanisms and their interactions with their governmental counterparts,
- Removing impediments to the flow of information between various entities in the government and the private sector (in both directions),
- Accelerating the process of addressing infrastructure protection issues.

Our thoughts and concerns on each of these action areas are listed below:

Resolving structural issues

As a general matter, members of PCIS accept the overall structure of the sector partnership model outlined in the Interim National Infrastructure Protection Plan (Interim NIPP). The formation of individual Sector Coordinating Councils (SCCs) (“sector coordinating mechanisms,” in the language of Homeland Security Presidential Directive 7 (HSPD-7)), the “pairing” of SCCs with Government Coordinating Council (GCC) counterparts, and the provision for higher-level cross-sector bodies, all appear reasonable to PCIS members. In addition, as you may be aware, PCIS believes that it already functions, as a practical matter, as the Private-Sector Cross-Sector Council contemplated in the Interim NIPP model. The recent PCIS reorganization was expressly intended to ensure that the PCIS conformed to that aspect of the model and could function in that capacity. During our recent meeting, individual sectors reported on the status of their own organizational efforts and it appears that these efforts are proceeding very effectively on both the private sector and governmental sides.

The PCIS has identified several issues important to the efforts of your working group in improving the partnership:

- The Interim NIPP model contemplates that the Sector Coordinating Councils are truly self-formed entities with the private sector determining how the groups are formed, who their members are, and how they are governed. The SCC must interact with government, and government will have certain expectations about those interactions (*e.g.*, what government expects to receive from the SCC), but most aspects of the SCCs’ operations are the private sector’s business.

- We agree with those principles. However, we note that “self governance” means, among other things, that SCCs are free to determine which leadership structure is most appropriate for the sector and to freely define their membership. In contrast, past pronouncements from DHS seem to indicate that DHS expects SCC leadership should invariably be drawn from “owners and operators” within the sector and that senior officials from sector trade associations or other similar sector organizations should not be senior officers of the SCC. PCIS believes that such a position conflicts with the principle of self-governance and fails to recognize that sector trade associations are formed precisely to provide collective support for the activities of “owners and operators” (and often their suppliers) within the sector, respond to the wishes of “owners and operators” within the sector, and must at all times remain aligned with the views of “owners and operators” within the sector. Certain sectors participating in PCIS have chosen to have senior trade association officials play key roles in those sector’s SCCs. We believe this decision should be acceptable to DHS and other governmental bodies involved in infrastructure protection provided no trade association is permitted to use its position in an SCC for competitive advantage with respect to other associations or to use that role as leverage in lobbying activities. In fact, many SCCs have multiple trade associations participating in their SCC in an open, inclusive structure thus assuring all segments of the sector have a voice in the decisions of the SCC.
- For certain sectors, HSPD-7 expressly designates “Sector-Specific Agencies” (SSAs) as having responsibility for critical infrastructure protection for their sector, within the overall direction of DHS. The discussion at our June 14th meeting suggested that roughly half of the sectors have SSAs other than DHS designated as their principal governmental interface. The Interim NIPP Sector Partnership Model is not clear as to the role the SSAs play in relation to their designated sectors, and several sectors report conflicts between the Information Analysis and Infrastructure Protection Directorate (IAIP) of DHS, their SSA, and/or other directorates inside DHS handling infrastructure protection activities. We believe that the Interim NIPP model, or some statement or guidance associated with it, should clarify that, for sectors with designated SSAs other than DHS/IAIP, the SSA will be the governmental interface for that sector’s SCC, and that DHS/IAIP should go through that SSA in interfacing with that sector. Certain sectors also report that representatives of the Federal Bureau of Investigation have approached the sectors and the SCCs with indications that the FBI should interface directly with the SCCs on infrastructure protection issues. Again, we feel strongly that such conflicts among governmental entities as to who has the “authority” to work with the sectors are confusing, duplicative, and enormously wasteful of the private sector’s time and effort. Again, for those sectors with SSAs other than DHS/IAIP, that SSA should be the interface. For those sectors which have a DHS office as their SSA, that DHS office should be the interface.

- The Interim NIPP contemplates sectors will self-organize into Sector Coordinating Councils and use associated information sharing and analysis mechanisms (ISAMs). Many sectors have already done this by creating Information Sharing and Analysis Centers (ISACs), and others are in the process. We expect that, with all the efforts the government is asking the private sector to put into creating these channels, whatever ISAM/ISAC is identified by the sector's SCC will be used by government to address alerts and infrastructure protection issues and information sharing. Far too often sectors have seen governmental representatives bypassing the existing SCCs and ISAMs/ISACs to interface with other sector organizations, distributing information, requests for information, requests for policy guidance, etc., to a broad array or subset of sector members, often with the SCC knowing nothing of these contacts. At other times SCCs are asked to provide information about specific sector contacts with this information subsequently used to bypass the SCC on follow-up matters that should be more appropriately directed to the SCC. These actions have to stop if we are to have an effective partnership with government. If we are creating these channels at the government's request for the governmental interface, those channels should be used as the primary interface, and, in the very rare situations where time does not permit their use, the SCCs need to be kept informed about other sector contacts.
- As you know, members of PCIS have participated in the discussions of your working group and are aware of the issues regarding the applicability of the Federal Advisory Committee Act (FACA). DHS was kind enough to arrange for DHS staffers to participate in the June 14th meeting to discuss these issues. It is clear from the discussion that: (1) there are very substantial questions regarding the applicability of FACA to the SCCs and their work, and (2) there are very serious concerns regarding the information disclosures that would be required under FACA. With respect to private sector entities, we are of the view that Secretary Chertoff should use his statutory authority to exempt the SCCs and PCIS from FACA requirements in order to assure the private sector that its information will not be subject to disclosure and to avoid overly bureaucratic, delaying, and confusing mechanisms to meet and communicate on such time-sensitive matters as protecting our nation's critical infrastructures.

Removing impediments to two-way information flow

A principal concern of the PCIS continues to be the need to improve the process of information flow both from the private sector to government and from the government to the private sector. Government information that should be provided to private sector owners and operators of critical infrastructure often is not provided (frequently due to security restrictions that clearly are counterproductive). Government requests for information from the private sector are frequently duplicative and raise concerns about

confidentiality and potential misuse. The group identified some specific points to help address these issues:

- While we commend DHS for the efforts to implement programs under the Critical Infrastructure Information Act, we think efforts to date have fallen short. Once protected critical infrastructure information (PCII) has been submitted, submitters lose all control over what is done with that information and to whom it is given. We believe that the concept of “originator control” needs to be introduced for all information submitted by the private sector, allowing the submitter to limit how the information is used both in extent and in time. In addition, the purpose, need, and applicable protections (PCII or otherwise) for any information given to the government by the private sector whether voluntarily responding to a request or otherwise needs to be clarified.
- As a corollary to the above, additional legal protections ensuring voluntarily submitted information will not be used for additional regulation or government mandates need to be established.
- Legislation should be enacted to ensure non-discovery of shared information as well as limitations on liability associated with that information (current legislation protects some information from discovery by or from the government but needs to better prevent discovery by third party litigants in private actions against the company). This is not meant to limit the availability of information to state and local emergency service providers for planning and response purposes.
- The private sector needs assurance that information it submits via the Homeland Security Information Network (HSIN) will remain confidential. This applies to information distributed over HSIN between the government and private sector as well as information disseminated only among private sector participants using HSIN.
- The government has taken some very positive steps with its efforts to form Government Coordinating Councils comprised of the relevant government agencies working with particular sectors. This effort should continue to ensure that the private sector is not approached with duplicative requests for information and that the SCC is not confused as to how to both get and receive information from the government. As with coordinated efforts in communicating with the private sector, more government agency coordination will increase the amount and quality of information from the private sector. It is important to note that the issue of duplicative requests from governmental entities involves not just duplication among Federal agencies, but also duplication by State and local governmental entities similar to the requests at the Federal level (and vice versa). This last concern indicates the importance of integrating state, local and regional efforts into federal initiatives from the beginning.
- An effective two-way communication regime is particularly important to ensure that threat information is effectively communicated to the private sector and the

private sector provides needed critical information to the intelligence, preparedness and response communities. Security clearances need to be processed promptly for SCC members (our sense is that this is moving along reasonably well, but could be improved). In addition, some form of routine interaction should be implemented permitting cleared SCC representatives from particular sectors to interact with intelligence agency representatives regarding classified threat situations relevant to their sectors. We plan to raise this issue with the NIAC's Intelligence Coordination Working Group also.

Accelerating infrastructure protection

September 11th occurred almost four years ago. While we have all expended considerable effort in the intervening years to improve the resilience of our nation – and we have achieved substantial progress in doing so – it is clear to PCIS that there is much more that needs to be done. At our June 14th meeting, we had the benefit of a presentation from the nuclear sector regarding a “comprehensive review” process that sector has initiated that promises significant improvement (from already high security/protection levels) in the coordination of the response to an emergency involving a nuclear power plant. The presentation again underscored our sense of the urgency in moving forward with more concrete and directed efforts to protect the infrastructures in many of our critical sectors. To do this, we believe we need the following actions:

- Clarification regarding how, specifically, the government plans to proceed in assisting the private sector in protecting critical infrastructure, including identifying what added protection has already occurred and what is planned. This will help the private sector in giving additional comments to the government in meeting its goals.
- Work with each of the sectors to determine the most effective methodology for comprehensive reviews whether that be CARVER, RAMCAP, industry vulnerability studies, etc. Industry should be brought in at the beginning of this process to help formulate the relevant protection goals and information needed to obtain them.
- Increase the focus on protective measures and the goals set forth in the National Response Plan (NRP).
- Coordinate and integrate State, Local and Regional Planning initiatives with Federal initiatives (*e.g.*, State and Local Role in Sector-Specific Plans (SSPs), NIPP, NRP, etc.).

The PCIS wishes to thank you for the opportunity to share this list of actions and recommendations for an improved public-private relationship. We all realize that this is a unique undertaking with challenging issues. PCIS is prepared to work closely with DHS and the SSAs to place infrastructure protection on a fast track. We recognize, however, that there is no single solution to the nation's infrastructure protection needs. The process by which infrastructure needs can be met and the associated timeframe will necessarily vary depending

upon the sector involved. This is all the more reason, in our view, why it is imperative that we pick up the pace.

The members of PCIS are available for further discussions with you regarding these items.

Sincerely,

A handwritten signature in black ink, appearing to read "Donahue", with a long horizontal flourish extending to the right.

Donald F. Donahue
President, the Partnership for Critical Infrastructure Security

Cc PCIS Members
Robert Stephan, DHS
Al Martinez-Fonts, DHS
Jim Caverly, DHS
Nancy Wong, DHS
Rod Nydam, GMU