

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Office of Infrastructure Protection

Critical Infrastructure Partnership Advisory Council

AGENCY: Preparedness Directorate, Office of Infrastructure Protection, Department of Homeland Security.

ACTION: Committee management: notice of committee establishment.

SUMMARY: In order to facilitate an effective defense of our Nation's critical infrastructure, the Department of Homeland Security is creating the Critical Infrastructure Partnership Advisory Council. Pursuant to the Homeland Security Act of 2002, the Department is taking measures to facilitate strategic planning and effective discussion of critical infrastructure issues and to protect sensitive critical infrastructure information while also observing appropriate public disclosure procedures for the council.

Name of Committee: Critical Infrastructure Partnership Advisory Council (CIPAC).

FOR FURTHER INFORMATION CONTACT: Brett Lambo, Infrastructure Programs Office, Infrastructure Partnerships Division, Office of Infrastructure Protection, Preparedness Directorate, United States Department of Homeland Security, Washington, DC 20528, telephone (703) 235-5311 or via e-mail at brett.lambo@dhs.gov.

SUPPLEMENTARY INFORMATION:

Background

1. The Department's Relationship With Owners of Critical Infrastructure

Approximately 85 percent of this nation's critical infrastructure is owned by the private sector. *See, e.g.*, National Infrastructure Advisory Council Report, Sector Partnership Model Implementation: Final Report and Recommendations 6 (Oct. 11, 2005) ("NIAC Report"). Thus, in drafting the Homeland Security Act of 2002, Congress repeatedly stressed that the new Department of Homeland Security must have a close and highly effective relationship with the private sector owners of this infrastructure. *See,*

e.g., 6 U.S.C. 121(d)(11) (requiring consultation with “private sector entities to ensure appropriate exchanges of information”); 6 U.S.C. 112(c) (requiring coordination with non-federal entities); *see also* Statement of Senator Joe Lieberman, Nov. 16, 2005 (“That’s why we created an Infrastructure Protection division in the Department of Homeland Security which was the first of its kind at any federal agency. The point was that government needed to work with the private sector to make sure the systems so crucial to our way of life were adequately protected, and if attacked by terrorists or overwhelmed by natural forces, were able to recover quickly and restore services.”).

Congress explicitly instructed the Department to create an effective structure for sharing sensitive information with the private sector on infrastructure. Congress also explicitly mandated that the Department “ensure the security and confidentiality” of sensitive homeland security information, and gave the Department specific new authorities to protect such information. *See* 6 U.S.C. 131 *et seq.*; 6 U.S.C. 451; 6 U.S.C. 482.

Over the past two years, the Department has consulted with Congress and with the Department’s private and public sector partners and advisory committees to assess the strength and effectiveness of its relationships with private sector owners of critical infrastructure. The Government Accountability Office and others have reported that the private sector continues to resist sharing critical infrastructure information with the Department. *See, e.g.*, Govt. Acct. Off., Rep. No. GAO-03-1165T, Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues 26 (Sept. 17, 2003) (“As noted in our February 2003 report, some in the private sector expressed concerns about voluntarily sharing information with the government.”); Govt. Acct. Off., Rep. No. GAO-06-150, Homeland Security: DHS is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority is Needed 55-56 (Jan. 2006) (“While the industry wants to cooperate with DHS on its chemical security efforts, businesses are concerned that sensitive information could be released.”); Homeland Security Advisory Council Report, Homeland Security Information Sharing Between Government and the Private Sector 1 (August 10, 2005) (“HSAC Report”) (stating that effective cooperation between DHS and the private sector “has been hampered by a variety of legal and procedural obstacles”); *compare* 148 Cong. Rec. S11002, S11001 (Nov. 14, 2002) (Senator Lieberman) (“We have to close vulnerabilities in those [critical infrastructure] systems before terrorists strike them. To do so, we have to be working with the private sector.”).

A number of advisory councils have recently re-assessed this problem and provided recommendations to the Department. For example, after a lengthy study in August of 2005, the Homeland Security Advisory Council (HSAC) opined:

Fundamentally, the challenge of ensuring the resilient/reliable operation of critical infrastructure is unique, as it requires close communication and coordination between critical private sector entities and the Federal agencies charged with regulating them. Those communications, moreover, must remain non-public in order for those functions to be served. As specified in statute, these communications are to involve intelligence and

law enforcement information, and are to serve warning, preventative and protective functions. Disclosing this sort of information would defeat the purpose of these communications by giving our nation's enemies information they could use to most effectively attack a particular infrastructure and cause cascading consequences across multiple infrastructures.

HSAC Report at 30.

2. Identifying Solutions

The Department's principal advisory committees specifically concluded that concerns regarding the Federal Advisory Committee Act (FACA) have frustrated vital communication between DHS and critical infrastructure sectors. This Act, when it applies, generally requires advisory committees to meet in open session and make publicly available associated written materials. 5 U.S.C. App. 2 sec. 10. **It also requires a 15-day notice before any meeting may be "closed" to public attendance, a requirement which could prevent the Department from meeting on short notice to discuss sensitive information in an appropriate setting.** The Act contains a number of exceptions to its general disclosure rules, but the applicability of those exceptions presents what many view as a significant litigation risk. *See, e.g.,* NIAC Report at 14. **The Department's consultations with the Department of Justice have reinforced this conclusion.**

The HSAC summed up the potential consequences of public disclosure of the sensitive information:

Communications [between critical private sector entities and the Federal Government] must remain non-public * * * Disclosing this sort of information would defeat the purpose of those communications by giving our nation's enemies information they could use to most effectively attack a particular infrastructure and cause cascading consequences across multiple infrastructures.

HSAC Report at 30. Because of these concerns, the HSAC recommended that DHS consider using its authority under section 871 of the Homeland Security Act of 2002, 6 U.S.C. 451, to exempt critical infrastructure advisory committees from the FACA requirements. Section 871 provides the Secretary of Homeland Security with the authority to establish advisory committees and exempt them from the FACA. 6 U.S.C. 451(a). **This authority allows the Department to enhance the incentives for providing the Department with information and recommendations that would not otherwise be provided.** The National Infrastructure Advisory Council (NIAC) also considered this authority and drew a conclusion similar to the HSAC:

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 communications during emergencies.

NIAC Report at 12. The NIAC went on to opine that exercising the exemption will have a direct effect: “Interactions between the government and private sector will increase, and the flow of information will be much more efficient.” *Id.* at 15. The NIAC found the exercise of the exemption authority to be “essential” for “short- and long-term success.” *Id.* Without exercising the exemption authority, according to the NIAC, DHS will not be able to accomplish its critical infrastructure protection and information sharing goals. *Id.* at 15-16; *cf.* Govt. Acct. Off., Rep. No. GAO-02-811T, National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy 9 (June 7, 2002) (“[I]n recent discussions with us, industry officials said that their chief concern in sharing information about vulnerabilities and attacks is disclosure of proprietary data.”).

3. Exercise of 871 Authority in a Manner Intended To Respect Principles of FACA

Despite many past requests, **the Department has not previously exercised the authority Congress provided in Section 871. This reluctance has been due in part to a respect to the principles of open-government. Given mounting evidence that the use of this authority could improve the Department’s ability to protect critical infrastructure and perform strategic planning, the Department is now invoking that authority *but*, as explained below, in a manner intended to preserve the principles of open government embraced by FACA. Out of concern for those principles, the Department has chosen to institute procedures calling for as much public disclosure as is consistent with homeland security goals.**

The decisions announced in this Notice are consistent with longstanding efforts to increase our capacity to protect our critical infrastructure and key resources. Since September 11, 2001, numerous authoritative bodies—the Congress, advisory councils, and the 9/11 Commission among them—have stressed the importance of information sharing between the federal government and the private sector. *See, e.g.*, National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States 398 (authorized ed. 2004) (“Homeland security and national preparedness * * * often begins with the private sector.”); 148 Cong. Rec. S11405, S11414 (Nov. 19, 2002) (statement of Senator Lieberman stressing the importance of “engaging the private sector” in anti-terrorism efforts).

Protecting critical infrastructure and key resources (CI/KR) requires a comprehensive, effective, and collaborative partnership between all stakeholders. Collaboration among stakeholders must involve many activities: planning; coordination; security program implementation; operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution from events both

man-made and naturally occurring; and the sharing of information about threats, vulnerabilities, protective measures, best practices, and lessons learned.

An effective partnership must be predicated on the ability to have ongoing, immediate, and multi-directional communication and coordination between the CI/KR owners and operators and government, including under highly exigent circumstances. During the course of these activities, policy advice and recommendations may emerge and be provided to the Department of Homeland Security and Sector-Specific Agencies (SSAs). Consequently, the depth and breadth of the mission have unique requirements for comprehensive interactions. The CI/KR sectors are so vital to the nation's economy, public safety and confidence that it merits use of all necessary authorities to support their protection.

4. Establishment of the Critical Infrastructure Partnership Advisory Council

In furtherance of DHS' mission to safeguard CI/KR sectors, the Secretary has determined that the public interest requires the establishment of the CIPAC. The CIPAC will support implementation of the National Infrastructure Protection Plan (NIPP) and will help to effectuate the sector partnership model set forth in the NIPP. Specifically, the CIPAC will **facilitate interaction among government representatives at the Federal, State, local, and tribal levels and representatives from the community of CI/KR owners and operators in each critical sector to engage in, among other things, planning; coordination; security program implementation; operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution from events both man-made and naturally occurring; and the sharing of information about threats, vulnerabilities, protective measures, best practices, and lessons learned.**

These activities require regular, ongoing, and multi-directional communication and coordination between CI/KR owners and operators and government, and to have the ability to do so under highly exigent circumstances. During the course of these activities, policy advice and recommendations may emerge and be provided to the Department of Homeland Security, the SSA for each sector identified in HSPD-7, and the other Federal departments and agencies supporting the critical infrastructure protection mission under the NIPP. These departments and agencies have responsibility for establishing and implementing Federal policy and managing Federal programs. The CIPAC has no authority to establish Federal policy or otherwise undertake inherently governmental functions.

Exemption from Public Law 92-463: In recognition of the highly-sensitive, and often confidential, nature of the subject matter involved in the activities of the CIPAC, under the authority of section 871 of the Homeland Security Act of 2002 (6 U.S.C. 451), **the Secretary has decided to exempt the CIPAC from the requirements of Public Law 92-463 (5 U.S.C. App. 1 et seq.).** The decision to exercise the exemption authority in section 871 will improve the homeland security partnership between government and the private sector. **This exemption will support the free flow of information as those**

involved in protecting our critical infrastructure strive to meet the need for regular, interactive discussions concerning threats and vulnerabilities.

DHS recognizes and supports, however, the important principle of transparency as a foundation for public confidence in government. Accordingly, to the full extent compatible with the achievement of the critical infrastructure protection mission, DHS will, as a matter of policy, operate the CIPAC in a manner consistent with the spirit of this principle. DHS will maintain the CIPAC Executive Secretariat, which will manage and coordinate the activities of the CIPAC and maintain its records. While many meetings of the CIPAC will be closed to the public, meetings will be open as feasibly consistent with security objectives. Unless exigent circumstances arise, the CIPAC Executive Secretariat will provide public notice of when scheduled meetings of the CIPAC are expected to be held. Among its other responsibilities, the CIPAC Executive Secretariat will also develop and maintain on an ongoing basis a publicly-accessible Web site. The CIPAC Executive Secretariat will also prepare and, to the extent consistent with security objectives, publish on the Web site copies of meeting agendas and periodic reports on the CIPAC's accomplishments. The Executive Secretariat will also maintain the membership list for the CIPAC. DHS will support the administrative needs of the CIPAC through the CIPAC Executive Secretariat.

Membership and Structure: The CIPAC will be representative of the following CI/KR sectors identified in HSPD-7:

- Food and Agriculture
- Banking and Finance
- Chemical
- Commercial Facilities
- Defense Industrial Base
- Drinking Water and Waste Water
- Dams
- Emergency Services
- Energy
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation Systems

The specific membership of the CIPAC will consist of: (a) The CI/KR owners and operators that are members of their respective sector's recognized Sector Coordinating Council (SCC), including their representative trade or equivalent organizations ["SCC CIPAC Members"]; and (b) Federal, State, local, and tribal governmental entities comprising the members of the Government Coordinating Council (GCC) for each sector, including their representative trade or equivalent organizations ["GCC CIPAC Members"].

CI/KR owners and operators are those entities that own and invest in infrastructure assets, in the systems and processes to secure them, and that are held responsible by the public for their operations and the response and their recovery when their infrastructures or key resources are disrupted.

SCCs are independent, self-governed bodies organized (or presently being organized) by the owners and operators of the nation's CI/KR within each of the critical sectors identified in HSPD-7 to enable them to coordinate among themselves on sector initiatives on critical infrastructure protection, including response and recovery. The SCCs are broadly representative of the owners and operators within each CI/KR sector. While these councils are independent of government, they provide the CIPAC the ability to draw as representational a membership as possible from each sector and from across all sectors.

GCCs are interagency coordinating bodies that enable interagency and cross-jurisdictional coordination within each HSPD-7 sector. Each GCC is comprised of representatives from across various levels of government (*i.e.*, Federal, State, local, and tribal), as appropriate to the security landscape of each sector, and includes the Federal departments and agencies with a relevant interest in the sector. Each GCC is co-chaired by a representative from the designated SSA for the sector and by DHS' Assistant Secretary for Infrastructure Protection.

Appendix A sets forth a list of the present membership of the CIPAC from each sector as of this date, including all of the GCC CIPAC Members and the designated leadership of each SCC now in existence. Immediately following publication of this Notice in the **Federal Register**, the CIPAC Executive Secretariat will work with each SCC's leadership, and the SSA for each sector, to compile a complete list of the CIPAC SCC Members from each sector. Not later than April 24, 2006, the Department will publish a subsequent Notice identifying these additional members of the CIPAC. As new SCCs are formed and existing ones mature, the membership of the CIPAC will grow and change to accommodate changes in the membership of these bodies. DHS will publish quarterly updates in the **Federal Register** to announce changes in the membership of the CIPAC.

Membership Status: Non-Federal members of the CIPAC serve as representatives of their sectors, not as special government employees. Private sector members bear the cost of participating in the CIPAC.

Meetings: **The CIPAC may meet as a whole or in any combination of subgroups that is most conducive to the effective conduct of its activities including, without limitation, in groups encompassing discrete sectors to address sector-specific issues and concerns** (*e.g.*, a meeting of the members of the Food and Agriculture Sector GCC with their counterpart owners and operators from the sector's SCC), or in a small group with a single designated representative from each sector to address interdependencies and other cross-sectoral issues. **As independent bodies, meetings consisting solely of members of the SCCs, or those consisting solely of members of the GCCs, shall not constitute meetings of the CIPAC.** In addition, the CIPAC may establish informal working groups for the purpose of fact-finding, issue development, or other preliminary

non-deliberative activities. **Such activities in support of the CIPAC shall also be within the scope of the exemption noted above.**

The CIPAC will meet at least quarterly to address matters within the scope of this Charter. The CIPAC Executive Secretariat will prepare summary minutes of CIPAC meetings; maintain calendars and agendas; coordinate preparation and review of communications with government entities; extend invitations to government officials and other expert consultants, as needed, to attend meetings; and other administrative functions as may be required.

Duration of Committee: Two years, subject to extension pursuant to section 871(b) of the Homeland Security Act of 2002 (6 U.S.C. 451(b)).

Responsible DHS Official: Nancy J. Wong, Director, Infrastructure Programs Office, Infrastructure Partnerships Division, United States Department of Homeland Security, Washington, DC 20528, telephone (703) 235-5349.

Dated: March 20, 2006.

Michael Chertoff,
Secretary.

Appendix A—Membership of the Critical Infrastructure Partnership Advisory Council

Leadership of Existing SCCs:

Association of American Railroads
Cellular Telecommunications & Internet Association
Computer Sciences Corporation
Constellation Generation Group
Depository Trust and Clearing Corp.
Duke Energy
DuPont
Exelon Corporation
FedEx Corporation
Greenville Water System
Independent Electricity System Operator, Ontario, Canada
International Association of Fire Chiefs
International Dairy Foods Association
Madden & Patton, LLC
National Cattleman's Beef Association
National Food Processors Association
New Jersey Transit
New York City Department of Environmental Protection
NiSource Pipelines
Northwestern Hospital
Pacific Gas and Electric Co.
The Real Estate Roundtable
Telecommunications Industry Association
U.S. Telecom Association
United States Postal Service

Valero Energy Corporation
VeriSign
Xcel Energy

Federal, State, local, tribal and quasi-governmental entities, or their designated representative trade or equivalent associations, identified as members of existing GCCs:

American Red Cross

Association of Food and Drug Officials

North American Securities Administration Association

Association of State and Interstate Water Pollution Control Administrators

Association of State and Territorial Health Officials

Association of State Drinking Water Administrators

Commodity Futures Trading Commission

Conference of State Bank Supervisors

Farm Credit Administration

Federal Communications Commission

Federal Deposit Insurance Corporation

Federal Energy Regulatory Commission

Federal Housing Finance Board

Federal Reserve Bank of New York

Federal Reserve Board

Interagency Security Committee

Intertribal Agriculture Council

National Association of County and City Health Officials

National Association of Departments of Agriculture

National Association of State Chief Information Officers

National Association of State Credit Union Supervisors

National Credit Union Administration

Nuclear Regulatory Commission

Securities Investor Protection Corporation

Tennessee Valley Authority

United States Army Corps of Engineers

United States Department of Agriculture

United States Department of Commerce

United States Department of Defense

United States Department of Education

United States Department of Energy

United States Department of Health and Human Services

United States Department of Homeland Security

United States Department of Housing and Urban Development

United States Department of Interior

United States Department of Justice

United States Department of Labor

United States Department of Transportation

United States Department of the Treasury

United States Environmental Protection Agency

United States National Archives and Records Administration

United States Securities and Exchange Commission
[FR Doc. 06-2892 Filed 3-23-06; 8:45 am]
BILLING CODE 4410-10-P