GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

December 8, 2003

The Honorable Dave Camp
Chairman, Subcommittee on Infrastructure and
Border Security
Select Committee on Homeland Security
House of Representatives

The Honorable Mac Thornberry
Chairman, Subcommittee on Cybersecurity,
Science, and Research and Development
Select Committee on Homeland Security
House of Representatives

Subject: *Posthearing Questions from the September 17, 2003, Hearing on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness"*

As requested in your letter of November 5, 2003, this letter provides our responses for the record to the questions you posed to GAO. At the subject hearing, we discussed the challenges that the Department of Homeland Security (DHS) faces in integrating its information gathering and sharing functions, particularly as they relate to fulfilling the department's responsibilities for critical infrastructure protection (CIP).

> *GAO released a report on information sharing in August of this year. It found that "no level of government perceived the [information sharing] process as effective, particularly when sharing information with federal agencies." How does [this] finding relate to what happened during the August 2003 blackout?*

In our August 2003 report on information sharing, we identified initiatives that had been undertaken to improve the sharing of information to prevent terrorist attacks and surveyed federal, state, and city government officials to obtain their perceptions on how the current information-sharing process was working.[1] Our survey showed that none of the three levels of government perceived the current information-sharing process to be effective when it involved the sharing of information with federal agencies. Specifically, respondents reported that information on threats, methods,

[1]U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: Aug. 27, 2003).

and techniques of terrorists was not routinely shared, and the information that was shared was not perceived as timely, accurate, or relevant. Further, 30 of 40 states and 212 of 228 cities responded that they were not given the opportunity to participate in national policy making on information sharing. Federal agencies in our survey also identified several barriers to sharing threat information with state and city governments, including the inability of state and city officials to secure and protect classified information, their lack of federal security clearances, and a lack of integrated databases. Further, this report identified some notable information-sharing initiatives. For example, the Federal Bureau of Investigation (FBI) reported that it had significantly increased the number of its Joint Terrorism Task Forces and, according to our survey, 34 of 40 states and 160 of 228 cities stated that they participated in information-sharing centers.

Performed primarily before DHS began its operations and not focused on the federal government's CIP efforts, this report did not specifically relate to the impact of these information-sharing challenges on any specific events, including the August 2003 blackout. However, as indicated in our written statement for the September 17 hearing,[2] our past information-sharing reports and testimonies have identified information sharing challenges and highlighted its importance to developing comprehensive and practical approaches to defending against potential cyber and other attacks, as well as to DHS meeting its mission.

> *A June 2003 GAO report on federal collection of electricity information found significant gaps in collection for information needed by different federal agencies. The report does not mention DHS. In light of the Department's responsibilities with respect to the electrical component of critical infrastructure, what can you say about the kinds of information it needs, and whether it has the ability to obtain that information?*

With the ongoing transition (or restructuring) of electricity markets from regulated monopolies to competitive markets, accurate information on electricity trading and pricing is becoming more critical not only for evaluating the potential benefits and risks of restructuring, but also for monitoring market performance and enforcing market rules. Our June 2003 report focused on describing the information that is collected, used, and shared by key federal agencies—such as the Federal Energy Regulatory Commission and the Energy Information Administration within the Department of Energy—and the effect of restructuring on these agencies' collection, use, and sharing of this information.[3] In the aftermath of electricity price spikes and other efforts to manipulate electricity markets in California, our work focused on the oversight of restructured electricity markets—not the physical security of the system's components. With this focus, we did not include DHS in the scope of our work.

---

[2]U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: Sep. 17, 2003).
[3]U.S. General Accounting Office, *Electricity Restructuring: Action Needed to Address Emerging Gaps in Federal Information Collection*, GAO-03-586 (Washington, D.C.: Jun. 30, 2003).

However, we have made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area concerns the federal government's CIP efforts, which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made, further efforts are needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;

- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;

- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and

- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.

Regarding the kinds of information that DHS needs, the Homeland Security Act and other federal strategies acknowledge the importance of information sharing and identify multiple responsibilities for DHS to share information on threats and vulnerabilities for all CIP sectors. In particular:

- The Homeland Security Act authorizes DHS's Under Secretary for Information Assurance and Infrastructure Protection to have access to all information in the federal government that concerns infrastructure or other vulnerabilities of the United States to terrorism and to use this information to fulfill its responsibilities to provide appropriate analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis management support in response to threats or attacks on critical information systems, and technical assistance upon request to private-sector and government entities to respond to major failures of critical information systems.

- The *National Strategy to Secure Cyberspace* encourages DHS to work with the National Infrastructure Advisory Council and the private sector to develop an optimal approach and mechanism to disclose vulnerabilities in order to expedite the development of solutions without creating opportunities for exploitation by hackers.[4] DHS is also expected to raise awareness about removing obstacles to

[4]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

sharing information concerning cybersecurity and infrastructure vulnerabilities between the public and private sectors and is encouraged to work closely with private-sector information sharing and analysis centers (ISACs) to ensure that they receive timely and actionable threat and vulnerability data and to coordinate voluntary contingency planning efforts.

- The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* describes DHS's need to collaborate with the intelligence community and the Department of Justice to develop comprehensive threat collection, assessment, and dissemination processes that are distributed to the appropriate entity in a timely manner.[5] It also enumerates several initiatives directed to DHS to create a more effective information-sharing environment among the key stakeholders, including establishing requirements for sharing information; supporting state and local participation with ISACs to more effectively communicate threat and vulnerability information; protecting secure and proprietary information that is deemed sensitive by the private sector; implementing processes for collecting, analyzing, and disseminating threat data to integrate information from all sources; and developing interoperable systems to share sensitive information among government entities to facilitate meaningful information exchange.

Other efforts may help to identify specific information needs for the critical infrastructure sectors, including the electric power sector. For example, we are currently beginning work to determine the status of the ISACs in undertaking the voluntary activities suggested by federal CIP policy to gather, analyze, and disseminate information to and from infrastructure sectors and the federal government. In addition, according to the chairman of the recently established ISAC Council, the mission of the council is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for interaction between and among the ISACs. Council activities include establishing and maintaining a policy for inter-ISAC coordination, a dialog with governmental agencies that deal with ISACs, and a practical data and information sharing protocol (what to share and how to share).

Finally, as we discuss in more detail in the response to the next question, Congress and the administration have taken steps to help improve information sharing. These include the incorporation of provisions in the Homeland Security Act of 2002 to restrict the use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. However, the effectiveness of such steps may largely depend on how DHS implements its information sharing responsibilities and the willingness of the private sector and state and local governments to share such information. It may also require the consideration of various public policy tools, such as grants, regulations, or tax incentives.

---

[5]The White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003).

The creation of "Critical Infrastructure Information" provides companies with a mechanism to voluntarily give this information to the federal government. Do you think that private companies will avail themselves of this opportunity? Do you think that Critical Infrastructure Information protections are sufficient? What other incentives might the federal government use to obtain this information for homeland security purposes? Should the federal government require the submission of this information so as to inform the Department of Homeland Security of potential cross-sectoral weaknesses and vulnerabilities?

The Homeland Security Act of 2002 includes provisions that restrict federal, state, and local governments' use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. These restrictions include exemption from disclosure under the Freedom of Information Act, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee who improperly discloses any protected critical infrastructure information. In April 2003, DHS issued for comment its proposed rules for how critical infrastructure information volunteered by the public will be protected. At this time, it is too early to tell what impact the act will have on the willingness of the private sector to share critical infrastructure information or whether the protections that these provisions provide are sufficient.

Regarding other incentives that the federal government might use and the need to require submission of critical infrastructure information, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP.[6] However, the strategy also discusses the need to use all available public policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets. The *National Strategy to Secure Cyberspace* also states that the market is to provide the major impetus to improve cybersecurity and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on the need for strong partnerships with those outside the federal government and stated that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.[7] We have also previously testified on the choice and design of public policy tools that are available to governments.[8] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address

---

[6]The White House, *National Strategy for Homeland Security* (Washington, D.C.: July 2002).
[7]U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success*, GAO-01-886T (Washington, D.C.: June 25, 2002).
[8]U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO-02-549T (Washington, D.C.: Mar. 28, 2002).

security concerns. Some of these tools are already being used, for example, in the water and chemical sectors.

Without appropriate consideration of public policy tools, private-sector participation in sector-related information sharing and other CIP efforts may not reach its full potential. For example, we reported in January 2003 on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sector-wide efforts.[9] We also reported on the efforts of federal entities and regulators to partner with the financial services industry to protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the public policy tools that potentially could encourage the financial services sector to implement information sharing and other CIP-related efforts. Because of the importance of considering public policy tools to encourage private-sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress that five ISACs (including the Electricity ISAC) had made in accomplishing the activities suggested by Presidential Decision Directive (PDD) 63.[10] We recommended that the responsible lead agencies assess the need for public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government.

> *In the absence of a comprehensive critical-infrastructure risk assessment from the DHS, can you let the committee know, in your opinion, which of the critical infrastructure sectors pose the greatest national security concern? Rank—in relative order starting with the highest concern—the top five critical infrastructure sectors that you believe pose the greatest risk. Briefly discuss the reasons for your selections and rankings. In each of the sectors you describe, what has the private sector done since 9/11 to increase protection? What key initiatives have the Administration and the DHS pursued to improve protection and since when?*

Much of our work on federal CIP has focused on cybersecurity and the overall threats and risks to critical infrastructure sectors. This work did not include assessments of specific sectors that would enable us to identify or rank which of the sectors pose the greatest national security concern or greatest risk. We believe that all the critical infrastructures are important in that, as defined by the USA PATRIOT Act and highlighted in the *National Strategy for Homeland Security*, they represent "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Further, determining which sectors pose the greatest

---

[9]U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, DC,: Jan. 30, 2003).
[10]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

risk would require not only an assessment of individual sector security, but also consideration of the interdependencies among sectors. For example, assuring electric service requires operational transportation and distribution systems to guarantee the delivery of the fuel that is necessary to generate power. Also, the devices that control our physical systems, including our electrical distribution system, transportation systems, dams, and other important infrastructures, are increasingly connected to the Internet. Thus, the consequences of an attack on our cyber infrastructure could cascade across many sectors.

The administration has taken a number of steps to improve the protection of our nation's critical infrastructures, including issuance of the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Called for by the *National Strategy for Homeland Security*, these two strategies identify priorities, actions, and responsibilities for the federal government, including lead agencies and DHS, as well as for state and local governments and the private sector. However, we have not undertaken an in-depth assessment of DHS's cyber CIP efforts that could enable us to describe what DHS or the private sector have done to improve protection.

In past testimony and reports, the General Accounting Office (GAO) has identified a number of significant CIP challenges, including:

i) Clear delineation of CIP roles and responsibilities for federal, state, local, and private sector actors; clarification of how CIP entities will coordinate their activities
ii) Clear definition of interim objectives and milestones
iii) Clear timeframes for achieving objectives
iv) Establishment of performance metrics
v) Improvement in analytical and warning capabilities

Please provide a detailed list of what significant interim objectives and milestones the DHS Infrastructure Protection Office has in place to improve critical infrastructure protection. What firm timeframes does the Office of IP have in place for these objectives? What performance metrics does the Office of IP have in place to measure its progress against objectives, milestones, and timeframes?

We have made numerous recommendations over the last several years related to information-sharing functions that have now been transferred to DHS, including those related to the federal government's CIP efforts. As you indicate, among the challenges we have identified is the need for a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures. We also identified the need to improve the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector. The Homeland Security Act of 2002 makes

DHS and its Information Assurance and Infrastructure Protection directorate responsible for key CIP functions for the federal government, including developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States.

The *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* issued in February 2003 by the President identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and DHS, as well as for state and local governments and the private sector. Both define strategic objectives for protecting our nation's critical assets. The cyberspace security strategy provides a framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace. The physical protection strategy discusses the goals and objectives for protecting our nation's critical infrastructure and key assets from physical attack. However, as we have previously testified, neither of the strategies (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; or (4) establishes performance measures for which entities can be held responsible.

We have not undertaken an in-depth review of the department's cyber CIP efforts, which would include an assessment of its progress in developing a comprehensive national plan that addresses identified CIP challenges and the development of analysis and warning capabilities.

> *How is the DHS Office of IP organized to coordinate with private sector Information Sharing and Analysis Centers (ISACs)? Are the ISACs the best organizations to lead sector-based industry efforts to share critical infrastructure information? What role do you see for the ISACs going forward? Is the federal government doing enough to support ISAC efforts? Do you see [a] role for federal funding of ISACs?*

According to an official in the Infrastructure Protection Office's Infrastructure Coordination Division, this division is responsible for building relationships with the ISACs and is currently working with them and the sector coordinators (private sector counterparts to federal sector liaisons) to determine how best to establish these relationships. In addition, this official said that DHS's interagency Homeland Security Operations Center provides the day-to-day operational relationship with the ISACs to share threat and warning information.

As mentioned previously, we are currently beginning work that will focus on the status of ISAC efforts to implement the activities suggested by federal CIP policy. This work should provide more information about obstacles to greater information sharing, the role of the ISACs in sharing critical infrastructure information, and the assistance provided to these organizations by DHS and other federal lead agencies. Such federal assistance could include funding, such as the examples of ISAC funding

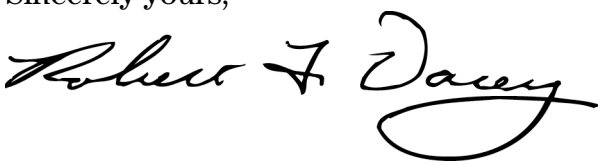
that we discussed in our February 2003 report.[11] Specifically, the Energy ISAC reported that in the fall of 2002, the Office of Energy Assurance (then within the Department of Energy and now transferred to DHS) had agreed to fund ISAC operations—an agreement sought so that membership costs would not prevent smaller companies from joining. The new, cost-free Energy ISAC began operations and broad industry solicitation for membership in February 2003. Further, for the Water ISAC, the Environmental Protection Agency provided a grant for system development and expanded operations.

> *This month, the American Society of Civil Engineers (ASCE) released a Progress Report on its 2001 Report Card on America's Infrastructures. In this report, the ASCE examined current status and trends in the nation's deteriorating infrastructure. In their assessment, the Energy infrastructure received a D+. Roads and bridges received a D+/C. Does the poor state of a number of our infrastructure sectors have serious negative implications for the security of those sectors against potential terrorist attack? What is the relationship between reliability and security when it comes to critical infrastructure protection?*

The ASCE's 2003 progress report on its 2001 report card does not discuss the implications of deteriorating infrastructure conditions and security against potential terrorist attack.[12] Further, GAO has not specifically assessed whether the poor state of infrastructure sectors may have serious negative implications for security against potential terrorist attack. However, the relationship between reliability and security may be an appropriate consideration as DHS and the critical infrastructure sectors identified in federal CIP policy continue their efforts to assess the vulnerabilities of these sectors to cyber or physical attacks.

We are sending copies of this letter to DHS and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-3317. I can also be reached by e-mail at *daceyr@gao.gov*.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

(310517)

---

[11] GAO-03-233.
[12] American Society of Civil Engineers, *2003 Progress Report: An Update to the 2001 Report Card*, September 2003.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548