United States General Accounting Office

GAO

Report to Senator Robert F. Bennett, Ranking Minority Member, Joint Economic Committee, Congress of the United States

October 2001

INFORMATION SHARING

Practices That Can Benefit Critical Infrastructure Protection

GAO-02-24

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
00OCT2001	N/A	-

Title and Subtitle INFORMATION SHARING: Practices That Can Benefit Critical Infrastructure	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) U.S. General Accounting Office P.O. Box 37050 Washington, D.C. 20013	**Performing Organization Report Number** GAO-02-24
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
This report responds to your May 2001 request that we study the practices of organizations that successfully share sensitive or time-critical information. Information sharing and coordination are key elements in developing comprehensive and practical approaches to defending against computer-based, or cyber, attacks, which could threaten the national welfare. Such attacks could severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. Computer-based incidents, such as the ILOVEYOU virus in May 2000 and the recent Code Red, SirCam, and Nimda attacks, have caused significant disruptions and damage.1 In addition, the terrorist attacks of September 11 illustrate the importance of having timely information from others on threats and possible precursors to an attack.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR

Number of Pages
39

Contents

Letter

Appendixes

Figures

Abbreviations

CDC	Centers for Disease Control and Prevention
CERT/CC	CERT® Coordination Center
FBI	Federal Bureau of Investigation
FedCIRC	Federal Computer Incident Response Center
ISAC	information sharing and analysis center
JTF-CNO	Joint Task Force—Computer Network Operations
NCC	National Coordinating Center for Telecommunications
NERC	North American Electric Reliability Council
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
PDD 63	Presidential Decision Directive 63

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

October 15, 2001

The Honorable Robert F. Bennett
Ranking Minority Member
Joint Economic Committee
Congress of the United States

Dear Senator Bennett:

This report responds to your May 2001 request that we study the practices of organizations that successfully share sensitive or time-critical information. Information sharing and coordination are key elements in developing comprehensive and practical approaches to defending against computer-based, or cyber, attacks, which could threaten the national welfare. Such attacks could severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. Computer-based incidents, such as the ILOVEYOU virus in May 2000 and the recent Code Red, SirCam, and Nimda attacks, have caused significant disruptions and damage.[1] In addition, the terrorist attacks of September 11 illustrate the importance of having timely information from others on threats and possible precursors to an attack.

The importance of sharing information and coordinating the response to cyber threats among various stakeholders has increased as our government and our nation have become ever more reliant on interconnected computer systems to support critical operations and infrastructures, such as telecommunications, power distribution, financial services, national defense, and critical government operations. Information on threats and incidents experienced by others can help stakeholders identify trends, better understand the risks they face, and determine what preventative measures should be implemented. Accordingly, the federal government's strategy for protecting the nation's critical computer-dependent infrastructure sectors includes efforts to establish information sharing and analysis centers (ISACs) within both the federal government and individual industry sectors. Such analysis centers can use comprehensive, timely information on incidents to determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack.

[1] *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* (GAO-01-1073T, August 29, 2001).

To identify practices that could be adopted by federal agencies and others to (1) promote successful sharing of information on computer-based vulnerabilities and incidents and (2) overcome related challenges, we studied 11 organizations experienced in developing pertinent information-sharing relationships and procedures. Appendix I contains a description of our objectives, the scope of our study, and the methodology we used. Appendix II describes each organization covered by our review.

Results in Brief

The organizations identified a number of factors that they deemed critical to their success in building successful information-sharing relationships with and among their members. All of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships. Other critical success factors identified included (1) establishing effective and appropriately secure communication mechanisms, such as regular meetings and secure Web sites, (2) obtaining the support of senior managers at member organizations regarding the sharing of potentially sensitive member information and the commitment of resources, and (3) ensuring organization leadership continuity. In addition, to be successful, information-sharing organizations provided identifiable membership benefits, such as current information about threats, vulnerabilities, and incidents; information on lessons learned; and free member advice. Without such benefits, according to the representatives we met with, members would not continue participating.

Among the challenges identified, one of the most difficult was overcoming new members' initial reluctance to share information. Other challenges included (1) developing agreements on the use and protection of shared information, (2) obtaining adequate funding to cover the cost of items such as Web sites and meetings while avoiding seeking contributions intended primarily to promote the interests of an individual organization, (3) maintaining a focus on emerging issues of interest to members, and (4) maintaining professional and administrative staff with appropriate skills.

The critical success factors and challenges described by the organizations provide useful insights for other entities that are developing information-sharing relationships to assist in critical infrastructure protection. In addition, as it did regarding the Year 2000 computing challenge, the Congress can play a key role by actively monitoring progress in meeting critical infrastructure protection goals, including improved information

sharing, and by assisting in clarifying the way federal agencies may use sensitive information provided for critical infrastructure protection purposes. In 1998, Congress passed legislation intended to address concerns from private-sector entities about exposure to legal liability and antitrust law violations that might arise due to sharing information on Year 2000 readiness. The Congress is currently considering measures intended to address several of the practices and challenges we identified pertaining to critical infrastructure protection.

In commenting on a draft of this report, the participants of our study agreed with the critical success factors and challenges that we identified. Several provided additional supporting points and examples, which we have included in the report as appropriate.

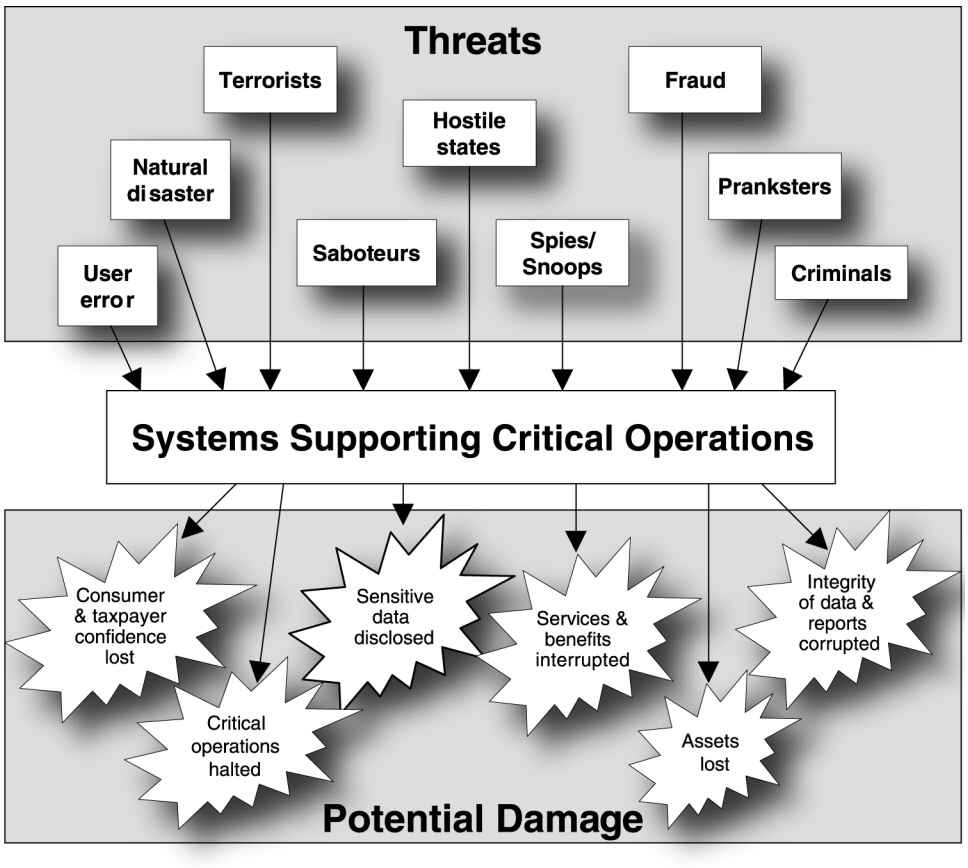
Background

Over the last decade, our government and our nation have become increasingly reliant on computer systems to support critical operations and infrastructures, such as telecommunications, power distribution, financial services, emergency services, national defense, and critical government operations. Over the same period, computer interconnectivity experienced an unprecedented growth, most notably in the use of the Internet, that has revolutionized the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous in terms of facilitating communications, business processes, and access to information. However, without proper safeguards, this widespread interconnectivity poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support.

Attacks could severely disrupt computer-supported operations, compromise the confidentiality of sensitive information, and diminish the integrity of critical data. A significant concern is that terrorists or hostile foreign states could severely damage or disrupt critical operations, resulting in harm to the public welfare. Threats are increasing, in part, because the number of individuals with computer skills is increasing and because intrusion, or "hacking," techniques have become readily accessible through magazines, computer bulletin boards, and Internet Web sites. However, the sources of and motives behind cyber attacks often cannot be readily determined. This is because groups or individuals can attack remotely from anywhere in the world, over the Internet, other networks, or dial-up lines, and they can disguise their identity, location, and intent by launching attacks across a span of communications systems and

computers. Figure 1 provides an overview of the various types of risks to computer-based operations.

Figure 1: Risks to Computer-Based Operations



The federal government has recognized that mitigating risks to our nation's critical computer-dependent infrastructures, many of which are privately owned, is a serious challenge requiring coordination and cooperation among federal agencies, public and private-sector entities, and other nations. In 1991, the National Research Council studied the issue and reported that "as computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems."[2] In July 1996, the President's Commission on Critical Infrastructure Protection was established to investigate the nation's vulnerability to both cyber and physical threats. The commission's October 1997 report, *Critical Foundations: Protecting America's Infrastructures*, described the potentially devastating implications of poor information security from a national perspective.

In May 1998, in response to the commission's 1997 report, the President issued Presidential Decision Directive (PDD) 63, which outlined a strategy for combating the threat of cyber attacks by terrorists, nation states, criminals, or others. The directive tasked federal agencies with developing critical infrastructure protection plans.

In addition, PDD 63 recognized the importance of establishing mechanisms for sharing information on system vulnerabilities, threats, intrusions, and anomalies so that both government and industry could better prepare to warn and defend against computer-based attacks. Specifically, it designated "lead agencies" within the federal government to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. The eight infrastructures identified were (1) information and communications; (2) banking and finance; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. The five special function areas were (1) law enforcement and internal security, (2) intelligence, (3) foreign affairs, (4) national defense, and (5) research and development. The directive also encouraged the creation of ISACs that could serve as mechanisms for gathering, analyzing, appropriately sanitizing, and disseminating information to and from infrastructure

[2]*Computers at Risk: Safe Computing in the Information Age*, the National Research Council, 1991.

sectors and the government. Further, it recognized the Federal Bureau of Investigation's National Infrastructure Protection Center as a national threat assessment, warning, vulnerability, and law enforcement investigation and response center.

Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating computer-based threats. Having information on threats and on actual incidents experienced by others can help an organization identify trends, better understand the risks it faces, and determine what preventative measures should be implemented. In addition, comprehensive, timely information on incidents can help federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack.

However, we previously reported that progress in implementing PDD 63, including the establishment of information-sharing relationships, has been slow. Although six ISACs in five industry sectors had been established as of March 2001, three had been in existence only since December 2000.[3] Further, as we reported in April 2001, the National Infrastructure Protection Center had mixed success in establishing information-sharing relationships with other government entities and private industry.[4]

Despite this limited progress, a number of government and private organizations have gained experience in establishing information-sharing relationships. These organizations range from groups that disseminate information on immediate threats and vulnerabilities, to those that seek to facilitate information sharing between public and private entities on industry-specific threats, to those that promote coordination across infrastructure sectors and on an international scale. However, developing the information-sharing and coordination capabilities that could assist in effectively addressing computer-based threats and actual incidents has proven to be challenging as organizations grapple with ways to ensure that useful and complete data are collected; appropriately analyzed; protected from inappropriate disclosure; and efficiently and effectively disseminated, often in the form of warnings.

[3]*Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

[4]*Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

Factors Critical to Successful Information Sharing

The organizations identified several critical success factors that they viewed as essential to establishing, developing, and maintaining effective information-sharing relationships, which could benefit critical infrastructure protection efforts. These factors included (1) fostering trust and respect; (2) establishing effective, timely, and appropriately secure communication; (3) obtaining top management support; (4) ensuring organization leadership continuity; and (5) generating clearly identifiable membership benefits.

Foster Trust and Respect

An underlying element to the success of information-sharing organizations was developing trusted relationships among the members and the organizations' staffs. Several of the organizations had professional and administrative staffs that provided analytical capabilities and facilitated their members' participation in the organization's activities. Others were less formally structured organizations that relied primarily on members for such support. Trust was critical to overcome members' reluctance to disclose their weaknesses, vulnerabilities, and other confidential or proprietary business information to other members—some of whom were business competitors. In general, members were reluctant to share information due to concerns that an inadvertent release of this type of information could damage reputations; lower customer confidence; provide an advantage to competitors; and possibly negatively affect members' businesses and lead to punitive measures against an individual member or a member organization.

All of the organizations agreed that trust had to be built over time and through personal relationships, and they had taken various steps to facilitate the process, such as the following:

- Most held regular—bimonthly, quarterly, or annual—meetings or forums to discuss issues and establish face-to-face contact. Beyond the time used to discuss technical issues, these meetings included time for members to build personal relationships and contacts. Many of the organizations and the members stated that the personal relationships and contacts developed through participating in information-sharing organizations was as important, if not more important, in developing trust than the information received by attending an organization's function.

- Many organizations encouraged consistent member participation, noting that trust was built most effectively when members consistently attended and participated in the organizations' activities. Also important was for members to consistently send the same representatives and not rotate different people as representatives to the organizations' functions. To maintain consistency, some organizations did not allow alternate attendees when designated representatives could not attend.

- Most followed established procedures or performed background checks to evaluate prospective members before allowing their participation. For example, some organizations allowed nonmembers to participate only if the organization invited them or an existing member invited and escorted them. Another organization had an official board that reviewed membership applications to determine whether the applicant and the applicant's organization met established membership criteria. Also, groups that served specific audiences had established lists of pertinent organizations that were allowed to participate as members and receive information of specific interest to that group.

- Many attempted to establish an atmosphere of mutual respect among the members so that each member's issues and expertise merited consideration regardless of the company they represented or the individual representative's position in that company. Often, each member was required to share information or, in some cases, time was set aside to give each member an opportunity to raise issues for discussion. In addition, many organizations encouraged members to subordinate individual or individual organizations' interests to the interests of the entire information-sharing group. For example, one organization had simple rules of behavior. Members were to support one another in improving the security posture of each other's organization without regard for their own self-promotion or for the profit or publicity of their individual organization.

- All had established procedures for handling violations of the rules because any violation of trust undermined the organization's purpose and diminished members' willingness to share in the future. The organizations had both formal and informal means of encouraging compliance and sanctioning violators. In some cases, members were formally asked to terminate their participation, a member's access was terminated, or a member's organization was asked to replace its representative. For example, one organization would restrict access to a secure server, thereby terminating the individual's ability to share or

receive information. Informally, other members would no longer include a violator in sensitive conversations. One participant emphasized that once the group lost trust in a member, trust could not be easily restored. Our study participants said that their organizations rarely experienced a violation of trust because members did not want to jeopardize their ability to participate and, thus, lose the benefits of membership.

Establish Mechanisms For Effective, Timely, and Appropriately Secure Communication

The organizations used a variety of mechanisms to ensure effective and timely communication among members and with the professional and administrative staffs that some of the organizations had established. In addition, the organizations were concerned about appropriately securing the information being shared to maintain member anonymity, when desired, and avoid inappropriately disseminating sensitive or proprietary information to nonmembers.

Regularly scheduled meetings were the primary method for sharing information as well as a method for building trust, as previously discussed. These meetings offered a generally secure environment to share information, while also encouraging broader member participation. The organizations also adjusted the meeting times and lengths to accommodate member needs and attempted to enhance the meeting's efficiency and effectiveness by limiting the time for presentations, approving most topics and presentations before the meetings, and adjusting meeting times to maximize face-to-face discussions between members.

Typically, the meetings lasted 1/2 day to 2 days for the entire membership, and some meetings included separate sessions for smaller groups to discuss specific technical or member issues. For example, one organization had quarterly 2-day meetings, the first day of which was typically restricted to a small number of members with expertise pertinent to the specific topic under discussion. These closed meetings tended to be more technical than the open meetings and include information and discussions that were more sensitive and detailed. The second day's meeting, which was for all members of the organization, included discussions about the latest software tools and the latest technology and allowed time for any member to openly discuss specific topics. Another organization held more informal quarterly half-day meetings that included presentations about a wide variety of topics and allowed considerable time for members to develop personal contacts and have face-to-face discussions. Beyond the regularly scheduled meetings, three organizations had created committees to perform specific tasks, such as policy setting, that allowed for greater

contact between some members and more topic-based information sharing.

Various types of information technology provided important communication mechanisms as well. For example, Web sites were used to (1) disseminate all types of information, including alerts, advisories, reports, and other analysis; (2) make databases available to the members; and (3) provide methods for members to ask each other about particular incidents, vulnerabilities, or potential solutions. Many organizations had secure Web sites to share sensitive information; others used open sites to share general information with their members and the public. One organization established a secure telephone line that allowed immediate contact with multiple parties, thereby speeding communication of time-critical information. In addition, some organizations used e-mail to communicate less sensitive information to the entire membership. However, members from one organization did not typically use e-mail because of the lack of security and the inability to control subsequent distribution. This organization relied primarily on regular mail and telephone conversations to disseminate information about most things, including meeting agendas and real-time problem solving.

Due to concerns about the inadvertent release of sensitive information, membership lists, and victim identification, some of the organizations had implemented special security procedures. For example, several organizations carefully sanitized victim identifiers from documentation or did not document discussions about specific vulnerabilities and incidents. One organization took special precautions to hide the identity of victims by limiting its staff's access to the information and segregating the information on a special network. Another organization's membership list was maintained by only one person and never generally released to all members.

Several representatives stated that an underlying requirement for communications was establishing standard terms and reporting thresholds so that the magnitude of an incident could be easily and consistently understood and members could quickly determine an incident's potential impact on them. According to one official, such standardization helped to ensure that (1) members understood the level of risk imposed by the circumstance, (2) information was appropriately sanitized to protect the victim's identity, and (3) solutions were easily understood. One organization had developed an extensive policy that defined each member's responsibility for reporting information, the terms that would be used for

the reporting, and the thresholds that required reporting. Also, two organizations were developing reporting forms to standardize the mechanism and language used to report incidents to the organization for further analysis and dissemination.

In addition, organizations sought member input in developing new systems and mechanisms for communicating information, thereby better fulfilling member needs and giving the members a sense of ownership in the system or product. For example, one organization solicited suggestions about how to improve existing databases and what new databases were needed by the members.

Obtain Top Management Support

Members told us that senior management support for their participation in an information-sharing organization was critical to their success in obtaining valuable information and contributing to the success of the entire information-sharing organization. For example, management approval was needed before individuals could share information about potentially sensitive incidents and vulnerabilities. Without such support, members could not fully participate in the information-sharing process. Top management support was also needed to ensure that a member organization's representative could obtain funding for travel and other resources. For example, two organizations charged membership fees—one of which exceeded $25,000 a year—and other organizations requested people to provide support staff and analysts.

Ensure Leadership Continuity

Several organizations were led by individuals who had spent years building personal relationships with members and working to champion the purpose and mission of their organizations. In our discussions with members, these leaders were given considerable credit for the quality and value of the information that the members received and the success of the information-sharing organizations. These long-term leaders told us that, to help ensure continuity and diminish reliance on a single individual, they attempted to institutionalize their roles by bringing in additional people to assist in leading their organizations and performing such duties as enforcing membership rules and keeping current on issues and topics affecting their organization's members.

Generate Clearly Identifiable Membership Benefits

Organization representatives said that generating clearly identifiable benefits was essential for maintaining active member participation and support in their organizations. Many representatives told us that due to members' own resource and time constraints, members would not participate in information-sharing organizations unless they received benefits. Benefits the representatives cited included the following:

- Members were provided access to current information about incidents, threats, and vulnerabilities that had been analyzed by trusted experts. Some of the organizations performed expert analysis on incidents reported to them by members or the public and provided analyses and alerts to the members that included information on the incident's level of threat and any possible mitigation techniques. Another organization provided its members with a method for soliciting advice from the entire membership. In this case, a member would send a query to the organization's experts, who would review the request, clarify any questions with the member, and then send the request to the rest of the membership. While the rest of the membership reviewed and commented on the query, the organization's experts continued to analyze the problem, eventually providing its final analysis, which could include a threat rating and potential solutions to the entire membership. Some participants stated that the amount of analysis performed before informing the members had to be balanced with the need to quickly warn the members about the potential threat. Several participants stated that sharing information for the sake of sharing was not valuable because information security professionals need analyses that offer solutions.

- Members were informed about emerging technology so that they could discuss or at least be aware of possible vulnerabilities and the associated risks. These discussions were valuable to members because the information was useful in their employer's planning efforts. For example, several of the organizations had recently discussed, or were planning to discuss, the vulnerabilities surrounding the use of wireless networking technology.

- Members shared information concerning information security management practices, including corporate governance practices, business risk management processes, computing and network contract provisions, application development and support, disaster recovery planning, and performance measurement regarding control effectiveness.

- Members shared lessons learned and offered free expert advice on individual projects. The opportunity to draw on a network of experts gave members insight into their own problems and the shortfalls in proposed projects. For example, in many cases, one organization's members were willing to help each other by reviewing the requirement documentation for new systems development projects or system enhancement projects and participate in meetings to expose weaknesses and raise questions about a proposed project. According to one participant, his employer had received hundreds of thousands of dollars worth of free expert advice during a half-day discussion of a proposed information system that his employer was developing. The discussion led to the development of a better, more secure system. The sharing of free advice also occurred more informally.

- Members received real-time assistance in response to problems. For example, one member's entity experienced a sophisticated network intrusion that was originating from a foreign Internet service provider. Through the contacts made at one of the information-sharing organizations, the system administrator was able to contact the Internet service provider and stop the intrusion. According to an individual involved, this incident was stopped much faster than it otherwise would have been because of the trusted relationships developed through the information-sharing organization that allowed open and candid discussions to occur.

- Members established more cooperative relationships with law enforcement entities than would have otherwise occurred. Of 11 organizations, 2 were sponsored by law enforcement entities and most included members from the law enforcement community. Although law enforcement organizations could not share certain sensitive information, including them in the information-sharing groups led to trusted relationships between law enforcement organizations and the others; shared expertise about computer forensics and evidence gathering related to electronic crimes; and, thus, awareness about these topics, which encouraged organizations to report crimes. Representatives of one group told us that their members' ability to properly gather and protect computer-related evidence had facilitated law enforcement investigations, thus limiting the time and resources that the victim and the law enforcement officers needed to carry out an investigation. In addition, the trusted relationships provided law enforcement with a greater pool of experts to use as expert witnesses or consultants.

- Members developed valuable professional relationships through participation. Many members that participated in our study stated that their exposure to other experts and cutting-edge technology was a valuable learning experience that increased their own technical expertise. In addition, the large network of colleagues that members developed by participating assisted their employers in identifying potential professionals to fill open positions.

- Members told us that they believed that the information sharing their organizations engaged in contributed to the overall security of the nation's critical infrastructures—an effort that they viewed as being in their own self-interest, as well as that of others.

Challenges to Building and Maintaining Effective Information Sharing

In addition to the critical success factors previously discussed, organizations identified a number of related challenges to effective information sharing. These challenges included (1) initially establishing and maintaining trust relationships, (2) developing agreements on the use and protection of shared information, (3) obtaining adequate funding, (4) developing and retaining a membership base, and (5) developing and maintaining an organization staff with appropriate skills.

Initially Establishing and Maintaining Trust Relationships

All of the participating organizations told us that initially establishing trust among the original members was a challenge. This was because members were reluctant to share their organization's problems and vulnerabilities with outsiders, some of whom were commercial competitors. Members stated that the first meetings discussed broad subjects that individuals were concerned about or equally affected by, such as computer forensics.

In some cases, members initially participated because of an existing trust relationship with individual leaders or sponsors, and it was a challenge to keep them returning until they saw value in participating and had built trust with other members. In such situations, the persistence of trusted leaders in encouraging effective member participation was essential.

Over time, this challenge diminished as members became familiar with each other, enthusiastic members moved past general topics, and rules of behavior were clarified. In addition, over time, members began to better understand the perspectives of others. For example, discussions among members gradually led those from the private sector to gain an

understanding of the law enforcement community's approach to investigating crime. Further, some members from federal agencies said that it took time for them to determine how they could share sensitive, including classified, information with nonfederal government entities.

Another challenge, previously mentioned, was the need to institutionalize trust, rather than depend indefinitely on personal one-on-one relationships. Institutionalizing trust was especially important for large organizations and federal entities that typically experienced a great deal of staff turnover.

Developing Agreements on the Use and Protection of Shared Information

Information sharing is impeded when there is a lack of clearly understood agreements and expectations on how potentially sensitive information will be used and protected by the recipients. To overcome this obstacle, most of the organizations required members to sign confidentiality or information-sharing agreements. These agreements varied among the organizations: some agreements were general, while others were specific. Though many of the organizations did not consider these agreements to be essential, representatives of one organization considered them important because they clarified and helped to institutionalize agreements, ensured senior management understanding and support, and fostered acceptance of new members. For example, one organization determined that more formal agreements were needed when its membership was significantly expanded. The more formal agreements helped ensure that new members were familiar with the organization's practices, which had previously been informal and undocumented. These new agreements described how the sensitivity of information would be defined, how shared information would be protected from dissemination outside the group, and what information could be shared with nonmembers.

Noting that information-sharing agreements cannot cover every situation that may arise, one organization emphasized the importance of promoting an attitude of sensitivity to the concerns of others regarding disclosure of potentially confidential or damaging information. Officials from this organization described a situation in which a company had notified them of a newly identified vulnerability. Before disseminating information on the vulnerability to its constituent members, the information-sharing organization worked with the company to develop a message that would provide the needed vulnerability information but not disclose sensitive details. This collaborative effort helped ensure and maintain trust between the organization and the company.

Representatives of a few organizations said that members had raised concerns about their potential liability for any damage that occurred as a result of the information they shared and the advice they gave. Specifically, members were concerned that they might be held liable if other members took their advice and experienced negative results. Officials from one organization were also concerned that they might be held responsible if their advice adversely affected a vendor. To mitigate the risk of any such liability, some organizations addressed this issue specifically in their information-sharing agreements, stating that members who took the advice of others did so at their own risk. In addition, some members of federally sponsored organizations expressed the concern that members' potentially sensitive information voluntarily shared with federal entities could be required to be made publicly available under provisions of the Freedom of Information Act, despite existing exemptions for sensitive or proprietary information.

Obtaining Adequate Funding

The organizations also faced challenges obtaining adequate funding for various items, including mailings; meeting space; technological enhancements; and other administrative activities and, when applicable, salaries for permanent staff. They noted that the funding must be reliable so that the organization could plan, budget, and remain consistent in its activities. For example, one organization had to stop development of a secure Web site because the sponsor withdrew its support. Representatives from several organizations that relied on voluntary contributions from members emphasized, however, that such funding must be unbiased—that is, used for promoting open and honest information sharing rather than furthering an individual's or organization's stature in the community or for gaining clients.

Developing and Retaining the Membership Base

Most of the organizations said that they had to work to overcome the challenge of maintaining their memberships' enthusiasm and participation so that members would use the communication mechanisms, maintain confidentiality, and continue to share relevant information. In addition, organizations had to solicit new members to stay at their chartered number and to keep an influx of new ideas.

For the organizations that strictly controlled their membership or the number of members, developing and maintaining their membership base was a formidable challenge. For these organizations, the loss of members (e.g., due to the loss of the members' management support or difficult

economic times) threatened their survival. For one organization, this meant that the leaders had to continually establish contacts in their industry and determine which prospective companies would provide the most benefit to the entire group.

In addition, the organizations that focused on the information technology area faced the challenge of a very transient membership because information technology professionals often moved from organization to organization. When the individuals moved, the information-sharing organizations had to determine if they would be allowed to continue participating, which was usually based on the contributions and the enthusiasm of the individual. The organizations usually allowed individual members who had changed employers to continue participation. However, two organizations specifically did not allow individuals to continue participating if they changed employers and their new employer was not a member of the organizations because their membership was based on the organizations, not the individuals.

Developing and Maintaining Appropriate Analytical and Administrative Skills

Most of the organizations faced the challenge of developing and maintaining an organization with the appropriate operational skills to facilitate the members' participation and oversee administrative activities that ensured continued and effective information sharing. For example, the organizations that had professional and administrative staffs said that it was difficult to find and retain employees with the level of skills and foresight that would contribute to the organization's mission. Staff members were expected to assist members in participating in information sharing by arranging meetings and travel, maintaining the communications mechanisms, and keeping abreast of current and emerging issues. Further, to build trusted relationships and gain the acceptance of member organizations, staff needed to have pertinent skills and knowledge.

Because the job market was so competitive, one of the sponsoring organizations established flexible working arrangements for and gave competitive pay to their professional staff that supported its information-sharing organization. Another organization recruited staff from its industry who had relevant technical experience and understood the organization's role in the industry. In addition, one of the organizations used contractors to maintain its communications mechanisms and analyze reported incidents.

In addition, the representatives from organizations without professional and administrative staffs believed that an even more difficult challenge was encouraging volunteers to donate additional time to perform the administrative tasks required to organize meetings and further facilitate information sharing. In one organization, the leader had taken most of the responsibility for these tasks.

Information on Critical Success Factors and Challenges Can Benefit Critical Infrastructure Protection

Information sharing and coordination among organizations are important aspects of producing comprehensive and practical approaches to combating computer-based attacks. Information on threats and incidents experienced by others can help an organization identify trends, better understand the risks it faces, and determine what preventative measures should be implemented. In addition, comprehensive, timely information on incidents can help federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack.

The critical success factors and challenges described by organizations experienced in sharing sensitive and time-critical information and the lessons they have learned provide useful insights for other entities who are also trying to develop means of appropriately sharing information on computer-based vulnerabilities and the related risks. As the government's critical infrastructure protection strategy evolves, both public and private-sector entities can adopt the practices described to

- establish trusted relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- develop standards and agreements on how shared information will be used and protected;
- establish effective and appropriately secure communication mechanisms;
- take steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory changes;
- ensure that benefits are realized by developing and maintaining staff with the skills to support analytical capabilities and facilitate communication among information-sharing partners;

- obtain the support of senior officials in both federal and nonfederal entities; and

- obtain adequate funding.

The Congress can play a key role in facilitating the information-sharing aspect of critical infrastructure protection, as it did regarding the Year 2000 computing challenge. For example, the Congress can actively monitor progress in meeting critical infrastructure protection goals, including improved information sharing, and promote trust by assisting in clarifying the way federal agencies may use sensitive information provided for critical infrastructure protection purposes. Prior to 2000, the Congress held important hearings on Year 2000 readiness, and, in 1998, passed legislation intended to address concerns from private-sector entities about exposure to legal liability and antitrust law violations that might arise due to sharing information on Year 2000 readiness.

The Congress is currently considering measures intended to address several of the practices and challenges we identified. Two recently introduced bills, S. 1456 and H.R. 2435, include provisions that address the receipt, care, and storage of critical infrastructure protection information as well as specific exemptions from public disclosure of such information. Implementation of such provisions, as well as other monitoring actions, could facilitate information sharing and, thus, federal and private efforts to protect critical infrastructures.

Participants Comments

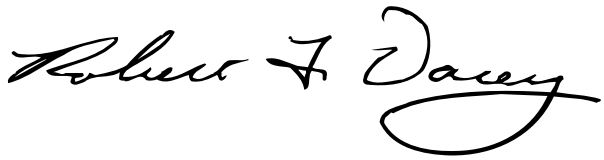
In commenting on a draft of this report, the participants of our study agreed with the critical success factors and challenges that we identified. Several provided additional supporting points and examples, which we have included in the report as appropriate.

As we agreed with your staff, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies to the Chairman, Vice Chairman, and Ranking Minority Member of the Joint Economic Committee. In addition, we are sending copies to other interested congressional committees. We are also sending copies to the heads of the lead agencies, including the Secretaries of Commerce, Defense, Energy, Health and Human Services, State, Transportation, and the Treasury and

the U.S. Attorney General; the Administrator, Environmental Protection Agency; the Director, Federal Emergency Management Agency; the Director, Federal Bureau of Investigation; the Director of Central Intelligence; the Assistant to the President for Science and Technology; the Director, Critical Infrastructure Assurance Office; the Director, National Infrastructure Protection Center; the organizations that participated in our study; and other interested parties. We will make copies available to other interested parties upon request. This report also will be available on our Web site at www.gao.gov.

If you have any questions, please call me at (202) 512-3317, or you may e-mail me at daceyr@gao.gov. Major contributors to this report included Jean Boltz, Michael Gilmore, Danielle Hollomon, and Catherine Schweitzer.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

Objectives, Scope, and Methodology

Our overall objective was to identify information-sharing practices that federal organizations and others can adopt to improve their ability to understand, anticipate, and address computer-based vulnerabilities and incidents. Our specific objectives were to identify (1) critical success factors in building information-sharing relationships and (2) related challenges and how to address them.

To meet these objectives, we studied 11 federal and nonfederal entities experienced in developing relationships and procedures for information sharing. We identified these organizations by soliciting suggestions from a variety of sources, including our analysts familiar with information-sharing organizations and members of our Executive Council on Information Management and Technology, which is a group of executives with extensive experience in information technology management who advise us on major information management issues affecting federal agencies. These sources recommended over 30 public and private organizations. After initial discussions and further research, we narrowed our focus to 11 organizations that most closely met our criteria of being a recognized, competent information-sharing entity, primarily sharing sensitive or time-critical information pertaining to computer-based vulnerabilities and incidents.

These 11 organizations included among their membership representatives from federal, state, and local governments; private companies of varying sizes; and the academic community. The individuals who were involved in the organizations had various technical and business backgrounds—such as information security specialists, computer scientists, engineers, auditors, lawyers, law enforcement officers, and medical professionals. Each of the 11 organizations covered by our review is described in Appendix II.

To identify common critical success factors, we researched each organization, analyzed relevant documents, interviewed pertinent organization officials and knowledgeable members, observed meetings and other operations, and compared their experiences for similarities. To identify challenges associated with successful information sharing, we obtained the views of officials and members of each organization and reviewed supporting documentation, when it was available.

We solicited comments from each of the eleven organizations that we studied. Additional supporting points and examples were incorporated as

appropriate. We conducted our study from May 2001 through October 2001 in accordance with generally accepted government auditing standards.

The 11 Organizations That Participated in GAO's Study of Information Sharing

The Agora

The Agora is a Seattle-based regional network of over 600 professionals representing a variety of fields, including information systems security; law enforcement; local, state, and federal governments; engineering; information technology; academics; and other specialties. The participants represent over 150 commercial firms and 140 government entities located in 20 U.S. States and 5 Canadian Provinces.

Founded in 1995, the Agora formed to address the enormous security challenges brought about by new computer, network, and Internet technologies. The Agora's objectives are to

- establish confidential ways for organizations to share sensitive information about common problems and best practices for dealing with security threats,
- develop and share knowledge about how to protect electronic infrastructures,
- establish shared services that enhance participants' ability to successfully perform their daily jobs,
- prompt more research specific to electronic information systems security,
- share educational opportunities, and
- enjoy the benefits of the fostered relationships.

Information sharing occurs primarily through quarterly meetings that typically include 175 Agora members. In addition to the quarterly meetings, informal meetings and teleconferences are held among members on an ad hoc basis to discuss issues as they arise, such as assisting entities under attack.

Centers for Disease Control and Prevention

The Centers for Disease Control and Prevention (CDC), which is an agency of the Department of Health and Human Services, is recognized as the lead federal agency for protecting the health and safety of people at home and abroad. CDC seeks to accomplish its mission by working with partners throughout the nation and world to monitor health, detect and investigate health problems, conduct research to enhance the prevention of disease,

foster safe and healthful environments, and provide leadership and training.

CDC uses several information-sharing computer systems to help accomplish its mission, three of which were covered by our review and are described below.

PulseNet

In 1998, CDC officially announced the establishment of PulseNet, a national network of public health laboratories that helps epidemiologists rapidly identify clusters of foodborne illness and alerts others in the surrounding geographic area and throughout the country regarding a possible outbreak. By sharing information on outbreaks quickly through computer systems connected to the Internet, PulseNet allows CDC to very quickly notify public health officials and food regulators of the health threat and assist investigators in identifying and removing the food source of the outbreak from distribution channels, thus mitigating the health risks associated with such outbreaks.

Epidemic Information Exchange

In November 2000, the Epidemic Information Exchange system was implemented as an interactive, secure, Internet-based network that provides information on epidemic outbreaks, toxic exposures, and other health events as they occur. Epidemic Intelligence Service officers at CDC, state and local laboratory personnel, and other public health officials use the system to securely conduct on-line discussions about posted events, communicate with public health officials, and request both financial and nonfinancial assistance. Because of the sensitivity of the system's information, both users and providers of the information must be granted access to the system. In addition, before the information is made available to the system's users, editors and a medical director, who is a physician, review the information to ensure accurate information exchange.

The Data Web

The Data Web, jointly developed by CDC and the U.S. Census Bureau, is a newly implemented system for cataloging and sharing social science data across the Internet. In this regard, the Data Web brings together demographic, economic, environmental, health, and other data maintained on different systems by different organizations wishing to make available their social-science-related data to a wide audience using a variety of systems.

The primary users of the Data Web are scientists, researchers, academicians, business personnel, and professionals who need real-time

access to government and scientific data originating from diverse systems and disciplines. While most data are widely accessible, the system provides a means for data providers to restrict access to sensitive information.

CERT® Coordination Center

The CERT® Coordination Center (CERT/CC) was established in 1988 by the Defense Advanced Research Projects Agency. The center is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts to limit the damage associated with, and respond to, computer-based incidents; (2) conducting research into the prevention of security incidents; and (3) building awareness of security issues across the Internet community. In this role, CERT/CC (1) receives from and provides to system and network administrators, technology managers, and policy makers Internet security-related information and (2) provides guidance and coordination for responding to major Internet security events, such as the Melissa virus and Year 2000 conversion challenge. The center attempts to be an unbiased and trusted source of information, in part by providing trend and composite information only, by deleting information that would allow victims to be identified, and by coordinating the response information it provides with academic, government, and corporate experts. Through this collaboration, CERT/CC has developed a distributed model for incident response teams. It also provides leadership in the response team community by assisting organizations in developing their own emergency response capabilities.

Federal Computer Incident Response Center

The Federal Computer Incident Response Center (FedCIRC) is the focal point for dealing with computer-related incidents affecting federal civilian agencies. Originally established in 1996 by the National Institute of Standards and Technology, the center has been administered by the General Services Administration since October 1998.

FedCIRC's primary purposes are to provide a means for federal civilian agencies to work together to handle security incidents, share related information, and solve common security problems. In this regard, FedCIRC

- provides federal civilian agencies with technical information, tools, methods, assistance, and guidance;
- provides coordination and analytical support;

- encourages development of quality security products and services through collaborative relationships with federal agencies, academia, and private industry;
- promotes incident response and handling procedural awareness within the federal government;
- fosters cooperation among federal agencies for effectively preventing, detecting, handling, and recovering from computer security incidents;
- communicates alert and advisory information regarding potential threats and emerging incident situations; and
- augments the incident response capabilities of federal agencies.

In accomplishing these efforts, FedCIRC draws on expertise from the Department of Defense, the intelligence community, academia, and federal civilian agencies. In addition, FedCIRC collaborates with the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center in planning for and dealing with criminal activities that pose a threat to the critical information infrastructure.

International Information Integrity Institute

The International Information Integrity Institute (I-4) is sponsored by AtomicTangerine, a provider of information security consulting services whose clients include major global corporations. I-4 is a forum for sharing information among its member companies on developing and sustaining effective information security programs to support their global business environments. Its membership is limited to 75 of *Business Week's* Global 1000 companies. In addition, I-4 maintains alliances with leading research organizations, such as SRI International and Kent Ridge Digital Labs, to stay abreast of the latest technical, communications, legal, and economic developments. AtomicTangerine also maintains a number of alliance partnerships with companies that specialize in various areas of emerging technology and architecture, which help provide information to I-4 members.

I-4 members communicate primarily through forums, regional meetings, and a secure Web site that allows for member queries and distribution of analytical reports. I-4 forums are held three times a year, allowing representatives from all 75 I-4 member companies an opportunity to establish and maintain personal contacts, make formal presentations with

follow-on discussions, and hold informal discussions about information protection and risk-management issues. Each member company is encouraged to send two representatives. Regional meetings, held five to six times a year, are generally shorter and targeted at members in a specific geographic region, such as the United States, Europe, or Asia. During these meetings, selected topics are discussed in greater depth than at forums. Throughout the year, members continuously carry on dialogs through queries on information security policy, procedure, and technology management issues, moderated by the I-4 staff.

InfraGard

The National InfraGard Program began as a pilot project in 1996 in the Cleveland FBI Field Office to build a better relationship between the FBI and the private sector in addressing cyber and physical threats. The National Infrastructure Protection Center, which is an interagency center housed at the FBI, in conjunction with representatives from private industry, the academic community, and government, has worked to expand InfraGard by encouraging development of local chapters associated with each of the FBI's 56 field offices. As of October 2001, InfraGard had over 2,000 members and 65 chapters.

InfraGard chapters establish direct contact between law enforcement and infrastructure owners and operators, such as utility companies and health care organizations, through periodic meetings and a secure Web site. These communication mechanisms allow the InfraGard to

- gather information on cyber threats, vulnerabilities, and intrusions and distribute it to members,
- educate the public and members on infrastructure protection,
- disseminate sensitive information to members who have signed a secure access agreement, and
- distribute analytical products on information received from InfraGard members.

In June 2001, InfraGard members elected a National Executive Board to govern the national InfraGard program and draft new policies and procedures to enhance the program's effectiveness.

Joint Task Force–Computer Network Operations

The Joint Task Force–Computer Network Operations (JTF-CNO) (formerly the Joint Task Force–Computer Network Defense) is the primary Department of Defense entity for coordinating and directing internal activities to detect computer-based attacks, contain damage, and restore computer functionality when disruptions occur. The unit was established in 1998 to serve as one organization with overall authority for directing defensive actions against computer-based attacks across the entire Department. As such, JTF-CNO is supported by the Departments of the Army, Navy, and Air Force and the Marine Corps computer emergency-response teams and other Defense components.

In April 2001, the JTF-CNO's scope of responsibility was expanded to include a new operational mission: computer network attack. In addition to expanding mission responsibilities, the JTF-CNO is growing in size and depth to better meet increased network defense responsibilities. The JTF-CNO expansion significantly increases its ability to perform the following: (1) preventive activities, such as conducting security reviews and issuing vulnerability alerts; (2) coordination and monitoring detection activities performed by components, including monitoring automated intrusion-detection systems; (3) investigative and diagnostic activities; and (4) event handling and response activities, which involve disseminating information and providing technical assistance to system administrators so that they can appropriately respond to cyber attacks.

JTF-CNO maintains a close relationship with the CERT/CC, the NIPC, and FedCIRC by participating in joint technical exchanges, working groups, and countermeasure development teams.

National Coordinating Center for Telecommunications

In 1983, the National Coordinating Center for Telecommunications (NCC), which is operated by the National Communications System[1] and staffed by government employees and representatives from major telecommunications service providers, was created by Executive Order 12472 as a joint industry and government organization to handle emergency

[1]In 1982, the National Communications System was established by executive order as a federal interagency group responsible for the national security and emergency preparedness telecommunications. These responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure, which includes the Internet, to achieve effectiveness in managing and using national telecommunication resources to support the federal government during any emergency.

requests related to the physical telecommunications network. The NCC's industry and government representatives' specific functions include

- advising executives and senior officials,
- maintaining points of contact with the parent organizations,
- coordinating and directing prompt restoration of telecommunications services in support of national security and emergency preparedness needs during crises such as natural disasters or war, and
- producing emergency response plans and procedures as a result of lessons learned during actual events.

In January 2000, the NCC was recognized by the President's National Security Council as the information sharing and analysis center (ISAC) for the telecommunications sector. As such, the NCC is responsible for facilitating the exchange of information among government and industry participants regarding computer-based vulnerability, threat, and intrusion information affecting the telecommunications infrastructure. Also, it analyzes data received from telecommunications industry members, government, and other sources to avoid or lessen the impact of a crisis affecting the telecommunications infrastructure.

Since its recognition as an ISAC, NCC's membership has expanded beyond traditional telecommunications entities, such as telephone companies, to include other technology companies involved in the telecommunications infrastructure.

Network Security Information Exchanges

In 1991, government and industry Network Security Information Exchanges (NSIEs) were established by the National Communications System and the President's National Security Telecommunications Advisory Committee (NSTAC)[2] to identify, research, and share information about computer-based incidents that could negatively affect national security and emergency preparedness telecommunications. The goal of the

[2]In 1982, the National Security Telecommunications Advisory Committee, which is composed of presidentially appointed senior executives from 30 major U.S. corporations in the telecommunications and financial services industries, was established to advise the President on national security and emergency preparedness telecommunications issues.

NSIEs is to exchange information about the security of the public telecommunications network, including the Internet, to improve the overall reliability and security of the entire network. In addition, the NSIEs strive to improve each member's total knowledge and understanding of the risks to the nation's telecommunications.

Although the two NSIEs are managed separately, their activities are closely coordinated, and they meet jointly every 2 months to exchange information and views about current threats, vulnerabilities, incidents, and solutions. As of August 2001, the government and industry NSIEs collectively had over 50 members from federal agencies and NSTAC member corporations, as well as a limited number of invited experts. Federal government members represent agencies that have functions related to telecommunications research, standards, regulation, law enforcement, or intelligence or are major telecommunications users. Industry NSIE members include representatives from telecommunications service providers, equipment vendors, systems integrators, and the financial services industry—a major telecommunications user.

New York Electronic Crimes Task Force

In 1995, the New York Electronic Crimes Task Force was formed by the United States Secret Service to investigate electronic crimes associated with computer-generated counterfeit currency, counterfeit checks, credit card fraud, telecommunications fraud, and access device fraud, to name a few. In addition, the task force has

- developed educational and training programs for children and parents to protect children from being exploited through the Internet,
- encouraged research and development of tools and methodologies to prevent crime,
- supported law enforcement education, and
- promoted development of trusted relationships between the public and the private sector.

The task force has over 400 individual members drawn from 50 different federal, state, and local law enforcement agencies; 100 private companies; and 6 universities. The Secret Service has also assigned eight agents who have received specialized training in all areas of electronic crimes through its Electronic Crimes Special Agent Program. The task force has created

this alliance to pool the expertise, authorities, and technical resources required to address electronic crimes—an effort that has been recognized by communities across the country and internationally as a model for local interagency cooperation and private/public partnership. South Carolina has recently implemented a similar model.

North American Electric Reliability Council

The North American Electric Reliability Council (NERC) was formed in 1968 after a 1965 power outage crippled much of the northeastern United States. The council is a voluntary organization of organizations involved in bulk power production and distribution to promote standards and procedures and improve the reliability of the electric power supply. Due to the interconnectivity and interdependency of the electric power grid, information sharing is a necessity for (1) maintaining the reliability of the power supply and (2) conducting business transactions in a deregulated environment. NERC depends on reciprocity, peer pressure, and the mutual self-interest of its members to prevent any future occurrence like the 1965 incident. It also serves as an officially recognized ISAC for combating computer-based attacks on the electric power industry. In this capacity, it cooperates with the federal National Infrastructure Protection Center to identify threat trends and vulnerabilities and disseminate assessments, advisories, and alerts to its members.

NERC membership consists of representatives from each of the 10 regional councils that represent geographic regions encompassing the entire United States and Canada and a small part of Mexico. Because any organization that is part of the power grid can potentially affect the operation and stability of the entire grid, members of these regional councils come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric power cooperatives; state, municipal, and provincial utilities; independent power producers; power marketers; and other interested parties.

The council primarily uses various databases accessible through secure Web sites for disseminating and collecting shared information on many aspects of energy generation and transfer. In addition, NERC allows members to create committees designed to solve particular problems or support ongoing efforts, such as standards setting and critical infrastructure protection.

GAO's Mission

The General Accounting Office, the 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 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 our home page and complete the easy-to-use electronic order form found under "To Order GAO Products."

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
P.O. Box 37050
Washington, D.C. 20013

To order by Phone: Voice: (202) 512-6000
TDD: (301) 413-0006
Fax: (202) 258-4066

Visit GAO's Document Distribution Center

GAO Building
Room 1100, 700 4th Street, NW (corner of 4th and G Streets, NW)
Washington, D.C. 20013

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm,
E-mail: fraudnet@gao.gov, or
1-800-424-5454 (automated answering system).

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

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00