United States Government Accountability Office

GAO

Report to Congressional Requesters

April 2006

INFORMATION SHARING

DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information

GAO-06-383

April 2006

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-383, a report to congressional requesters

INFORMATION SHARING

DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information

Why GAO Did This Study

A wide array of cyber and physical assets is critical to America's national security, economic well-being, and public health and safety. Information related to threats, vulnerabilities, incidents, and security techniques is instrumental to guarding these critical infrastructures against attacks and mitigating the impact of attacks that may occur. The ability to share security-related information can unify the efforts of federal, state, and local government as well as the private sector, as appropriate, in preventing and minimizing terrorist attacks. The Critical Infrastructure Information Act of 2002 was enacted to encourage nonfederal entities to voluntarily share critical infrastructure information and established protections for it. The Department of Homeland Security (DHS) has a lead role in implementing the act. GAO was asked to determine (1) the status of DHS's efforts to implement the act and (2) the challenges it faces in carrying out the act.

What GAO Recommends

GAO is recommending that the Secretary of Homeland Security, among other things, better define DHS's and other federal agencies' critical infrastructure information needs, and explain how DHS and the other agencies will use the information received from the private sector. In oral comments on a draft of this report, DHS concurred with our findings and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-383.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Dave Powner at 202-512-9286, Pownerd@gao.gov or Eileen Larence at 202-512-6510, Larencee@gao.gov.

What GAO Found

DHS has issued interim operating procedures and created a Program Office to administer the critical infrastructure protection program called for by the Critical Infrastructure Information Act. The interim procedures designate the responsibilities and authority of the Program Manager, and establish requirements related to accepting, protecting, sharing, and using critical infrastructure information as required by the act. The Program Office has begun to accept and safeguard critical infrastructure information submitted voluntarily by infrastructure owners and is sharing it with other DHS entities and, on a limited basis, with other government entities. For example, as of January 2006, the Program Office had received about 290 submissions of critical infrastructure information from various sectors. The Program Office also has initiated outreach efforts to publicize the program to the public and private sectors. In addition, it has trained approximately 750 potential users in DHS and other federal, state, and local government entities how to handle protected critical infrastructure information. This training is a prerequisite to being allowed to view the information. The Program Office has also trained at least 16 federal and state officials how to establish programs in their own entities so they can receive protected critical infrastructure information from DHS and then be authorized to store and share it.

DHS faces challenges that impede the private sector's willingness to share sensitive information. Key challenges include

- defining specific government needs for critical infrastructure information,
- determining how the information will be used,
- assuring the private sector that the information will be protected and who will be authorized to have access to the information, and
- demonstrating to critical infrastructure owners the benefits of sharing the information.

If DHS were able to surmount these challenges, it and other government users may begin to overcome the lack of trust that critical infrastructure owners have in the government's ability to use and protect their sensitive information.

Contents

Abbreviations

CII	critical infrastructure information
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
ISAO	Information Sharing and Analysis Organization
MOA	memorandum of agreement
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
NSA	National Security Agency
OMB	Office of Management and Budget
PCII	protected critical infrastructure information
PCIIMS	protected critical infrastructure information management system

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

April 17, 2006

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Todd Platts
Chairman, Subcommittee on Government Management,
Finance, and Accountability
Committee on Government Reform
House of Representatives

The Honorable Robert Bennett
United States Senate

Information about threats, vulnerabilities, and incidents is a crucial tool in fighting terrorism and protecting the nation's critical infrastructures—those cyber and physical assets essential to national security, national economic security, and national public health and safety. Because the private sector owns a large percentage of the nation's critical infrastructure—such as banking and financial institutions, telecommunications networks, and energy production and transmission facilities—public/private partnerships are crucial for successful critical infrastructure protection. The ability to share security-related information can unify the efforts of federal, state, and local governments as well as the private sector, as appropriate, to prevent and minimize terrorist attacks.

We have reported previously on critical success factors and challenges in the information-sharing relationships between public and private entities for critical infrastructure protection.[1] In addition, in January 2005, we designated information sharing to improve homeland security, including critical infrastructure protection, as a governmentwide high-risk area

[1]GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004); and *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

because, while receiving increased attention, the issue still poses significant challenges.[2]

The Homeland Security Act of 2002 created the Department of Homeland Security (DHS) and gave it wide-ranging responsibilities for critical infrastructure protection. Among other things, the Homeland Security Act required DHS to develop a comprehensive national plan for securing the nation's critical infrastructures; recommend measures to protect key infrastructures; and access, receive, analyze, and disseminate, as appropriate, information on terrorist threats to these assets.

The Critical Infrastructure Information (CII) Act of 2002 was enacted into law as part of the Homeland Security Act. The CII Act required that DHS establish procedures for the receipt, care, and storage of CII voluntarily submitted to the government.[3] The act was intended to encourage infrastructure owners to voluntarily share sensitive information, including vulnerability assessments and security methods, by providing rigorous protection mechanisms to ensure that the information would not be inappropriately released and used. The act authorized the federal government to use the information to issue advisories, alerts, and warnings regarding threats to critical infrastructures that the private sector and others could use to enhance protection measures.

In response to your request, our objectives were to determine (1) the status of DHS's efforts to implement the CII Act and (2) the challenges it faces in carrying out the act. To determine the status of DHS's efforts, we analyzed the relevant laws and interim procedures[4] that DHS issued in 2004 laying

[2]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005). GAO uses the high-risk designation to draw attention to the challenges associated with the economy, efficiency, and effectiveness of government programs and operations in need of broad-based transformation.

[3]CII is information that is related to the security of critical infrastructure or protected systems and that is not customarily in the public domain. Once the information is received by DHS and determined to meet the requirements of the act, it is designated as "protected CII."

[4]DHS published a notice of proposed rulemaking in the *Federal Register* in April 2003, and an interim rule that established procedures that were immediately effective on February 20, 2004. In the interim rule, DHS also stated that it would continue to consider public comments for 3 months and would determine whether supplemental regulations were needed. The act required the procedures to be established not later than 90 days after the date of enactment or on or about February 25, 2003.

out the structure and processes for the program, and public comments on the interim procedures. We also reviewed related strategies, policies, procedures, controls, and tools used for the receipt, care, and storage of CII, and interviewed key DHS officials such as the Protected CII Program Manager. We compared what was expected under the CII Act with what had been accomplished by DHS. To determine the challenges in implementing the act, we analyzed and reviewed reports by private sector advisory councils and critical infrastructure protection experts and held interviews with representatives from DHS, federal agencies, state and local governments, private sector entities, and public interest groups. We also relied on prior GAO work on information sharing between federal and nonfederal entities. Appendix I provides additional details on our objectives, scope, and methodology. Our work was conducted from May 2005 to February 2006 in accordance with generally accepted government auditing standards.

Results in Brief

DHS has issued interim operating procedures and created a Program Office to administer the critical infrastructure protection program called for by the CII Act. The interim procedures designate the responsibilities and authority of the Program Manager and establish requirements related to accepting, protecting, sharing, and using CII as required by the act. The Program Office has begun to accept and safeguard information submitted voluntarily by infrastructure owners and is sharing it with other DHS entities and, on a limited basis, with other government entities. The Program Office has been designating information that it determines to meet the act's requirements as "protected CII." For example, as of January 2006, the Program Office had received about 290 submissions of CII from various sectors. The Program Office has also initiated outreach efforts to publicize the program to the public and private sectors. In addition, it has trained approximately 750 potential users in DHS and other federal, state, and local government entities how to handle protected critical infrastructure information (PCII). This training is a prerequisite to being allowed to view the information. The Program Office has also trained at least 16 federal and state officials how to establish programs in their own entities so they can receive PCII from DHS and then be authorized to store and share it.

DHS faces a number of challenges that impede the private sector's willingness to share sensitive information. These challenges include defining specific government needs for CII, determining how the information will be used, assuring the private sector that the information will be protected and who will be authorized to have access to it, and

demonstrating to critical infrastructure owners the benefits of sharing the information. For example, DHS has not defined its specific needs nor has it determined how it will use information submitted under the program. In addition, DHS has not yet used the information to issue any advisories, alerts, or warnings. This lack of specificity and use has impeded the willingness of potential submitters to provide their sensitive information to DHS. If DHS were able to surmount these challenges, it and other government users may begin to overcome the lack of trust that critical infrastructure owners have in the government's ability to use and protect their sensitive information.

To encourage more individuals, private sector entities, and state and local governments that own the critical infrastructure to submit information under the program so that more entities will have access to the information they may need to protect these assets, we are recommending that the Secretary of Homeland Security take a number of actions, including better defining the CII needs of the department and other federal agencies with critical infrastructure responsibilities, defining how DHS and the other agencies will use the information received from the private sector, and expanding efforts to use incentives to encourage more users.

In oral comments on a draft of this report, an audit liaison official from the DHS Departmental GAO/OIG Liaison Office stated that DHS concurred with our findings and recommendations. DHS officials (as well as others who were cited in this report) also provided technical corrections that we have incorporated in this report as appropriate.

Background

Information sharing is an important part of activities that enhance the security of our nation's cyber and physical public and private infrastructures. Federal law and policy related to critical infrastructure protection activities recognize the importance of sharing information about threats, vulnerabilities, and incidents and call for related initiatives. Federal agencies and the private sector have jointly attempted to implement these initiatives for a number of years. The CII Act provides a mechanism to encourage nonfederal entities to voluntarily share sensitive information pertaining to the security and vulnerabilities of their critical infrastructure assets with the federal government, and for that information to be shared with the appropriate federal, state, and local governments for the purposes of analyzing threats and vulnerabilities and issuing alerts and warnings.

Federal Law and Policy Call for Improved Information Sharing

Since 2002, legislation, national strategies, and executive directives have specified actions to improve information sharing for homeland security:

- The Homeland Security Act of 2002[5] created DHS and assigned it critical infrastructure protection responsibilities, including (1) developing a comprehensive national plan for securing the key resources and critical infrastructures of the United States; (2) recommending measures to protect the key resources and critical infrastructures of the United States in coordination with other groups; (3) accessing, receiving, and analyzing law enforcement, intelligence, and other threat and incident information to identify and assess the nature and scope of terrorist threats; and (4) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks. In addition, it included specific mechanisms intended to improve information sharing, including the CII Act (discussed in the next section) and the Homeland Security Information Sharing Act.[6]

- In 2002 and 2003, the White House's *National Strategy for Homeland Security* and its implementing strategies, the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, also highlighted federal actions to promote two-way information-sharing mechanisms.[7]

- Issued in December 2003, Homeland Security Presidential Directive 7 established a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. It defined roles and responsibilities for DHS and agencies with critical infrastructure protection responsibilities to coordinate activities and to encourage the development of information sharing and analysis mechanisms and to

[5]Pub. L. No. 107-296 (Nov. 25, 2002).

[6]The Homeland Security Information Sharing Act requires procedures for facilitating homeland security information sharing and establishes authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information (Subtitle I, Title VIII, Homeland Security Act).

[7]The White House, *National Strategy for Homeland Security* (July 2002); *National Strategy to Secure Cyberspace* (February 2003); and *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003).

support coordinating mechanisms. It required that DHS (1) produce a national infrastructure protection plan (NIPP) summarizing initiatives for sharing information, including providing threat warning data to state and local governments and the private sector, and (2) establish the appropriate systems, mechanisms, and procedures to share homeland security information with other federal departments and agencies, state and local governments, and the private sector in a timely manner.

- In January 2006, the draft NIPP recognized the importance of an information-sharing network and policies and protocols for vetting and disseminating information among both government and private sector partners.[8] It identified 17 critical infrastructure sectors, with sector-specific agencies for each—agriculture and food; public health and healthcare; drinking water and wastewater treatment systems; energy (except nuclear power facilities); banking and finance; national monuments and icons; defense industrial base; chemical; commercial facilities; dams; emergency services; commercial nuclear reactors, materials, and waste; information technology; telecommunications; postal and shipping; transportation systems; and government facilities. In addition, the draft NIPP stated that a final PCII rule is expected in 2006. It also required that, upon signing the letter of agreement with DHS regarding critical infrastructure protection responsibilities, sector-specific agencies would commit to protecting critical infrastructure data according to the Protected Critical Infrastructure Information Program and to sharing NIPP-related information as appropriate. However, at the time of our review, DHS was uncertain when the final NIPP would be released.

CII Act Establishes Protection for Voluntarily Submitted Critical Infrastructure Information to Encourage Sharing

The CII Act was enacted into law as Title II, Subtitle B, of the Homeland Security Act. According to the act, CII is information that is related to the security of critical infrastructure or protected systems and that is not customarily in the public domain. Such information includes (1) actual, potential, or threatened interference with, attack on, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack; (2) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation; or (3) any planned or past operational problem or solution regarding critical

[8]Department of Homeland Security, *National Infrastructure Protection Plan: Base Plan* (Washington, D.C.: January 2006).

infrastructure or protected systems. To qualify for protections under the act, CII must be voluntarily[9] submitted to DHS by an individual, entity, or information sharing and analysis organization.[10] In addition, CII submissions must be accompanied by a written or oral "Express Statement" that states the information is voluntarily submitted in expectation that it will be protected from disclosure under the act. Voluntary submissions under the act cannot be an alternative for compliance with other laws, such as the requirement to submit data on a facility's emissions under the Clean Air Act. The CII Act does not apply to information obtained independently through such other laws or regulations.

Under the CII Act, voluntarily shared CII that meets the above requirements receives protections that include

- exemption from public disclosure under the Freedom of Information Act;[11]
- exemption from disclosure under state and local laws requiring release of information or records; and
- restrictions on sharing and use, such as restricting state officials from sharing with other state officials or using the information in civil actions.

The CII Act also imposes penalties for any federal employee who knowingly and inappropriately discloses CII submissions. The possible penalties include fines, imprisonment for not more than 1 year, or both, and the loss of office or employment.

[9]The CII Act defines "voluntary" as the submittal of CII in the absence of DHS's exercise of legal authority to compel access to or submission of such information (Sec. 212 (7)(A)).

[10]The CII Act defines an "information sharing and analysis organization" as any entity or collaboration created or employed by public or private sector organizations for the purposes of, among other things, (1) gathering and analyzing CII; (2) communicating or disclosing CII to help protect critical infrastructure; and (3) voluntarily disseminating CII to its members; state, local, and federal governments; or other entities (Sec. 212 (5)).

[11]The Freedom of Information Act (5 U.S.C. § 552) establishes the public's legal right of access to government information but also enables the government to withhold certain information from public release.

Key responsibilities assigned to DHS under the act are as follows:

1. A requirement for the Secretary of DHS to establish, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, uniform procedures for the receipt, care, and storage of voluntary CII submissions to the government. The act also specifies that the procedures include mechanisms for

   - acknowledging the receipt of the voluntarily submitted CII;
   - maintaining the identification of this information as voluntarily submitted to the government under the act;
   - caring for and storing such information; and
   - protecting and maintaining the confidentiality of the identity of the person or entity that submitted information, or the information itself if it is proprietary, is business-sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

2. An authorization for either the President or the Secretary of Homeland Security to designate a critical infrastructure protection program within DHS to receive CII.

3. An authorization for DHS to share the information within the federal government and with state and local governments, and that the federal government may use the information to issue advisories, alerts, and warnings using PCII as long as the identity of the source of the information and proprietary, business-sensitive, or information related specifically to a submitting entity is protected from disclosure.

As Required by the CII Act, DHS Has Established Procedures, Organized a Program Office, and Received and Shared Information

In February 2004, DHS issued an interim rule that established procedures, as required by the CII Act, and created a Program Office to administer the program. The office has developed and maintained processes for accepting, protecting, and sharing CII; received about 290 submissions from critical infrastructure owners; begun some outreach with potential submitters to increase information flow; shared PCII on a limited basis with users in DHS and several other federal entities; and trained approximately 750 potential users at DHS, other federal, state, and local government entities and, at least 16 state and local officials how to establish their own programs.

DHS Has Established Procedures as Required by the CII Act

DHS has issued procedures for the receipt, care, and storage of CII, as required by the CII Act. In doing so, DHS first issued a proposed rule on April 15, 2003, and solicited public comment on its provisions. After consideration of the comments received on the proposed rule, DHS issued an interim rule that was effective at the time of release on February 20, 2004.[12] In the interim rule, DHS invited additional comments, stating that it would consider issuing supplemental regulations. DHS received 32 sets of comments on the interim rule from a wide variety of organizations and individuals that raised concerns and offered suggestions and recommendations about various aspects of the program. Currently, the Program Office is operating under the interim rule.

The interim rule includes mechanisms specified by the act regarding

- acknowledging to the submitter that the Program Office has received the voluntarily submitted CII;
- maintaining the identification of this information as voluntarily submitted to the government under the act;
- receiving, handling, storing, and properly marking information as PCII, including reviewing submitted information, determining that it meets the requirements for protection (a process known as validation), and protecting it;

[12]Department of Homeland Security, *Procedures for Handling Critical Infrastructure Information: Interim Rule* (69 FR 8074) (Feb. 20, 2004).

- safeguarding and maintaining the confidentiality of the submitter of the information, but permitting the sharing of the information, as determined by the Program Manager; and

- protecting and maintaining the confidentiality of the information, so as to permit (1) the sharing of it within the federal government and with state and local governments and (2) the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such a manner as to protect from public disclosure the identity of the submitting person or entity or information that is proprietary, is business-sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

To accomplish these requirements, the interim rule established authorities regarding the sharing of protected information with federal, state, and local governments. Under the rule, the Program Manager has the authority to decide what protected information to provide to trained federal, state, or local government employees for purposes that include analysis, warning, asset recovery, reconstitution, and studies of the interdependence of critical infrastructure sectors. For example, the information might be provided if it is needed to study how the banking and finance sector depends on the security of the telecommunications sector so that backup systems can be developed in advance of an incident. In addition, the interim rule states that the Program Manager can share information for other purposes, including the identification, analysis, prevention, preemption, or disruption of terrorist threats to the homeland.

Under the rule, the Program Manager is responsible for administering the program, including (1) reviewing submissions to determine if they meet the requirements for protection—referred to as validation, (2) promulgating directives to operate the program, and (3) preparing training materials as appropriate for the proper treatment of PCII. The Program Manager is also required to establish procedures to ensure that any federal, state, or local entity that wants to use the information appoints one or more employees fully familiar with the procedures as PCII officers. These officers are required to oversee the handling, use, secure sharing, and storage of the information within their respective entity; prevent unauthorized access to the information; and coordinate with the Program Manager.

DHS Has Organized a Program Office, as Authorized by the CII Act

In February 2004, DHS established a Program Office to receive CII. During the course of our review, DHS reorganized and this office is now under the Preparedness Directorate, Office of Infrastructure Protection, and Infrastructure Partnership Division. The Program Office is led by the Program Manager and includes a combination of full-time federal and contractor employees. It is organized into four branches that, among other things, (1) develop and maintain applicable processes for information systems and networks, (2) receive submissions, (3) communicate with submitters about the status of their submission, (4) train users and entities that want to establish their own programs for handling the information, and (5) share PCII.

At the Program Office's establishment, it published an initial, internal procedures manual describing the activities to implement the provisions of the act and the interim rule and providing guidance for administration of the program. The manual describes the process that (1) the submitters from the private sector and others are to use to send the information to DHS and (2) the Program Office is to use to validate that submitted CII meets the act's requirements for protection. The manual also describes the process for sharing PCII with authorized users within DHS, other federal entities, and state and local governments.

The Program Office Has Received and Validated Submissions and Initiated Efforts to Increase Submissions

The CII Act specifies that DHS receive all submissions of CII. Once received by the Program Office, the CII submission enters a validation process for determining whether it qualifies for protection under the act. If the qualifications are met, the submission is marked PCII and is to be provided the protections in the act. If the qualifications are not met, the submission is rejected and destroyed. Appendix II discusses these processes in more detail.

As of January 2006, the Program Office had received 289 submissions, of which 266 were validated as PCII, 8 were in the process of being validated, 14 were rejected, and 1 was withdrawn. The validated submissions include risk and vulnerability assessments about individual infrastructure assets from a variety of critical infrastructure sectors, such as the energy, agriculture and food, banking and finance, and chemical sectors. In addition, entities have submitted data on their operations and on security methods used to protect their assets. According to program officials, submissions were rejected or withdrawn generally because they did not meet the program's requirements, such as not being submitted with an

Express Statement or not being CII as defined in the law, even after the Program Office contacted the submitters for additional information to try to resolve this problem.

To manage the submissions, the Program Office developed, as directed in the interim rule, and is using the Protected Critical Infrastructure Information Management System (PCIIMS)—an electronic database that tracks the receipt and storage of CII submissions, according to program officials. For each submission, the system allows reviewing officials to record the date of receipt, name of the submitter, description of the information received, manner of acknowledgment, tracking number, and validation status. Once a submission is validated as PCII, the information is placed on a secured electronic storage device within the Program Office. Staff in the Program Office reported that they are also working on an updated version of the management system that is expected to streamline and automate the validation process, reducing the time needed to determine if submissions qualify for protection.

To increase submissions, the Program Office has initiated outreach efforts to publicize the PCII program to the public and private sectors. As part of its outreach efforts, the Program Office launched a public Web site in March 2004, presenting program facts and answers to frequently asked questions. In addition, the Program Office prepared over 2,300 fact sheets and about 4,000 brochures that it distributed to public and private stakeholders. It also activated e-mail and telephone help lines to respond to inquiries or comments. To promote the PCII program to private industry, the Program Office has discussed the program in over 30 articles in trade publications, briefed infrastructure sector representatives and participated in industry conferences and seminars, and provided presentation kits that DHS analysts use to explain the program to potential submitters.

In addition, the Program Office implemented an e-submissions process in August 2005 to make submissions easier. According to the Program Office, the benefits to e-submissions include increased transaction speed, improved record-keeping efficiency, increased participation, and improved security. Submitted files are encrypted in transit to prevent access by anyone except Program Office staff and are stored in a stand-alone database maintained at a secure location.

The Program Office is also collaborating with other information sharing and collection efforts to make submission of CII easier. For example, the Program Office gave DHS's National Cyber Security Division (NCSD)

limited authority to receive recurring submissions. At the time of our review, NCSD had not used the authority; however, according to NCSD officials, the validation authority is a positive step because it provides a private sector entity with an additional method to share information with them. In addition, the Center for Food Safety and Applied Nutrition within the Department of Health and Human Service's Food and Drug Administration, is partnering with the Program Office. The center plans to ask a number of dairy facilities to share CII on the safety of the nation's milk supply. The information will be submitted to the Program Office to be validated and will then be made available to the Food and Drug Administration for safety analyses. In New York, the Risk Analysis and Management for Critical Asset Protection program—developed in a public/private sector partnership for DHS by the American Society of Mechanical Engineers as a methodology for performing risk assessments—is offering a method to electronically submit CII to the Program Office for protection. Using the program, infrastructure asset owners will be able to submit results about the security of their facilities to DHS.

The Program Office Has Begun to Share PCII, Trained about 750 Users, and Established a Mechanism to Initiate PCII Programs at Other Entities

As the CII Act authorizes, DHS has begun to share PCII with users. For example, according to NCSD officials, the Program Office received information that it later shared with them. They said that this information was important to investigating a cyber-related incident, but it would not have been provided by the infrastructure owners without CII Act protections. In addition, the Federal Emergency Management Agency (FEMA) received one piece of information from the Program Office. Agency officials said they learned about the information while in discussions with officials from a state who told them that they would not share the information unless it could be protected. On the basis of this requirement, FEMA requested the state to submit the information to the Program Office and had FEMA officials trained in the use and handling of PCII. According to a FEMA official, this information led to the development of generic best practices related to dam security that were presented at a workshop. Also, a few other federal agencies have used the information. For example, in February 2005, at the request of NCSD, the National Security Agency (NSA) became the first non-DHS federal agency to receive PCII. This information was used to assist in the research of a cyber-related incident and did not result in any public alerts. In addition, officials from the Nuclear Regulatory Commission reported that they had reviewed one PCII report.

Prior to allowing federal, state, or local government users access to the information, the Program Office trains them to ensure that users have a clear understanding of how to handle and safeguard PCII and how to access the information on an as-needed basis, according to program officials. The Program Office began user training sessions in February 2004 and established a Web-based training program in November 2004. At the time of our review, approximately 650 individuals from within DHS, including contract personnel, had been trained, along with 110 individuals from other federal, state, and local agencies.

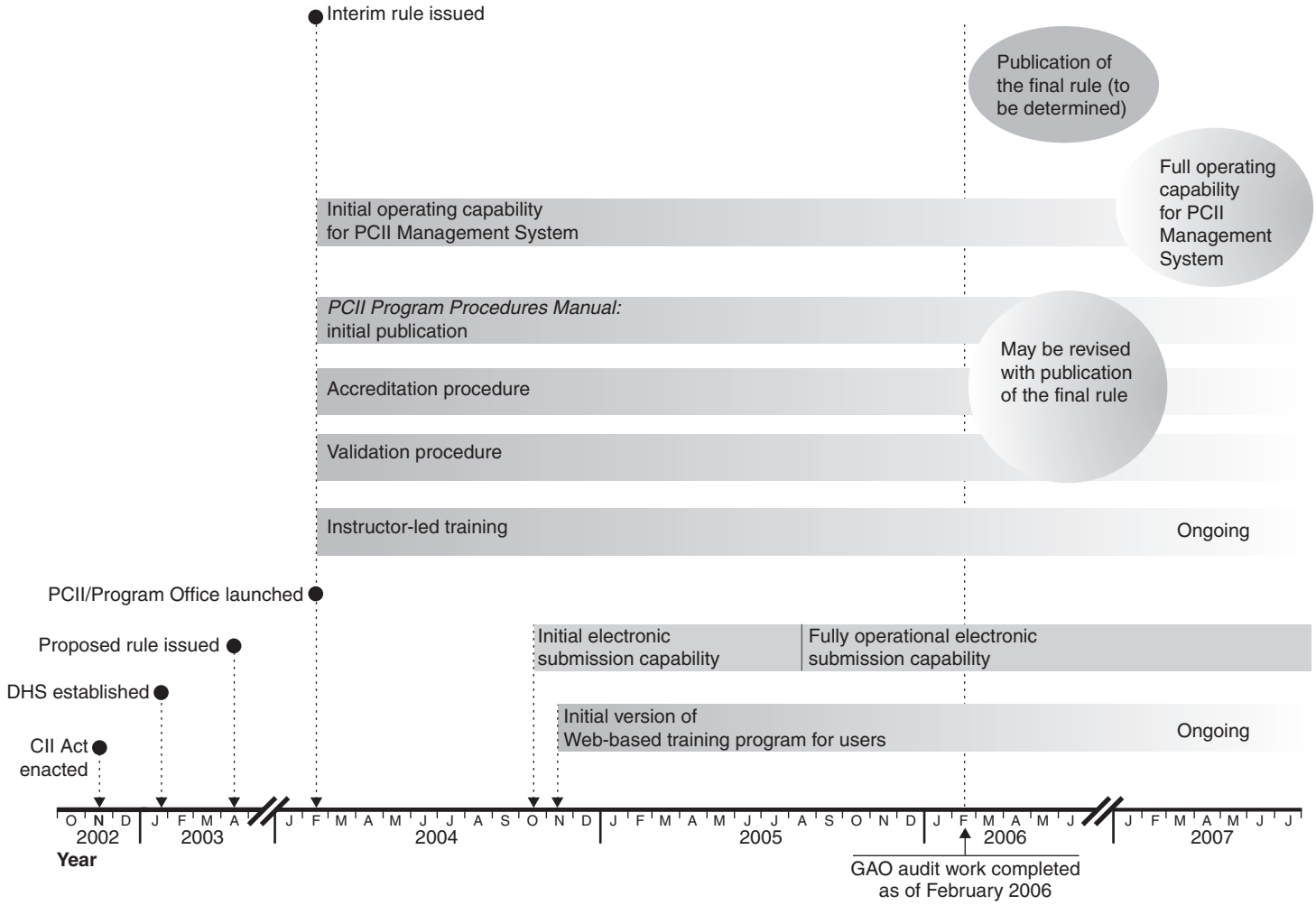
The Program Office also accredits federal, state, and local agency PCII programs. Only accredited entities can receive and store this information. Accreditation ensures that an entity is qualified to manage its own program for handling, using, sharing, and safeguarding PCII, including applicable databases and systems. After determining its need for PCII, an entity must complete the following steps to earn accreditation: (1) appoint a program officer and at least one deputy program officer, both of whom must complete a 3-day course about the use and handling of PCII and pass a certification examination; (2) provide a senior official with the authority to represent the entity and enter into a memorandum of agreement (MOA) with the Program Office; and (3) pass an accreditation review by the Program Office.

Since July 2005, when the PCII Accreditation Program began, the Program Office has trained at least 16 federal and state officials who serve or will serve as program officers or deputy program officers for their respective agencies, according to program officials. Not all of the federal and state entities represented by the 16 officers and deputies have completed the accreditation process. According to program officials, as of January 2006, two entities were fully accredited—Maryland and the Food and Drug Administration's Center for Food Safety and Applied Nutrition. In addition, Arizona, California, and Massachusetts were in the process of being accredited, and other federal entities and states had initiated discussions with the Program Office about becoming accredited. Regarding additional federal agencies, the Nuclear Regulatory Commission is participating in the accreditation process. In addition, according to the Department of Agriculture's Director of Homeland Security and information technology staff, the Department of Agriculture will establish a PCII program, which will require them to become accredited. (See app. II for a more detailed description of the accreditation process.)

According to the Program Manager, the Program Office is most interested in accrediting entities that have lead roles in critical infrastructure protection—such as the Departments of Agriculture, Energy, and the Treasury. However, the Program Manager noted that accreditation is voluntary and some of these agencies may not be interested. In addition, according to the Program Manager, the Program Office will continue to accredit other entities, such as states and other federal agencies, that express an interest in PCII.

Figure 1 summarizes the efforts related to implementation of the CII Act.

Figure 1: Efforts Related to CII Act Implementation



Source: GAO analysis of DHS PCII Program Office data.

DHS Faces Challenges in Implementing the CII Act

DHS faces challenges in implementing the CII Act through the PCII program. These challenges include better defining specific government needs for CII, determining how the information will be used, assuring the private sector that the information will be protected and who will be authorized to have access to it, and demonstrating to critical infrastructure owners the benefits of sharing the information. By overcoming these

challenges, DHS and other users may make strides toward reducing critical infrastructure owners' lack of trust in the government's ability to use and protect their sensitive information.

Defining specific government needs: The act broadly defines what CII can be voluntarily submitted to the government for protection, and the interim rule reiterates the same broad definitions for use by the Program Office in its implementation of the act. However, DHS has not defined the specific information—such as industry-specific vulnerabilities and interdependencies—needed under the program, nor has it comprehensively worked with other federal agencies with critical infrastructure responsibilities to find out what they need. The lack of specificity on the part of DHS in clearly communicating to the private sector what information is needed has impeded the willingness of potential submitters to provide their sensitive information to DHS. The Program Manager and other program officials said that until the potential users of PCII within DHS and other federal agencies with critical infrastructure responsibilities have fully identified their information needs, the private sector will not know what to submit.

An official representing the chemical infrastructure sector agreed that infrastructure owners need to know what kind of information is required so they can provide meaningful submissions. In October 2005, the National Infrastructure Advisory Council also made the point that when requesting information, the government must clarify why they need the information. In addition, defining the needs for information requiring protection is what drives potential users to participate in the program. For example, Maryland and California initiated the accreditation process because, according to responsible officials, they had defined specific information needs that required protection.

Determining how information will be used: The act broadly defines how PCII may be shared with other government entities and used to issue advisories, alerts, and warnings. The interim rule provides procedures on how information will be shared with other entities for the same broad uses. However, potential users within DHS have not specified how they will use the information. In addition, DHS has not yet used the information to issue any advisories, alerts, or warnings, according to DHS officials. An Infrastructure Partnership Division official also said that until more information is submitted under the program, it will be difficult for DHS to determine how it will use the information.

In October 2005, the National Infrastructure Advisory Council stated that the private sector might be more willing to share information if "when requesting information, the government clarified how they will use it." In addition, an official representing the chemical infrastructure sector agreed that entities would be more likely to submit CII if they knew how it would be used. We have also reported in the past that uncertainty about how the information would be used and who it would be shared with posed a barrier to critical infrastructure sectors sharing information with the government.[13]

The Program Office faces the challenge of building a demand for PCII among potential users of the information by demonstrating how it will help users achieve their critical infrastructure missions. Without identifying a specific use for PCII, entities are often reluctant to commit the necessary effort toward accreditation. For example, according to an NSA official who used PCII once, while there was value to having the information his office had already used, its use did not impact his office's final conclusions on the investigation they were conducting or result in any analytical or warning products being issued. Because the use for the information was considered an isolated case, NSA does not plan to establish an accredited PCII program.

In addition, FEMA officials who also used PCII once, noted that PCII they had received was valuable in developing security-related best practices that FEMA presented at a workshop. However, they have no current plans to establish a formally accredited program because they are uncertain how they will use the information in the future. Also, as previously discussed, user participation in the PCII program is completely voluntary, even for agencies that have particular responsibilities for a critical infrastructure sector. Nonetheless, the Program Office is attempting to train enough users and help other government entities establish programs so that there is a critical mass of users to help make the program viable.

Other DHS officials stated that their own use of PCII had been purely incidental. For example, DHS's Office of Intelligence and Analysis has not found PCII to be essential for its operations largely because its emphasis is on analyzing and responding to immediate threats, while PCII is

[13]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

information relating to vulnerabilities. At this early stage of the program's maturity, an official said PCII is not viewed by the Intelligence and Analysis analysts as providing better or more relevant information than that which they receive on a daily basis from the intelligence community and the many other sources used to identify threats. On the other hand, the Deputy Director of the Infrastructure Partnership Division stated that analysts within the division could find PCII very useful to their mission. In addition, DHS officials believe that as more PCII becomes available, they will use it in their new Homeland Infrastructure Threat and Risk Analysis Center—a national center for the integration, analysis, and sharing of information related to the threat of terrorist attacks on critical infrastructure.

Assuring the private sector that the information will be protected and who will be authorized to have access to it: To implement the protection requirements in the act, the interim rule establishes procedures for marking, safeguarding, and sharing the information. In addition, the Program Office has established (1) the training program to equip authorized users with knowledge of how to safeguard the information and (2) the PCII Accreditation Program to ensure that other organizations have processes and policies to promote the safeguarding of the information.

However, potential submitters often continue to be reluctant to provide their sensitive information because they are not certain that their information will be fully protected. They fear that the information could be inadequately protected, used for future legal or regulatory action, or inadvertently released. For example, as follows, specific provisions in the law and rule impact perceptions that the submitted information will not be protected, according to DHS, other federal agencies, and the private sector:

- Originator control: Under the rule, the Program Manager has the authority to decide what PCII to provide to federal, state, or local government employees for approved purposes; the originator of the critical information cannot control how the submission is shared at the federal level. According to an official representing a multisector organization, infrastructure sector entities are hesitant to share information because of its sensitivity, without having control over who has access to it. According to the Program Manager, the Program Office is considering a method that they believe would meet the act's intent—that is, submitters would identify at the time of submission what users they believe should or should not be able to receive the information. Under this method, the Program Office would contact the submitter if a need arose for another entity to use the information. According to DHS,

this method has been used for some PCII submissions. However, this method has not yet been instituted.

- Direct submissions: To receive protection, all submissions must be received by DHS directly from the original submitter. For example, the Department of Defense cannot receive information from members of the defense industrial base and protect it as PCII or forward it to DHS to be labeled and protected. However, in commenting on the interim rule, one federal agency, as well as four infrastructure sector organizations, expressed interest in being able to directly receive or submit this information because of existing relationships. For example, an official representing a multisector organization stated that private and public critical infrastructure entities have already built relationships with each other over many years and have sufficient trust to share information with each other. According to the Program Manager, the issue of direct submission will have to be addressed at some point; however, at this early stage in the program, it is not worth the risk of having PCII inappropriately released by an agency, because any mistake would undermine the entire effort to build trust.

- Legal precedents: According to the Program Manager, there have been no court cases addressing the CII Act. According to the Program Office and the Homeland Security Advisory Council report, until the courts uphold the protections, the private sector will frequently be hesitant to use the program.

In addition, potential submitters of CII have been hesitant to provide their sensitive information because they are not certain how information would be protected under the final rule. As of January 2006, DHS had not issued a final rule, as planned. DHS had established April 2005, June 2005, and August 2005 as deadlines for the rule to be issued, but it missed these time frames. The Program Manager and other program officials reported that the draft final rule had been undergoing legal review within DHS since the summer of 2005 and would go to the Office of Management and Budget (OMB) for interagency review before becoming final. However, they could not predict when this would occur and did not have any target deadlines established. In addition, the Program Manager and other program officials were uncertain what changes, if any, would be made to the rule during legal and interagency review.

We have reported in the past that the uncertainty about how information would be protected by federal agencies was a barrier to critical

infrastructure sectors sharing information with the federal government. For example, in May 2005, we reported that critical infrastructure entities did not openly share cybersecurity information with DHS, in large part, because they were concerned that the potential release of sensitive information could increase the threat to the respective entity.[14] Also, in April 2004, we testified that the reluctance by information-sharing organizations to share information had focused on concerns over potential government release of that information, among other things.[15]

In addition, the Program Office has been challenged to implement a program that will provide protection to CII consistently across federal, state, and local government entities while adhering to the scope of the act and the interim rule. Some of the challenges that DHS, states, and private sector entities identified were as follows:

- Sharing PCII with and among the state and local governments: Under the act, state officials are not allowed to directly share PCII with officials in other states, unless the Program Office gets written consent from the person or entity submitting the information. This is a challenge that limits sharing when state officials meet and when a state official knows that information could be useful to another state official to address a vulnerability or threat. The Program Office is considering resolving this issue by having submitters grant written approval for this type of sharing when they submit CII—similar to how the issue of originator control could be handled.

- Penalties for inappropriate disclosure are limited to federal employees: The act imposes criminal and administrative penalties for federal employees that disclose PCII; however, those penalties do not apply to contractors or state and local officials, who could face significantly less penalty for disclosure. The variation of penalties could impact the level of protection. For example, contractors are not subject to criminal penalties and contract termination serves as a deterrent to mishandling the information. For states, the Program Office has suggested that these issues can be resolved through a MOA between the state entity and the Program Office that would stipulate state laws are to be used to

[14]GAO-05-434.

[15]GAO, *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*, GAO-04-669T (Washington, D.C.: Apr. 21, 2004).

prosecute violators. According to the Program Office, this arrangement was made under the memorandum signed with Maryland and California.

Demonstrating benefits to critical infrastructure owners of sharing the information: DHS and other interested federal agencies have not clearly demonstrated to the potential CII submitters the benefit of sharing their sensitive information; therefore, potential submitters may not be willing to take the risk of inappropriate use and release. Federal, state, and private sector officials stated that some of the benefits that potential submitters expect to receive include improved reaction by first responders; improved intelligence and strategic analyses of threat information; and improved performance of services, such as vulnerability analyses for small entities unable to afford their own efforts. However, at the time of our review, DHS's emphasis was on analyzing and responding to immediate threats, rather than on combining threat and vulnerability information into strategic analyses.

Our prior work has shown that the federal government lacks the analytical processes that would provide the sorts of benefits sought by infrastructure owners.[16] We reported that further efforts are needed to address the critical challenges of improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources. We also reported that improvements are needed in the federal sharing of appropriate, timely, and useful warnings and other information concerning cyber and physical threats to federal entities, state and local governments, and the private sector.

Our prior work has also identified demonstrating benefits as a challenge to the federal government. In April 2004, we testified that in white papers, the Information Sharing and Analysis Center Council emphasized that perhaps the greatest barriers to information sharing stem from practical and business considerations, and that the benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable.[17] In addition, in May 2005, we reported that even when organizations within infrastructure sectors shared information with DHS, the entities did not consistently receive useful information in return.[18]

[16]GAO-04-780.

[17]GAO-04-699T.

[18]GAO-05-434.

Overcoming these challenges could help to encourage more submissions, which in turn would provide the opportunity for the government to provide benefits back to the private sector submitters, thereby creating a virtuous cycle that builds on itself until a critical mass of users and submitters is reached and the program becomes self-sustaining. This would help to address the lack of trust in the government that the private sector has consistently identified as a reason to limit information sharing. The Program Manager and other DHS officials acknowledged the need to establish trusted relationships between the CII submitters and the information users in federal, state, and local governments.

Conclusions

DHS has made progress in implementing the CII Act by establishing procedures and creating a Program Office to administer the program. However, DHS is still in the early stages of its efforts to expand the submission and use of PCII and will have to overcome major challenges for its program to be viable. This effort includes issuing a final rule, as DHS has planned to do, so that potential submitters will know how the program will operate. Further, although DHS has a lead responsibility for federal critical infrastructure protection efforts, its planning efforts to date have not articulated what specific information it and other federal agencies with critical infrastructure responsibilities need and how the information will be used. Without this knowledge, the private sector will continue to be hesitant to provide information to DHS. The Program Office is aware of changes it could make to the program that might increase submissions of CII and provide incentives to users, such as providing clarity regarding how the information will be protected, establishing some level of originator control, allowing direct submissions, and providing a mechanism for state-to-state sharing. However, to date, these options and initiatives have not been aggressively pursued. If DHS were able to surmount these challenges, it and other government users may begin to overcome the lack of trust critical infrastructure owners have in the government's ability to use and protect their sensitive information.

Recommendations for Executive Action

In order for DHS to address the challenges to the PCII program—defining specific needs, determining how and who uses the information, assuring submitters that the information will be protected, and demonstrating benefits to critical infrastructure owners—we recommend that the Secretary of Homeland Security take the following four actions:

- In the short term, establish a specific deadline in the near future for releasing the final rule to OMB and for interagency review so that potential submitters have more assurance about how their sensitive information will be protected.

- Concurrently, consistent with other infrastructure planning efforts such as the NIPP,

  - define and communicate to the private sector what CII DHS and federal entities need to fulfill their critical infrastructure responsibilities and how federal, state, and local entities are expected to use the information submitted under the program;

  - determine whether creating mechanisms, such as providing originator control and direct submissions to federal agencies other than DHS, would increase submissions; and

  - expand efforts to use incentives to encourage more users, such as mechanisms for state-to-state sharing.

We are not making new recommendations regarding improving the effectiveness of DHS's information-sharing efforts at this time because our previous recommendations, including performance of a national threat assessment and establishment of a strategic analysis capability for computer-based threats, have not yet been fully implemented.

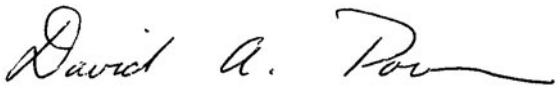
Agency Comments

We received oral comments on a draft of this report. An audit liaison official from the DHS Departmental GAO/OIG Liaison Office stated that DHS concurred with our findings and recommendations, based on the comments received from officials from the Preparedness Directorate, including the Program Office; the Transportation Security Administration; DHS's General Counsel; and others.

In addition, the DHS Departmental GAO/OIG Liaison Office provided technical corrections that it received from the Preparedness Directorate, including the Program Office; DHS's General Counsel; and others. We also received technical corrections from other officials who were cited in our report. We have incorporated the DHS and other technical corrections in this report as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies of this report to interested congressional committees, the Secretary of Homeland Security, and other interested parties. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staffs have any questions concerning this report, please contact either Dave Powner at 202-512-9286 or pownerd@gao.gov, or Eileen Larence at 202-512-6510 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Other GAO staff who contributed to this report are listed in appendix III.



David A. Powner
Director, Information Technology Management Issues

Eileen Regen Larence
Director, Homeland Security and Justice Issues

Objectives, Scope, and Methodology

In response to your request that we review the implementation of the Critical Infrastructure Information (CII) Act of 2002, we determined (1) the status of the Department of Homeland Security's (DHS) implementation efforts and (2) the challenges DHS faces in implementing the act.

To assess the current state of CII Act implementation, we analyzed the CII Act and the *Procedures for Handling Critical Infrastructure Information: Interim Rule*, the procedures that DHS issued in February 2004, and related public comments.[1] In order to understand DHS's efforts to establish a Protected Critical Infrastructure Information (PCII) Program to accept and protect CII, we gathered and analyzed relevant strategies, policies, and procedures, including the *PCII Information Program Management Directive* (draft)*; the PCII Program Procedures Manual*, *Configuration Management Plan*, *Mission Needs Statement*, *Concept of Operations for Management* (draft), and *Systems Risk Assessment*. We held interviews with key officials from DHS's Preparedness Directorate and Intelligence and Analysis Office (formerly, the Information Analysis and Infrastructure Protection Directorate, which included the Disclosure Office, the Infrastructure Coordination Division, and the Information Analysis Division). We observed controls and tools used for the receipt, care, and storage of PCII, as outlined in the Program Office's manuals. In addition, we interviewed officials from the Program Office, including the Program Manager and representatives from each of the office's four branches (Management, Communications, Operations, and Systems). We compared what was expected under the CII Act with what had been accomplished by DHS. Further, we interviewed key officials from DHS units in the Federal Emergency Management Agency and the Transportation Security Administration. We also held interviews with representatives from entities that could potentially submit CII, including infrastructure sector entities and public interest groups, such as the Partnership for Critical Infrastructure Security, the American Chemistry Council, the American Petroleum Institute, and the Edison Electric Institute. We also held interviews with representatives from entities that had used PCII, including federal, state, and local organizations, such as the Department of Defense, National Security Agency, Department of Agriculture, Federal Reserve

[1]The *Procedures for Handling Critical Infrastructure Information: Interim Rule* requires the PCII Program Manager to develop and use an electronic database, to be known as the Protected Critical Infrastructure Information Management System, to record the receipt, acknowledgment, validation, storage, dissemination, and destruction of PCII.

System, Nuclear Regulatory Commission, Maryland Emergency Management Agency, and California Office of Homeland Security.

To determine the challenges to implementing the CII Act, we analyzed reports by private sector advisory councils and critical infrastructure protection experts that have identified related challenges. We also interviewed officials knowledgeable about public/private information sharing and about the act from DHS, federal agencies, state and local governments, private sector entities, and public interest groups. In addition, we relied on prior GAO work on information sharing between federal and nonfederal entities.

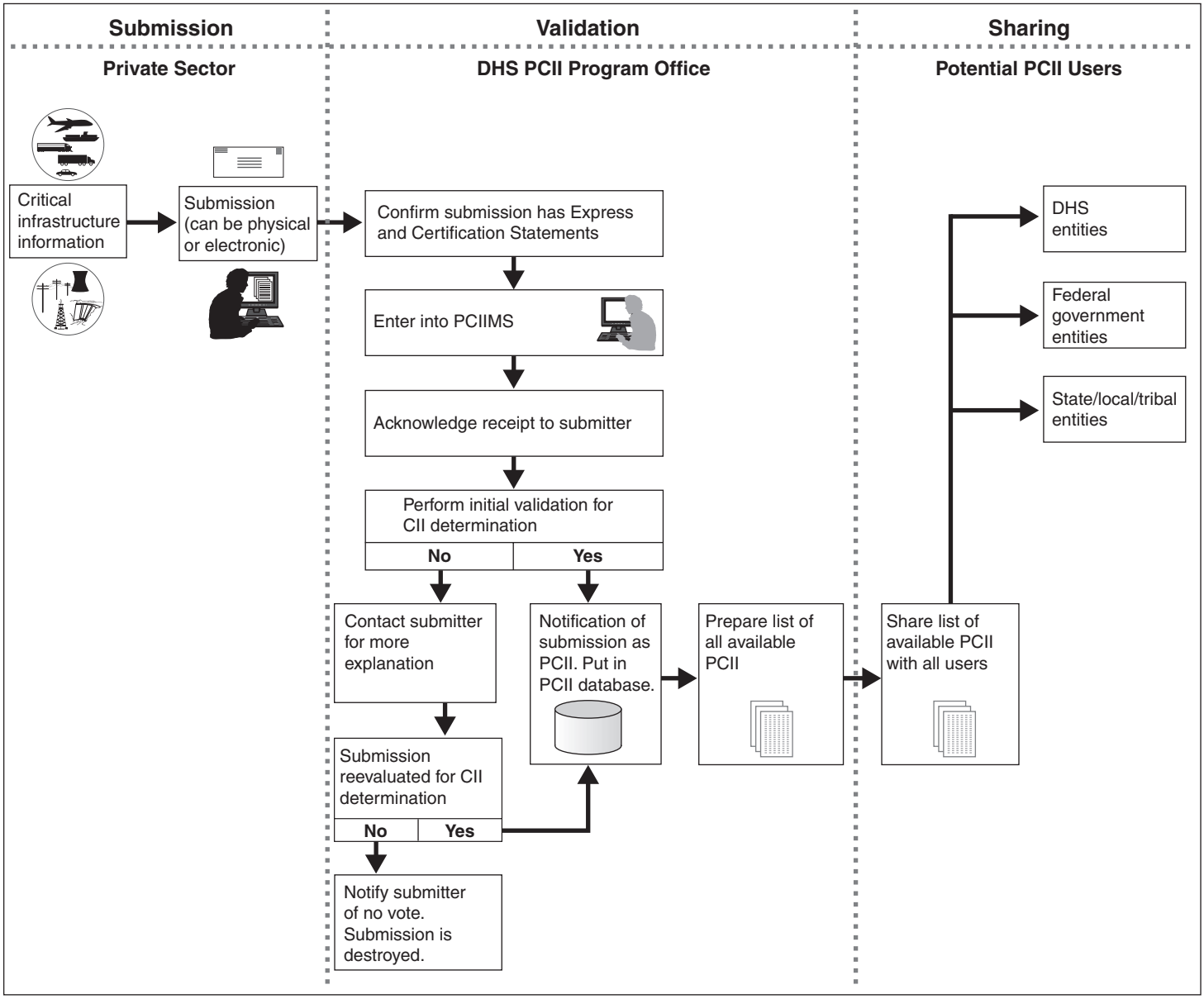
Our work was conducted from May 2005 to February 2006 in accordance with generally accepted government auditing standards.

Procedures for Processing CII and Accrediting Entities

Processing CII

The CII Act requires DHS to establish uniform procedures for the receipt, care, and storage of CII that is voluntarily submitted to DHS. In February 2004, the Program Office implemented a process to review CII and began accepting voluntarily submitted information to determine if it qualifies for protection. For this explanation, the process is divided into three steps: submission, validation, and sharing. Figure 2 summarizes the Program Office's process.

Figure 2: Diagram of the PCII Submission, Validation, and Sharing Process



Source: GAO analysis of DHS data.

Step 1: Submission

The CII Act requires all submissions of CII to be submitted to DHS for protection under the act. Submission to DHS means any voluntary transmittal of CII to the DHS PCII Program Office. CII that is not submitted to DHS does not qualify for protection. Based on the Program Office's process, the submission requirements include the following:

- Sources expected to submit CII to DHS for consideration for protection, or validation, are those with direct knowledge about the security of a critical infrastructure element, and include, but are not limited to, Information Sharing and Analysis Organizations (ISAO),[1] private sector entities, state and local governments, and foreign governments and companies.

- Federal agencies may not independently submit private sector information for PCII protection, unless they are working together in partnership with a private sector entity or the agency is part of an ISAO.

- Submissions must be accompanied by an Express Statement and a Certification Statement before they can be validated as PCII. According to the CII Act, only those submissions that are accompanied by an Express Statement will have the presumption of protection under the act.

- An Express Statement indicates that the information is voluntarily submitted to the federal government with the expectation that it will be protected under the CII Act. A Certification Statement states that the information is voluntarily submitted, is required or is not required to be submitted to the federal government, and is not customarily in the public domain.

- The Program Office accepts submissions electronically through a secure Internet portal or through physical materials, such as floppy disks, video tapes, audio tapes, facsimiles, or letters.

[1]An ISAO is any formal or informal entity or collaboration created or employed by public or private sector organizations for the purposes of, among other things, (1) gathering and analyzing CII to protect against or mitigate an attack; (2) communicating or disclosing CII for such purposes; and (3) voluntarily disseminating CII to its members, federal, state, or local governments; or any other appropriate entities.

Step 2: Validation

Validation is the process for determining whether a submission with an Express Statement qualifies for protection under the CII Act and, therefore, will be protected as provided by the act. The Program Manager will establish time frames for completing the validation process to ensure effective, efficient, and timely validation determinations. On the basis of a review of the information submitted, the Program Manager or designated representative makes an initial determination regarding whether the information qualifies for protection.

Program Office procedures require that submissions be acknowledged and tracked throughout the validation process. If the submission is received with both an Express Statement and a Certification Statement, it will be processed without delay.

Information received without an Express Statement will be destroyed immediately, and the submitter will be asked to resubmit. Submissions received with an Express Statement, but without a complete Certification Statement, will be presumed to be CII and will be processed. However, the submitter will be contacted to provide a Certification Statement.

When information is submitted with an Express Statement, the Protected Critical Infrastructure Information Management System (PCIIMS) will assign it a unique tracking number, which will be used in all future communications with the submitter and for recording the current status of submitted information.

The Program Office must acknowledge receipt of submitted information in writing within 30 calendar days of its receipt. Acknowledgment of receipt means only that the information has been received by the Program Office and is accompanied by an Express Statement.

If the submission is accompanied by both an Express Statement and a Certification Statement, and the Program Office determines that the information meets the definition of CII, then

- the information will be validated as PCII;
- the PCIIMS will be updated to indicate that the information qualifies for protection under the CII Act;
- the submitter will be notified of the decision, and

- the validated PCII will be made available to authorized users.

If the initial review determines that the information submitted does not meet the requirements for protection under the CII Act, the Program Office must

- inform the submitter that the initial determination is that the submission does not meet the requirements to be PCII;
- request the submitter to provide a complete Certification Statement and/or provide additional information within 30 days of the submitter's receipt of the Program Office's request;
- give the submitter the opportunity to withdraw the submission before reevaluation; and
- consider any additional information provided in making the final validation determination; whenever possible, the final review will be performed by the same staff member who performed the initial review.

Newly validated PCII is added to the PCII Submissions Catalog, which is a list of all available PCII information prepared in a non-PCII format so that it can be easily shared. For each submission, the PCII Submissions Catalog contains its tracking number, date of submission, description of submission, and number of pages.

Step 3: Sharing

A copy of the PCII Submission Catalog is provided to all PCII officers for distribution at their discretion to users and analysts for their review. If after reviewing the catalog the users want to request PCII, they may do so through their entity's PCII officer.

The Program Office is authorized to provide access to PCII when it determines that this access supports a lawful and authorized government purpose as specified in the CII Act. The Program Office may provide PCII to federal government departments and agencies and to state and local government entities that have executed the standard memorandum of agreement (MOA) with the Program Manager and have met the requirements of the PCII Accreditation Program.

Before accessing and storing PCII, organizations or entities must be accredited and have a PCII officer to supervise strict compliance with

procedures. Before individual users can access PCII, they must be trained in the proper use, handling, and safeguarding of PCII. Authorized users can request access to PCII on a need-to-know basis. However, users outside of DHS do not have the authority to store PCII until their agency is accredited. In cases where the user is from an entity that is not accredited, the Program Office and the user make arrangements for the user to access the information at the Program Office.

If access is granted, the information is downloaded from the Program Office's secure storage to a paper copy or compact disk. It is then either hand delivered to the user or loaded to another secure system and accessed by the user through a controlled folder on the secure system.

The Program Office is responsible for tracking PCII to the state or local government entity to which it was initially provided. The officially designated PCII officer of each government entity is responsible for sharing and tracking PCII under their control.

Federal government entities may share PCII in their possession provided they verify that the recipient entity has been accredited by the Program Office to receive PCII and will maintain a tracking mechanism that provides a record of what PCII they provided to whom and when they provided it.

State and local governments receiving PCII are not authorized to share PCII with entities external to their governmental entity, unless they obtain the express approval of Program Manager and the explicit written consent of the submitter.

Authorized recipients may use PCII for

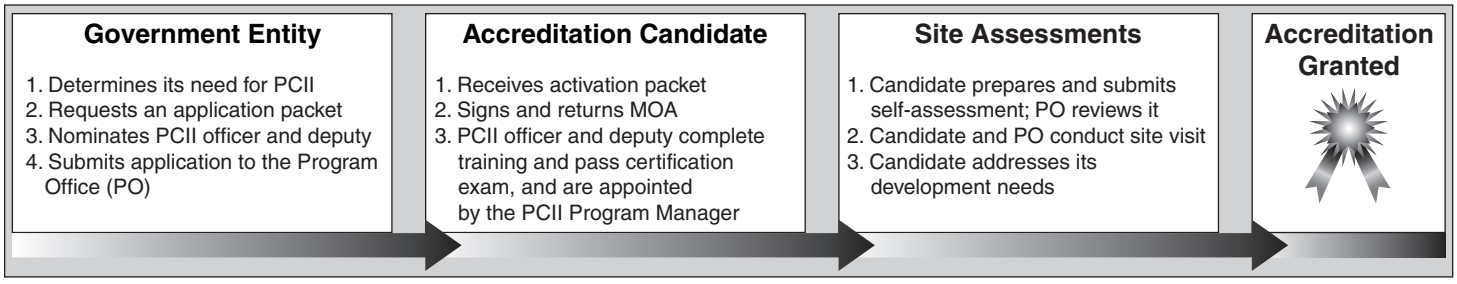
- securing the critical infrastructure and protected systems;
- analysis of potential threats and vulnerabilities;
- warning of imminent attack;
- studying the interdependency between critical infrastructure sectors;
- recovery and reconstitution of damaged infrastructures; or

- another information purpose, including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland.

Accrediting Entities to Receive PCII

Before federal, state, or local government entities can access and store PCII, they must have executed a MOA with the Program Office and have met the requirements of the PCII Accreditation Program. At the time of our review, the Program Office was updating its February 2004 procedures manual with guidance on its accreditation process. The accreditation process was established to ensure that each entity and user has a clear understanding of how to initiate and manage their entities' program and adequate policies, procedures, secure systems, and databases for handling, using, sharing, and safeguarding PCII. The Program Office's Operations Branch is responsible for managing the process, and the Communications Branch is responsible for outreach and training activities in support of the process. Figure 3 outlines the key steps in the accreditation process.

Figure 3: Accreditation Program



Source: GAO.

The following are key steps in the accreditation process.

- After a government entity or other accreditation candidate determines its need for PCII, the entity requests an application from the Program Office and nominates a PCII officer and deputy. Any nonfederal government employee who is nominated to be a PCII officer or deputy must sign a nondisclosure agreement concerning PCII.

- The Program Office appoints the nominated PCII officer and deputy for the candidate entity after they complete a 3-day training course and pass a certification examination.

- A senior official with the authority to represent the candidate entity enters into a MOA with DHS. The MOA (1) constitutes an entitywide obligation and an executive-level commitment to achieving and maintaining PCII accreditation and (2) sets forth the responsibilities and obligations of the PCII officer and deputy as well as the requirements for handling, using, sharing, and safeguarding PCII throughout the federal, state, or local entity.

- The PCII officer completes a self-assessment of how well the entity's policies, procedures, and oversight measures comply with the minimum requirements and procedures set forth in the accreditation guide. The Program Office reviews the self-assessment and works with the accreditation candidate's PCII officer to address any needs for further development activities.

- Once the PCII officer has submitted a self-assessment and addresses any immediate issue, a site assessment team visits the offices and facilities of the accreditation candidate to determine its ability to comply with the requirements set forth in the PCII procedures manual.

- The Program Office accredits the government entity after all needs identified by the assessments are addressed. The PCII officer must submit an annual report to the Program Office to keep the office appraised of any developments in the participant's PCII program. A fully accredited entity must be reaccredited every 3 years. In addition, the Program Office may also elect to conduct a site visit of an accredited entity at any time to ensure that the minimum requirements are continually being met or to respond to requests for consultation or guidance from the entity.

GAO Contacts and Staff Acknowledgments

GAO Contacts

David Powner, (202) 512-9286 or pownerd@gao.gov
Eileen Larence (202) 512-6510 or larencee@gao.gov

Staff Acknowledgments

In addition to the persons named above, R. Rochelle Burns, Neil Doherty, Michael Gilmore, Steve Gosewehr, Barbarol James, Victoria Miller, Susan Quinlan, Nik Rapelje, and Amos Tevelow made key contributions to this report.

GAO's Mission

The Government Accountability 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548