Privacy Impact Assessment
for the

Protected Critical Infrastructure Information Management System (PCIIMS)

June 20, 2007

Contact Point
Laura Kimberly
Protected Critical Infrastructure Information Program
National Protection and Programs Directorate
703-288-3550

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
703-235-0780

Abstract

The Protected Critical Infrastructure Information (PCII) Program, part of the Department of Homeland Security's (DHS) Infrastructure Partnerships Division (IPD), is an information-protection tool that facilitates the sharing of PCII between the government and the private sector. The Protected Critical Infrastructure Information Management System (PCIIMS) is an Information Technology (IT) system and the means by which PCII submissions from the private sector will be cataloged. The PCII Program conducted this privacy impact assessment (PIA) because personally identifiable information (PII) from the submitting individuals is collected for contact purposes.

Introduction

It is estimated that over eighty-five (85) percent of the critical infrastructures within the U.S. are owned and operated by the private sector. Recognizing that the private sector may be reluctant to share information with the federal government if it would be publicly disclosed, Congress passed the Critical Infrastructure Information Act in 2002 (CII Act) with its provisions for protection from public disclosure and charged the Protected Critical Infrastructure Information Program Office (PCIIP) to improve the readiness posture of the United States in order to prevent and/or respond to incidents related to our critical infrastructure by creating a new framework which would enable the private sector to voluntarily submit sensitive information regarding the nation's critical infrastructure.

The foundation for the PCIIP is the CII Act and the implementing regulation, Final Rule for Procedures for Handling Critical Infrastructure Information.[1] This regulation provides for the voluntary sharing of PCII with the Department of Homeland Security (DHS) by the private sector and exempts the information from the Freedom of Information Act (FOIA), state and local disclosure laws, and use in civil litigation. Part of the PCII Program involves the collection of personally identifiable information from points of contact for registered PCII submissions. PCIIP uses the contact information to coordinate and validate, as necessary, a particular CII submission.

The PCIIP supports DHS' first priority, which is "Stronger Information Sharing and Infrastructure Protection," by implementing capabilities to receive PCII from all seventeen (17) critical infrastructures sectors and key segments within each sector; by protecting this information from unauthorized disclosure; and by achieving a level of proficiency whereby DHS will be able to share PCII with federal agencies, state and local governments.

PCII is the information about key resources and critical infrastructures of the United States within seventeen (17) critical sectors such as, power production and generation, information technology and telecommunications systems (including satellites), financial, water, chemical, and several others. Said another way, the infrastructure is the systems, assets, and industries upon which our national security, economy, and public health depends, and PCII is the critical information about those systems, assets, and industries.

PCII is specifically defined by the CII Act § 212(A)-(C) as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems—(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the

[1] Federal Register: September 1, 2006 (6 CFR 29) (Volume 71, Number 170), Final Rule for Procedures for Handling Critical Infrastructure Information.

misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit: or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation."

Agencies, companies, and organizations find the PCIIP through media, trade publications, and newsletters. The information can be mailed, hand-delivered, sent via encrypted e-mail, or uploaded via a secure web site to the PCIIMS.[2] When the information is submitted staff from the PCIIP review the data to ensure its completeness and ensure the site falls under the CII Act's requirements. Once both of those criteria are met the PCII Program Manager or Operations Manager validate the submission and place it as a read-only file in the Protected Critical Infrastructure Information Management System (PCIIMS), the system which catalogs PCII information.

Further, the collection of PCII involves the collection of personally identifiable information from and about contact points for each PCII site. PCIIP collects contact information in order to coordinate and validate a particular CII submission. The PCIIMS is the database which records the receipt, acknowledgement, validation, storage facility, dissemination, and destruction of PCII. PCIIP may then share the PCII with governmental organizations who are accredited by the PCIIP to receive PCII (see Sections 4.0 and 5.0 for further discussion).

This PIA examines the privacy implications for the PCIIMS.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The contact information consists of full name, business title, business e-mail address, and business telephone and fax number for the individual submitting the information.

Information regarding the critical infrastructure itself composes the rest of the submission. For example, subject material (telecom, nuclear, chemical, commerce, etc), plans related to site (disaster, emergency response, security, buffer zone protection, etc), location of facility, site and asset vulnerabilities, blueprints, and any other information relevant to the protection of a facility. For example, if the facility stores any amount of chemical matter the submission would detail the amount, type, location, and storage of such material. The individual information for each site is different.

Additionally, each entry requires a Certification Statement. The Certification Statement certifies that the submitter believes the information meets the statutory requirements. Each entry also contains an express statement from the submitter officially requesting that the CII be protected.

1.2 From whom is information collected?

The PCII Program collects information from any private, critical sector organization that voluntarily submits their information to the PCIIP. The seventeen (17) critical sectors from which an organization may be qualified are described in the Homeland Security Presidential Directive/HSPD-7 which is published and

[2] The URL is https://www.dhs.gov/pcii. The appropriate link is in the upper right corner of the page.

may be viewed online at the url http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

1.3 Why is the information being collected?

Collecting administrative contact information from submitters of PCII supports the PCIIP mission of receipt, validation, protection, and dissemination of PCII. PCIIP limits the contact information collected to the amount of information necessary to coordinate and validate a particular PCII submission.

Collecting the PCII assists government entities in protecting the nation from, and aiding in response to, acts of terrorism, natural disasters, or other emergencies, as well as assisting in the identification of vulnerabilities. The collection of PCII in a central repository gives DHS and the PCII stakeholders across the country a comprehensive view of the nation's critical infrastructure. Such a comprehensive view enables quick and effective decision-making and communication should the need for response arise.

1.4 How is the information collected?

The information can be mailed, hand-delivered, sent via encrypted e-mail, or uploaded via a secure web site to the PCIIMS. DHS employees review the information contained in the submitting entity's PCIIMS submission form and the PCIIMS Certification Statement as it is inputted into the PCIIMS. The Certification Statement for PCIIMS is an acknowledgement from the submitter that the information presented meets the criteria of critical infrastructure information as defined in the Critical Infrastructure Information Act, the information was offered so voluntarily, and the information is not customarily contained within the public domain (per the statute; see Introduction).

Each submission is sent as a complete unit. The individual pieces of each submission are not divided and saved in different spaces. Each CII submission comes as a complete non-divisible package. This means that the PCII information is not divisible from the contact information, and vice versa. Contact information is not stored separately.

Established standard operating procedures require that the information be reviewed by a trained PCIIP employee to ensure the submission either does or does not qualify for PCII protection and to check for accuracy. Once the information has been processed by the PCIIP employee, only the Program Manager or Operations Manager of the PCIIP is able to validate the submission before it is stored as read-only in the PCIIMS.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The Critical Infrastructure Information Act of 2002 specifically authorizes this collection. The collection is done in accordance with the Final Rule, Procedures for Handling Critical Infrastructure Information (6 CFR 29).

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

PCIIP limits the information collected to the amount necessary to coordinate and validate a particular PCII submission. The contact information supports the greater requirement to acquire and analyze PCII. The scope of the information collected is appropriately limited according to this need.

Furthermore, all PCIIP user who receive PCII submissions, and by necessity process contact information, have received security clearance and the appropriate training regarding the use and handling of personally identifiable information.

Taken together these measures help to mitigate the risks of misuse of data.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

PCIIP and approved PCII users utilize PCII to prepare the nation for acts of terrorism, natural disasters, or other emergencies, as well as assist in the identification of vulnerabilities. Analysis of PCII is conducted by authorized PCII analysts within the PCIIP and potentially other authorized government users (see Sections 4.0 and 5.0).

PCII information is also used by Federal, state, and local governments in response to natural disaster recovery efforts. The PCIIP may communicate requests to submitting entities in support of the PCIIP mission of receipt, validation, protection, and dissemination of PCII. The contact information for PCII is considered part of the submission, and therefore, afforded the same protection as the rest of the data.

PCIIP uses contact information to contact the submitting entity with questions related to the PCII. This information, along with the PCII, will also be disseminated to analysts who have undergone PCII training.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No. Analysts will examine relationships between critical infrastructure sites in certain regions or sectors, but contact information is not analyzed in any way.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

DHS employees review the information contained in the submitting entity's submission and the Certification Statement as it is inputted into the PCIIMS. Established standard operating procedures require that the information be reviewed by a trained DHS employee to ensure the submission either does or does not qualify for PCII protection and to check for accuracy. Once the information has been processed by the DHS employee, only the Program Manager or Operations Manager of the PCIIP is able to validate the submission before it is stored as read-only in the PCIIMS.

The PCIIP does not verify the accuracy of each piece of PCII in the PCIIMS. As noted in sections 4 and 5 below, PCII will send information to other agencies whose expertise in certain critical sectors allows them to analyze the PCII sent to them. The agencies to which PCII is sent are free to verify any PCII information as it relates to their analysis or research.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

All uses of the information are specifically defined in the Final Rule and the System of Records Notice (see Section 6.0), as well as in narrative form in this PIA. The uses of the contact information are limited to the coordination and validation of a PCII response. Maintaining limited uses of personally identifiable information is mandated in the Critical Infrastructure Information Act § 201 (b)(15)(B) which states any information contained in a PCII database must comply with federal privacy law.

Additionally, PCIIP users are authorized to see only the information necessary for the completion of their duties. These role-based access measures help to mitigate potential misuse.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Until an approved records retention and disposal schedule is established, validated CII records will be retained indefinitely. DHS Records Officer authorized the following disposition for rejected applications: Return to submitter if requested, or destroy within 30 calendar days of making the final non-protection determination in accordance with provisions found in 6 CFR Part 29, or when no longer needed for current business, whichever is later.

PCIIP submitted a records checklist worksheet to DHS Headquarters. Upon receipt of a response, PCIIP will dispose of records according to the received instructions.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The PCIIP is currently working with DHS headquarters to receive review and a final determination of an appropriate retention schedule. After DHS headquarters proposes the schedule it will be submitted to NARA for final approval.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The PCIIP recognizes that the collection of PCII involves the collection of personally identifiable information. Because of the added risks associated with this collection PCII has taken steps to ensure that personally identifiable information is destroyed at the appropriately to eliminate unnecessary storage but also to allow the PCIIP to accomplish its mission.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Currently, the PCIIP does not share data with any internal DHS organizations. The PCIIMS is self-contained and is not connected to other systems or networks.

The PCIIP has partnered with the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) to begin developing programs for receiving, handling and using PCII in their respective critical infrastructure programs. Once internal organizations complete their certification to receive PCII this PIA will be updated.

4.2 For each organization, what information is shared and for what purpose?

Currently, the PCIIP does not share data with any internal DHS organizations.

4.3 How is the information transmitted or disclosed?

Because PCIIMS is a standalone system with no system inter-connects (except for the web-based submission form), information will be disclosed by hardcopy, CD ROM, or encrypted email.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Because the contact information is considered part of the PCII submission, a privacy risk will exist when PCIIP begins disseminating PCII to internal DHS organizations. The PCIIP has ensured that despite with whom DHS shares internally, all users must be authorized by the PCIIP to handle PCII; this ensures proper security measures and handling of the material, specifically the associated contact information.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

External organizations currently partnered with and accredited by the PCIIP include the following: Center for Food Safety and Nutrition (CFSAN); Nuclear Regulatory Commission (NRC); and the Homeland Security Offices of the states of Maryland, Arizona, Massachusetts, California, and Washington.

The PCIIP will continue to partner with federal, state, local, and tribal governments related to Homeland Security duties to begin developing programs for receiving, handling, safeguarding, and using PCII in their respective critical infrastructure programs. The PCIIP will accredit external organizations to receive PCII. External governmental entities may not receive PCII until they are accredited.

5.2 What information is shared and for what purpose?

The information potentially disclosed to external partners will include specific PCII per the request of the authorized entity and the Point of Contact information respective to that PCII.

5.3 How is the information transmitted or disclosed?

Because PCIIMS is a standalone system with no system inter-connects (except for the web-based submission form), information will be disclosed by hardcopy, CD ROM, or encrypted email.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

A Memorandum of Agreement (MOA) exists between DHS and all external organizations with which information is shared. The MOA is comprehensive and clearly defines the scope of the information being shared. Additionally, the Final Rule for Procedures for Handling Critical Infrastructure Information (1 CFR Part 29) outlines information sharing. The MOA templates are attached as Appendices A (for Federal agencies) and B (for state agencies).

5.5 How is the shared information secured by the recipient?

Information shall be secured by the recipient in accordance with the security defined in the Final Rule for Procedures for Handling Critical Infrastructure Information (1 CFR Part 29).

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

PCII authorized users are trained and are responsible for ensuring the proper use and protection of the data. The PCIIP has established a computer based training that is necessary for any individual internal or external to DHS to handle PCII.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

A privacy risk exists when disseminating PCII to external DHS organizations because the contact information is considered part of the PCII. The PCIIP has ensured that despite with whom DHS shares internally, all users of PCII must be authorized by the PCIIP; therefore ensure proper security measures and handling of the material. The MOA and the Final Rule outline appropriate procedures for the sharing of PCII.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act statement on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The information being submitted to the PCIIP must be done so voluntarily by the individual submitting the information. Notice to the individual submitting the information is described in the Final Rule for Procedures for Handling Critical Infrastructure Information (1 CFR Part 29). PCIIMS is not a System of Records under the Privacy Act therefore no SORN has been published.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Entities that submit PCII and associated personal contact information to DHS do so voluntarily and DHS informs them of that fact. The PCIIP may need to contact a submitter for additional information in order to complete a validation of submitted material. The submitter can decline to provide any additional information or may withdraw the submission before it is validated. The PCIIP does not accept anonymous submissions.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The uses of PCII are outlined in the CII Act of 2002 and in the implementing regulation, Final Rule for Procedures for Handling Critical Infrastructure Information (1 CFR Part 29). By voluntarily submitting information, the individual is consenting to its use for the purposes found in the Critical Infrastructure Information Act and the Final Rule. The PCII submission includes a Certification Statement where the submitter certifies the information is voluntarily provided, as defined in the CII Act, for the purposes of the CII Act.

By voluntarily engaging in the PCII Program, and by submitting the contact information, submitters grant consent concerning how information contained within the PCIIMS is used.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The notice provided to entities submitting PCII is robust. This PIA and the Final Rule provide detailed notice regarding the use of any personally identifiable information provided. Once an entity chooses to submit PCII information they are aware of the extent of the information required, including the limited amount of contact information collected and the limited use of the contact information.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Once the PCII and submitter's contact information are input into the PCIIMS, it is designated as part of the entire PCII submission. As such, it is protected and only authorized users will have access to the information. Individuals do not have direct access to their own information but can request updates or changes to their previously submitted information.

7.2 What are the procedures for correcting erroneous information?

Individuals should notify the PCII Program Manager of any erroneous information found in the entity's contact information. Currently, the only method available for correcting erroneous information is deletion of the submission containing erroneous information and the creation of a new entry.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals do not have direct access to their own information but can request updates or changes to their previously submitted information. Any change to an individual's information may be done so by contacting the PCIIP office. Notice to the individual submitting the information is described in the Final Rule for Procedures for Handling Critical Infrastructure Information (1 CFR Part 29).

7.4 If no redress is provided, are alternatives available?

Opportunities for correction are available.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

PCIIP provides ongoing opportunities for submitting entities to edit or change the contact information submitted with the PCII submission. By contacting the PCIIP directly entities may update the person listed as the contact for the PCII or edit the information initially submitted.

Because the contact information is secondary to the PCII itself, the opportunities provided are sufficient to mitigate any potentially inaccurate information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

PCIIMS developers and maintenance administrators are employees or contractors of DHS who have privileged access to the PCIIMS Contract employees must sign a PCII Non-Disclosure Agreement, have a need-to-know, and contracts must be modified to include a PCII Clause as determined by the PCIIP. User requirements are the same as for PCII Authorized Users.

There is no public user access to the PCIIMS and, therefore, no public access to PCII or the related contact information.

8.2 Will contractors to DHS have access to the system?

Yes. DHS contractors will have access to the system. Any one with access to they system will have appropriate clearance. See Question 8.1.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. User access is restricted based on the job duties of each person working with PCIIMS. See Question 8.1.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Statutory guidelines provide that the Under Secretary for National Protection and Programs or the Under Secretary's designee, may choose to provide or authorize access to PCII when it is determined that this access supports a lawful and authorized government purpose as enumerated in the Critical Infrastructure Information Act of 2002, other law, regulation, or legal authority. Any disclosure or use of PCII within the Federal government is limited by the terms of the Critical Infrastructure Information Act of 2002.

The PCII Program Procedures Manual, PCII Systems Security Plan, and 6 CFR 29 document the criteria, procedures, controls, and responsibilities regarding access.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The PCIIP has several policies and guidelines provided for in the System Security Plan (SSP) to ensure that security controls are working properly. The policies and guidelines are listed in the PCIIMS Security Plan manual. PCII authorized users undergo PCII training as outlined in the PCII Accreditation Guide. PCIIMS administrators review security event logs daily per the PCII System Security Plan. The PCIIP conducts a NIST 800-26 Self Assessment on a yearly basis.

Additionally, the system is required to undergo Certification and Accreditation every 3 years and is reviewed by the National Protection and Programs Directorate's CIO Security Staff.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The integrity of PCIIMS data is maintained by strict adherence to technical and administrative controls. Technical controls include standard access control lists and system audit logs, all of which are documented in the Systems Security Plan. Administrative controls include end-user training on handling and safeguarding procedures and system auditing Standard Operating Procedures.

PCIIMS administrators review security event logs daily per the PCII System Security Plan.

The PCIIP conducts a NIST 800-26 Self Assessment on a yearly basis.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

PCII authorized users undergo PCII training as outlined in the PCII Accreditation Guide. All PCII authorized users are required to be trained and enforce the guidelines set forth in the PCII Systems Security Plan, Accreditation Guide, Standard Operating Procedures, and other applicable governing documents.

PCIIMS users consist of validators, senior validators, Program Manager, and Operations Manager who have full read-, write- and delete-accesses to the PCIIMS User requirements are the same as for PCII Authorized Users.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The PCIIMS has an Authority to Operate, received October 2004, from the DHS (formerly IAIP) Designating Approving Authority. The National Preparedness and Programs Directorate will issue a renewed ATO in 2007.

The PCIIMS follows the following policies, practices, guidance and legal requirements for this process:

1. DHS 4300 - IT Systems Security - Sensitive Systems Pub - Volume I Part A
2. Federal Information Security Management Act of 2002 (FISMA)
3. OMB Circular A-130 Appendix III, Security of Federal Automated Information Systems
4. Computer Security Act of 1987
5. OMB Circular A-11, Preparation and Submission of Budget Estimates
6. Presidential Decision Memorandum (PDD-63), Critical Infrastructure Protection
7. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Security Metrics Guide for Information Technology Systems

The PCIIP and the National Preparedness and Programs Directorate Information System Security Managers have a risk assessment on file. The PCIIP is a part of the National Preparedness and Programs Directorate thus PCIIP has its own Program Manager. This was conducted in 2004. Risks are continually being assessed on the program through an established Risk Management process for the program.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

PCII has met the criteria for Certification and Accreditation established by the DHS Chief Information Security Officer and the Chief Information Officer. By meeting these standards, specifically utilizing role-based access, the PCIIP can minimize any risk of misuse of data and ensure against intrusion attacks.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

The system was built from the ground up. The PCII MS is self-contained and not connected to other systems or networks.

The PCII MS includes the following features:

- Prominent links to specific content identified as being of particularly high interest;
- Search and retrieval capabilities based on keywords and data content;
- Search and retrieval capabilities based on the domain-specific taxonomy and meta tags;
- Collaborative tool suite such as message boards and calendars;
- Directory of subject-matter experts for each domain; and
- Security measures to protect against unauthorized access and usage.

Specifically, the system is designed with the following specifications:

- The application is web-based. The portal application was designed using ASP.net.
- The information content is stored on a Windows 2003 server running an Oracle 9i database and a file server.
- The portal was designed and built on-site at LMIT. The system will be transferred to DHS servers at DHS's request. Initially the system will be developed based on access through the Internet.

Virus protection controls are integrated in the DHS approved C&A "DHS Gold Image" baseline desktop image.

The PCII A-LAN Workstations and Servers use Symantec Antivirus software for virus protection. Update

mechanisms are controlled by the DHS CIO.

The virus scanning software is set up to automatically scan any file that is accessed (including when a file is downloaded) by the user from any drive.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The PCIIMS IT infrastructure is centrally located on site in the PCII offices in the secure server room, and is self-contained without connectivity to any other system. All 7 PCIIMS workstations are located in the PCIIP suite of offices at LMIT. All PCIIMS servers have been hardened against unauthorized access or operation by DHS CIO personnel using accepted DHS standards.

The PCII MS processes information treated as Sensitive But Unclassified (SBU) and For Official Use Only Information (FOUO). PCII data is exempt from public disclosure under the FOIA. The PCII MS is the focal point for the federal government to receive, validate, manage, and disseminate CII that is voluntarily submitted.

9.3 What design choices were made to enhance privacy?

No changes have been made to the system architecture, hardware, software or implementation plans as a result of this privacy impact assessment.

Conclusion

In conclusion, PCII is collected via voluntary submissions from the private sector through the use of PCII MS. These data are than classified as PCII, which can be distributed to Authorized Users in government entities to protect the nation from terrorist attacks, assist in the identification of vulnerabilities, aid in a response when an attack is under way, and to help state and local governments in recovery efforts.

Each entry into the database is composed of data regarding the submitting entity's critical infrastructure and the contact information for the submitting entity. The contact information consists of full name, title, e-mail address, telephone and fax number for the individual submitting the information. All information submitted by the participant organization is provided on a voluntary basis; users are neither compelled nor required to provide personal information.

Responsible Officials

Laura Kimberly
Protected Critical Infrastructure Information Program
National Protection and Programs Directorate
703-288-3550

Approval Signature Page

Original signed and on file with DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

Department of Homeland Security Memorandum of Agreement with Federal Agencies for Access to

Protected Critical Infrastructure Information

1. Parties: The parties to this Memorandum of Agreement (MOA) are the Department of Homeland Security, through its Protected Critical Infrastructure Information Program Office (hereinafter referred to as "DHS"), and the _____ (hereinafter referred to as the "Recipient").

2. Authorities: DHS is authorized to enter into this MOA under the Critical Infrastructure Information Act of 2002, Subtitle B of Title II of the Homeland Security Act of 2002, 6 U.S.C. §§131-134 ("CII Act"), and 6 C.F.R. Part 29.

3. Purpose: The purpose of this MOA is to set forth the agreed terms and conditions under which Protected Critical Infrastructure Information (PCII) is provided to the Recipient. The CII Act, establishes the statutory requirements for the submission and protection of critical infrastructure information ("CII"). Under 6 U.S.C. § 133(e), DHS is required to establish uniform procedures for the receipt, care, and storage of PCII by Federal agencies. These procedures have been set forth in the Code of Federal Regulations at 6 C.F.R. Part 29. Specifically, 6 C.F.R. 29.8 outlines the requirements for sharing information with Federal agencies and Federal contractors. The PCII Program Procedures Manual provides further guidance, and requires that Federal agencies that obtain PCII from and through the PCII Program Manager (PM) enter into an MOA. This MOA fulfils that requirement. Furthermore, the PCII Program Office must accredit recipient entities before they can access PCII.

4. Responsibilities:

A. DHS will:

(i) Accredit the Recipient and appoint a PCII Officer and PM designee, if applicable, provided that the entity has satisfied the accreditation requirements set forth in Section 4.B.(ii) below.

(ii) Provide access to PCII to the Recipient for the purposes set forth in the CII Act and under the conditions outlined in this MOA;

(iii) Validate CII or pre-validate categorical inclusions of certain types of CII as PCII;

(iv) Delegate, as appropriate and necessary, certain functions of the PCII Program Office, to an identified PM designee;

(v) Obtain written consent, as applicable, from the person or entity that submitted the information or on whose behalf the information was submitted, before that information is disclosed by the Recipient to an unauthorized party or for an unauthorized use;

(vi) Provide applicable procedures and guidelines for the receipt, safeguarding, handling and dissemination of PCII;

(vii) Train the Recipient's PCII Officer(s) and PM's designee(s) and be available for consultation and guidance;

(viii) Provide content and format for training of individuals seeking authorization to access PCII; and

(ix) Assist the Recipient in issuing any alerts, advisories and warnings that require DHS' prior approval as set forth in 6 C.F.R. 29.8(e).

B. The Recipient will:

(i) Warrant and agree that each of its employees and contractors who will have access to PCII is familiar with, will be trained in, and will comply with, the statutes, regulations, and rules that address PCII

set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and other relevant guidance issued by the PCII PM, and will periodically check such guidance for updates and amendments;

(ii) Use its best efforts, and cooperate with the PCII Program Office, to become accredited as expeditiously as possible, by:

(a) Submitting an application
(b) Signing this MOA
(c) Nominate a PCII Officer
(d) Nominate a PCII PM designee, if applicable
(e) Ensuring that the the PCII Officer and the PCII PM designee complete their training
(f) Completing the self-inspection plan
(g) Ensuring that the PCII Officer certifies any contractors
(h) Ensuring that any contractors sign a Non-Disclosure Agreement in the form prescribed by the PCII Program Office

(iii) Use any PCII provided to it only for the purposes set forth in the CII Act at 6 U.S.C. §133(a)(1), and, in accordance with 6 C.F.R. 29.3(b), will not use PCII as a substitute for the exercise of its own legal authority to compel access to or submission of that same information, and further, will not use PCII for regulatory purposes without first contacting the PCII Program Office;

(iv) Nominate one or more persons to be PCII Officers, all of whom shall be familiar with and trained in the receipt, safeguarding, handling and dissemination requirements for PCII as set forth in 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and any other guidance issued by the PCII PM;

(v) Nominate, if applicable, a PCII PM designee to undertake certain PCII Program Office responsibilities in the context of a categorical inclusion program;

(vi) Upon request from DHS, immediately take such steps as may be necessary to return promptly all PCII, including copies, however made, to DHS;

(vii) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its employees, and will refer violations of the CII Act and 6 CFR Part 29 or other applicable law to appropriate authorities for prosecution;

(viii) Immediately report all compromises of PCII and violations of applicable procedures to the PCII PM and cooperate with any investigation that may be initiated;

(ix) Ensure that information it receives from DHS that is marked "Protected Critical Infrastructure Information" shall be controlled as required and is used only for allowed purposes; that records of disclosure of PCII are maintained within that entity, as appropriate and that any PCII markings shall not be removed without first obtaining authorization from the PCII PM or the PCII PM's designee;

(x) Except as provided for in 6 C.F.R.29.8(f), or in exigent circumstances as provided for in 6 C.F.R. 29.8(e), not further disclose PCII to any other party without the prior approval of the PCII PM or the PCII PM's designee, or by order of a court of competent jurisdiction;

(xi) Before sharing with contractors :

(a) Certify that contractors and subcontractors are performing services in support of the CII Act;

(b) Ensure that each employee of a consultant, contractor, or subcontractor who will have access to PCII has signed an individual non-disclosure agreement approved of, or provided by, DHS, and is familiar with, will be trained in, and will comply with the provisions of this MOA, the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and other relevant guidance issued by the PCII PM; and

(c) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its consultants, contractors and subcontractors and will refer violations of law to appropriate authorities for prosecution.

(xii) Ensure that contractors have agreed by contract to comply with all of the requirements of the PCII Program;

(xiii) Fully comply with any requests, whether scheduled or unscheduled, by the PCII PM or the PCII PM's designee, to review the Recipient's compliance with the terms of this MOA, and will take any corrective action recommended;

(xiv) Forward any submission of CII received by the Recipient that is not part of a categorical inclusion of CII to the PCII Program Office for validation;

(xv) Enter into any Agreements to Operate and/or System Requirements Documents required by the PCII Program Office in the context of a categorical inclusion or otherwise; and

(xvi) Notify and coordinate with DHS prior to responding to any requests for release of PCII under a court order, agency decision, the Freedom of Information Act, or any other statute or regulation.

5. Amendments: This MOA is permitted by statute and regulation and required by the PCII Program Procedures Manual. Should there be a change in any of these authorities, DHS will require conforming amendments to this MOA. This MOA can only be amended by an instrument in writing signed on behalf of both DHS and the Recipient.

6. Reimburseables: This MOA does not provide authority for any reimburseable expenditures, or funding. In the event that such authorization is required, DHS and the Recipient will, in a separate agreement, coordinate funding reimbursement through appropriate channels and will execute appropriate Reimbursable Agreements or other funding documents in accordance with the Economy Act and DHS procedures for such agreements including an Economy Act Determination & Findings.

7. Other Provisions: Nothing in this MOA is intended to conflict with current law or regulation. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

8. Effective Date and Termination Provisions: This MOA is effective as of the date of the last required signature. It continues until terminated in writing by either party. It may be terminated effective upon the delivery by any means of written notice of termination signed by an authorized DHS official. Unwillingness by the Recipient to agree to amendments required by DHS will constitute a basis for termination. If terminated, the Recipient agrees to promptly return all PCII that it has received to the PCII PM.

9. Original Memorandum of Agreement: The original of this document will be kept by the PCII PM. Copies may be made as necessary.

10. Points of Contact:

DHS:	Recipient:
Name	Name
Phone	Phone
Email	Email

Agreed to and Accepted By:

For The Department of Homeland Security

For _____
(Federal Agency)

By: Laura L.S. Kimberly

Title: PCII Program Manager

Signature

Date

By: _____
(Print Name)

Title: _____

Signature

Date

Appendix B

Department of Homeland Security Memorandum of Agreement with State Agencies for Access to

Protected Critical Infrastructure Information

1. Parties: The parties to this Memorandum of Agreement (MOA) are the Department of Homeland Security, through its Protected Critical Infrastructure Information Program Office (hereinafter referred to as "DHS"), and the _____ (hereinafter referred to as the "Recipient").

2. Authorities: DHS is authorized to enter into this MOA under the Critical Infrastructure Information Act of 2002, Subtitle B of Title II of the Homeland Security Act of 2002, 6 U.S.C. §§131-134 ("CII Act"), and 6 C.F.R. Part 29.

3. Purpose: The purpose of this MOA is to set forth the agreed terms and conditions under which Protected Critical Infrastructure Information (PCII) is provided to the Recipient. The CII Act, establishes the statutory requirements for the submission and protection of critical infrastructure information ("CII"). Under 6 U.S.C. § 133(e), DHS is required to establish uniform procedures for the receipt, care, and storage of PCII. These procedures have been set forth in the Code of Federal Regulations ("C.F.R.") at 6 C.F.R. Part 29. Specifically, 6 C.F.R. 29.8 outlines the requirements for sharing information with State and local government agencies and contractors. 6 C.F.R. 29.8(b) requires a State or local government entity to enter into an arrangement with DHS providing for compliance with 6 C.F.R. Part 29 and acknowledging the understanding and responsibilities of the recipient entity. The PCII Program Procedures Manual provides further guidance, and requires that State and local agencies that obtain PCII from and through the PCII Program Manager (PM) enter into an MOA. This MOA fulfils that requirement. Furthermore, the PCII Program Office must accredit recipient entities before they can access PCII.

4. Responsibilities:

A. DHS will:

(i) Accredit the Recipient and appoint a PCII Officer, provided that the entity has satisfied the accreditation requirements set forth in Section 4.B.(ii) below.

(ii) Provide access to PCII to the Recipient for the purposes set forth in the CII Act and under the conditions outlined in this MOA;

(iii) Validate and mark CII and disseminate it to the Recipient;

(iv) Obtain written consent, as applicable, from the person or entity that submitted the information or on whose behalf the information was submitted, before that information is disclosed by the Recipient to an unauthorized party or for an unauthorized use;

(v) Provide applicable procedures and guidelines for the receipt, safeguarding, handling and dissemination of PCII;

(vi) Train the Recipient's PCII Officer(s) and be available for consultation and guidance;

(vii) Provide content and format for training of individuals seeking authorization to access PCII; and

(viii) Assist the Recipient in issuing any alerts, advisories and warnings that require DHS' prior approval as set forth in 6 C.F.R. 29.8(e).

B. The Recipient will:

(i) Warrant and agree that each of its employees and contractors who will have access to PCII is familiar with, will be trained in, and will comply with, the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and other relevant

guidance issued by the PCII PM, and will periodically check such guidance for updates and amendments;

(ii) Use its best efforts, and cooperate with the PCII Program Office, to become accredited as expeditiously as possible, by:

(a) Submitting an application
(b) Signing this MOA
(c) Nominate a PCII Officer
(d) Ensuring that the the PCII Officer complete his or her training
(e) Completing the self-inspection plan
(f) Ensuring that the PCII Officer certifies any contractors
(g) Ensuring that any contractors sign a Non-Disclosure Agreement in the form prescribed by the PCII Program Office

(iii) Use any PCII provided to it only for the purposes set forth in the CII Act at 6 U.S.C. §133(a)(1), and, in accordance with 6 C.F.R. 29.3(b), will not use PCII as a substitute for the exercise of its own legal authority to compel access to or submission of that same information, and further, will not use PCII for regulatory purposes without first contacting the PCII Program Office;

(iv) Nominate one or more persons to be PCII Officers, all of whom shall be familiar with and trained in the receipt, safeguarding, handling and dissemination requirements for PCII as set forth in 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and any other guidance issued by the PCII PM;

(v) Ensure that any employees required by DHS to undergo a background check pursuant to 6 C.F.R. 29.7(b) submit any required paperwork to, and cooperate with, DHS;

(vi) Upon request from DHS, immediately take such steps as may be necessary to return promptly all PCII, including copies, however made, to DHS;

(vii) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its employees, and will refer violations of the CII Act and 6 C.F.R. Part 29 or other applicable law to appropriate authorities for prosecution, including any administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations and directives of the Recipient's jurisdiction;

(viii) Immediately report all compromises of PCII and violations of applicable procedures to the PCII PM and cooperate with any investigation that may be initiated;

(ix) Ensure that information it receives from DHS that is marked "Protected Critical Infrastructure Information" shall be controlled as required and is used only for allowed purposes; that records of disclosure of PCII are maintained within that entity, as appropriate and that any PCII markings shall not be removed without first obtaining authorization from the PCII PM;

(x) Except as provided for in 6 C.F.R.29.8(f), or in exigent circumstances as provided for in 6 C.F.R. 29.8(e), not further disclose PCII to any other party without the prior approval of the PCII PM, or by order of a court of competent jurisdiction;

(xi) Before sharing with contractors :

(a) Certify that contractors and subcontractors are performing services in support of the CII Act;

(b) Ensure that each employee of a consultant, contractor, or subcontractor who will have access to PCII has signed an individual non-disclosure agreement approved of, or provided by, DHS, and is familiar with, will be trained in, and will comply with the provisions of this MOA, the statutes, regulations, and rules that address PCII set forth in the CII Act, 6 C.F.R. Part 29, the DHS PCII Program Procedures Manual, and other relevant guidance issued by the PCII PM; and

(c) Consider any violations of procedures regarding PCII as matters subject to rules of conduct (including sanctions) that apply to its consultants, contractors and subcontractors and will refer violations of law to appropriate authorities for prosecution.

(xii) Ensure that contractors have agreed by contract to comply with all of the requirements of the PCII Program;

(xiii) Fully comply with any requests, whether scheduled or unscheduled, by the PCII PM, to review the Recipient's compliance with the terms of this MOA, and will take any corrective action recommended;

(xiv) Forward any submission of CII received by the Recipient to the PCII Program Office for validation;

(xv) Enter into any Agreements to Operate and/or System Requirements Documents required by the PCII Program Office; and

(xvi) Notify and coordinate with DHS prior to responding to any requests for release of PCII under a court order, agency decision, the Freedom of Information Act, or any other statute or regulation, including similar State and local disclosure laws that apply in the Recipient's jurisdiction.

5. Amendments: This MOA is permitted by statute and regulation and required by the PCII Program Procedures Manual. Should there be a change in any of these authorities, DHS will require conforming amendments to this MOA. This MOA can only be amended by an instrument in writing signed on behalf of both DHS and the Recipient.

6. Reimburseables: This MOA does not provide authority for any reimburseable expenditures, or funding. In the event that such authorization is required, DHS and the Recipient will, in a separate agreement, coordinate funding reimbursement through appropriate channels and will execute appropriate Reimbursable Agreements or other funding documents in accordance with the Economy Act and DHS procedures for such agreements including an Economy Act Determination & Findings.

7. Other Provisions: Nothing in this MOA is intended to conflict with current law or regulation. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

8. Effective Date and Termination Provisions: This MOA is effective as of the date of the last required signature. It continues until terminated in writing by either party. It may be terminated effective upon the delivery by any means of written notice of termination signed by an authorized DHS official. Unwillingness by the Recipient to agree to amendments required by DHS will constitute a basis for termination. If terminated, the Recipient agrees to promptly return all PCII that it has received to the PCII PM.

9. Original Memorandum of Agreement: The original of this document will be kept by the PCII PM. Copies may be made as necessary.

10. Points of Contact:

DHS:	Recipient:
Name	Name
Phone	Phone
Email	Email

Agreed to and Accepted By:

For The Department of Homeland Security

For _____
(State Agency)

By: Laura L.S. Kimberly

Title: PCII Program Manager

Signature

Date

By: _____
(Print Name)

Title: _____

Signature

Date