Privacy Impact Assessment
for the

Protected Critical Infrastructure Information Management System (PCIIMS) Final Operating Capability (FOC)

July 13, 2011

DHS/NPPD/PIA-006(a)

Contact Point
Tammy Barbour
Protected Critical Infrastructure Information Program
Office of Infrastructure Protection
National Protection and Programs Directorate
(703) 235-3656

Reviewing Official
Mary Ellen Callahan
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 (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP), Infrastructure Information Collection Division (IICD), facilitates the sharing of PCII between the government and the private sector. The Protected Critical Infrastructure Information Management System (PCIIMS) Final Operating Capability (FOC) is an Information Technology (IT) system and the means by which PCII submissions from the private sector are received and cataloged, and PCII Authorized Users are registered and managed. The PCII Program conducted this privacy impact assessment (PIA) to analyze and evaluate the privacy impact resulting from the consolidation of the PCIIMS Initial Operating Capability (IOC) functionalities into PCIIMS FOC, as well as the collection of limited personally identifiable information (PII) from the submitting individuals and PCII Authorized Users for contact purposes.

Overview

It is estimated that over 85 percent of the critical infrastructures within the United States are owned and operated by the private sector. Recognizing that the private sector was reluctant to share information with the federal government for fear that it could be publicly disclosed, Congress passed the Critical Infrastructure Information Act of 2002 (6 USC §131 *et seq.*) (CII Act). This Act provides Critical Infrastructure Information (CII) with protection from public release and disclosure. It also charges the PCII Program Office 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, such as subject material (telecom, nuclear, chemical, commerce, etc.), plans related to a 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.

CII, which becomes PCII upon completion of the submission and validation process, is defined in the CII Act 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 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.[1]

Entities who share CII with DHS include state and local government entities, private entities or persons, or Information Sharing and Analysis Organizations acting on behalf of their members or otherwise. These entities who submit CII to DHS for protection as PCII are referred to as "submitters" throughout this PIA. Collecting 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. Collecting administrative contact information from submitters of PCII supports the PCII Program mission of receipt, validation, protection, and dissemination of PCII. The PCII Program limits the contact information collected to the amount of information necessary to coordinate and validate a particular CII submission. PCII protection exempts the information from the Freedom of Information Act (FOIA), state and local disclosure laws, and use in civil litigation. The submitter's contact information is considered part of the CII submission, and therefore, is afforded the same protection as the rest of the data.

In September 2006, DHS further defined and developed the PCII Program through an implementing regulation, "Procedures for Handling Critical Infrastructure Information; Final Rule," 6 CFR Part 29 (Final Rule). This regulation provides protections, defines terms, and outlines handling and use limitations, as well as the submission and sharing process of CII with DHS. The Final Rule also requires the use of PCIIMS to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of PCII. PCIIMS FOC consolidates and integrates functions that previously existed as part of the two separate PCIIMS IOC systems, PCIIMS eSubmissions and Workflow and the Program Administrative Support (PAS) system. PCIIMS FOC consolidates the two systems into one fully integrated system with three main functions: (1) eSubmissions is an electronic submission functionality enabling private sector critical infrastructure personnel to submit information electronically for protection; (2) Workflow is a functionality enabling validation and protection of the PCII; and (3) User Management is where PCII Authorized Users are registered, trained, authorized, and their accounts managed.

PCIIMS FOC has three user groups: (1) submitters of CII for PCII protection (e.g., state, local, or private sector entities); (2) PCII Program personnel who are DHS employees or contractors that perform the submission review, processing, validation, and administration; and (3) PCII Authorized Users who use the PCII for analyses, assessments, and other tasks in support of their homeland security duties (may include individuals outside of DHS). All PCII Program personnel with access to the PCIIMS FOC system are required to be PCII Authorized Users. However, to maintain accountability of the system and its data, not all PCII Authorized Users have direct access to the PCII contained in the PCIIMS FOC system. Only PCII Program personnel have direct access to PCII maintained within PCIIMS FOC, and PCII is disseminated to PCII Authorized Users by approved PCII Program personnel only after all sharing

[1] 6 USC §131(3)(A)-(C)

requirements are met, including the establishment of the PCII Authorized User's need to know. Submitters are not required to be PCII Authorized Users since they are submitting CII to be considered for protections as PCII and are not using PCII for homeland security duties.

As described in the CII Act and the Final Rule, PCII submissions will include PII from submitters. The PCII Program Office uses the contact information to coordinate and validate, as necessary, a particular CII submission. The PCII Program also collects PII during the PCIIMS FOC user registration process to manage PCII Authorized Users with access to the system. In both instances, the PII collected is limited to business contact information, such as:

- name;
- company;
- business email;
- business phone; and
- business address.

CII/PCII Submission Process

The submitter may share CII with DHS using one of the following methods: (1) directly to PCIIMS FOC through the eSubmissions functionality; or (2) manually via email, regular mail, fax, orally, in-person, etc. All information the PCII Program collects must be accompanied by an express statement and a signed certification statement from the submitter. If a submitter opts to submit information orally, the submitter must follow up with an express statement, certification statement, and documents that memorialize the oral submission, and a PCII Program official will input and upload the submission into PCIIMS FOC on the submitter's behalf

The express statement affirms that:

- The information is voluntarily submitted to the federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.

The certification statement affirms that:

- To the best of the submitter's knowledge, information, and belief, the information being submitted is not customarily in the public domain.
- The submitter attests that information is not being submitted in lieu of a regulatory requirement.
- The submitter is authorized to submit this information to be considered for protection under the Critical Infrastructure Information Act of 2002.

Within PCIIMS FOC, the tracking of a CII submission begins with eSubmissions, and is managed through the Workflow and User Management applications.

eSubmissions

The eSubmissions functionality collects submitter information (business contact information), as well as information about the CII data being submitted to DHS for protection, and then enables the submitter to upload various supporting documents and files. The eSubmissions application scans the submitted documents for viruses and malware prior to the submission being accepted and inputted into the Workflow application. If the virus check fails, the submission is not accepted and the submitter must resolve the document issue prior to resubmitting. Once the submission is accepted, eSubmissions provides a unique submission identification number to the submitter.

Workflow

The submission identification number follows the submission through the entire PCII submission, validation, approval, and storage process, which occurs in the Workflow application. The Workflow functionality is an information management application, logging CII submissions (either inputted directly from eSubmissions or via a manual entry by the PCII Program personnel) and then enabling the PCII Program personnel to perform a validation process. CII submitted to the PCII Program is not restricted to any particular format. Therefore, during processing and validation, PCII Program personnel review the submission for specific PCII requirements. They also have the ability to systematically generate letters to send to a submitter for various information requests or status updates regarding the submission. Workflow creates a log of such correspondence, in addition to allowing PCII Program personnel to input their comments about a submission, such as administrative notes or status updates. Once a submission undergoes the PCII validation workflow, the PCII Program will either validate the submission as PCII, reject, or withdraw the submission. If the submission is validated as PCII, the Workflow application adds required headings, markings, cover pages, etc. to all of the applicable data, per the PCII Final Rule requirements, and stores the newly designated PCII submission in the PCIIMS FOC database indefinitely or until the original submitter requests the PCII protection to be withdrawn. If the submission is rejected or withdrawn, the system automatically removes all data related to the submission, with the exception of the submitter's certification and express statements that are required as part of the CII submission process. This retention practice conforms to the National Archives and Records Administration (NARA) records retention schedule for PCIIMS FOC.

PCII Program personnel can also perform limited search and reporting capabilities on the CII and PCII submissions, including the reporting of first-level dissemination of PCII retained in the application. This Workflow functionality is only accessible from the DHS A-LAN, requiring a separate login from eSubmissions and User Management functions. The search results and report information are only accessible to the PCII Program personnel. No other PCIIMS FOC system users have access.

User Management

The User Management functionality enables the PCII Program to manage its PCII Authorized Users. The PCII Program has a requirement to maintain a central repository of all users who are authorized to access PCII. In order for a user to become a PCII Authorized User, the user must complete several requirements, including: certify the performance of homeland security duties, sign a non-disclosure agreement (non-Federal employees only), be certified for access (contractors only), and complete PCII training and subsequent exam. The PCII Program relies heavily on a distributed user

management framework consisting of PCII Officers within the many Federal, State, local, and tribal government organizations, which access PCII, to oversee and manage the PCII Authorized User community. The User Management application aids the PCII Program and designated PCII Officers in the oversight and management of the PCII Authorized User community by enabling user registration, user screening, training delivery and certification, user notification, account maintenance, and PCII Program and Officer administrative tasks. All PCII Authorized Users are required to take PCII Authorized User training, which covers the consequences of loss or misuse of PCII data, including criminal and administrative penalties. After completing the PCII Authorized User training, a user may access PCII for up to one year and receives a unique PCII Authorized User number and a PCII Authorized User certificate. The User Management application automatically notifies users via email before their one year PCII Authorized User status expires. To keep their PCII Authorized User status, the user must complete refresher training prior to the expiration date. To assist PCII Authorized Users in identifying other current PCII Authorized Users, before sharing PCII, the User Management application also includes an Authorized User number check feature, whereby one Authorized User can enter another user's number and the feature will return that person's name, PCII Authorized User status, expiration date, organization, and employer (if contractor).

Partnership Systems

The PCII Program also collects data on PCII submissions through partnership systems. Partnership systems are systems managed by PCII Officers in other federal agencies who have received an elevated training level for handling PCII. These systems collect, protect, and disseminate original PCII in a format that has been pre-approved by the PCII Program. PCII Officers in other federal agencies share their data with DHS either by granting the PCII Program access to the partnership system, sending a file by email, or by transmitting a CD or hardcopy of the information by mail, if necessary. Each partnership system is required to meet the PCII requirements of the final rule and is covered by an individual memorandum of understanding (MOU) between the system owner and PCII Program, which details how information is collected, protected, and disseminated from the partnership system (See Appendices A and B).

PCII Program personnel may input PCII submission metadata records from approved PCII partnership systems into the PCIIMS FOC Workflow application in a standardized XML format. Workflow stores these metadata records and enables the PCII Program to execute searches and generate reports on the data.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 201(d) of the Homeland Security Act (6 USC §11(d)) and the CII Act authorize this collection, and the collection is done in accordance with the final rule.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The PII about Submitters is not covered by the Privacy Act because the information is not retrieved by personal identifier as required by the Privacy Act. This information is covered and protected under the CII Act.

The PCII Program Office collects PII for the purpose of granting access to the PCIIMS FOC system. This collection of information is covered by the DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The PCIIMS FOC system has a System Security Plan (SSP) that is part of the new system C&A package. This C&A package is currently undergoing review, and an ATO will be granted before the system goes live (expected to go live in July 2011). The current production system (PCIIMS IOC) has an ATO that was signed September 9, 2010 and is valid for three years.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The following records schedules cover PCIIMS FOC and have been approved by NARA: Job No. N1-563-08-36, which covers the PCIIMS system, and N1-563-04-9, which covers CII submissions.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Per 6 CFR 29, Volume 71, Number 170: "Under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501-3520 (PRA), a Federal agency must obtain approval from the OMB for each collection of information it conducts, sponsors, or requires through regulations. The Final Rule for the Procedures for handling Critical Infrastructure Information does not contain provisions for collection of information, does not meet the definition of 'information collection' as defined under 5 CFR Part 1320, and is therefore exempt from the requirements of the PRA. Accordingly, there is no requirement to obtain OMB approval for information collection."[2] However, the final rule does not exempt partnership systems, and as such, each partnership system may be required to follow PRA guidelines.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

[2] Procedures for Handling Critical Infrastructure Information; Final Rule, Preamble §V(H), 6 CFR part 29 (2006).

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The eSubmissions functionality of PCIIMS FOC collects limited contact information from individuals submitting CII to DHS. The contact information consists of full name, business title, business e-mail address, business telephone, and business fax number and is used by DHS to contact the submitter in the event there are any questions about the submission during the verification process.

Information regarding the critical infrastructure itself comprises the rest of the submission and does not include PII. The types of information that PCIIMS FOC collects may include the subject material (e.g., telecom, nuclear, chemical, commerce, etc.), plans related to a site (e.g., disaster, emergency response, security, buffer zone protection, etc.), location of facility or site, asset vulnerabilities, blueprints, and/or any other information relevant to the protection of a facility. The types of information PCIIMS collects are specific to each site. For example, if the facility stores any amount of chemical matter, the submission would detail the amount, type, location, and storage of such material.

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.

The user management functionality of PCIIMS FOC also collects business contact information (e.g., name, email, business address, business phone, and organization) on personnel that are PCII Authorized Users. Future PCIIMS FOC functionality may include the ability for PCII Authorized Users to search for other PCII Authorized Users by their business contact information.

2.2 What are the sources of the information and how is the information collected for the project?

The original source of information that the PCII Program collects is always the submitter. Submitters may submit CII for protection as PCII to DHS through one of the following methods: (1) directly to PCIIMS FOC through the eSubmissions functionality; or (2) manually via email, regular mail, fax, orally, in-person, etc., in which case a PCII Program official inputs and uploads the submission into PCIIMS FOC on the submitter's behalf. In the case of faxed or hard copy submissions, a PCII Program official scans and uploads the information to PCIIMS FOC. Original, hard copy documents are stored in a safe.

When information is not collected directly by the PCII Program, it is collected through partnership systems, which are systems managed by PCII Officers in other federal agencies who have received an elevated training level for handling PCII. Partnership systems collect, protect and disseminate original PCII in a format that has been pre-approved by the PCII Program. The data is shared with the PCII Program office either by granting access to the partnership system, sending a file by email, or by transmitting a CD or hardcopy of the information by mail, if necessary. Each partnership system is required to meet the PCII requirements of the Final rule and is covered by an individual memorandum of understanding (MOU) between the system owner and the PCII Program, which details how information is collected, protected and disseminated from the partnership system (See Appendices A and B).

Additionally, the User Management functionality of PCIIMS FOC collects business contact information (e.g., name, email, business address, business phone, and organization) directly from individuals that are applying to be PCII Authorized Users.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

All information collected by PCIIMS FOC is provided by the individual, not collected from commercial sources or otherwise obtained from public records.

2.4 Discuss how accuracy of the data is ensured.

The PCII Program office verifies the submitter's contact information at the time of the CII submission. PCII Program personnel review the information contained in the submitting entity's submission and express and certification statements, as it is inputted into the eSubmissions functionality of the PCIIMS FOC. In the case of an oral submission, the submitter must follow up with written documents to memorialize the submission, which are then reviewed by PCII Program personnel. Upon receipt and review of the submission, the PCII Program issues an acknowledgment to the submitter, at which point the submitter may verify the accuracy of their contact information.

Established standard operating procedures require that the information be reviewed by a trained federal 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 employee, only the Program Manager of the PCII Program Office is able to validate the submission before it is stored as read-only in the PCIIMS FOC.

Once the data is stored as PCII, no changes are made to the submission, including the contact information, unless DHS is specifically notified to do so. Notifications would include, for example, a submitter contacting the help desk to update their information or to withdraw protections from their submissions. Notifications are also sent to PCII Authorized Users via email to conduct various PCIIMS FOC user management activities, including training renewal notices and password resets. Responses to these notifications ensure that the contact information within PCIIMS FOC is up to date. A non-response would trigger the PCIIMS FOC system to remove the user, as required by the PCII Program policy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more PII than is needed will be collected and retained.

Mitigation: The PCII Program Office limits the information collected to only that business contact information necessary to coordinate and validate a particular PCII submission or to perform PCII Authorized User management activities. Information entered is limited by the fields that are available in the user management functionality of PCIIMS FOC.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The PCII Program Office and PCII Authorized Users utilize PCII to prepare the nation for acts of terrorism, natural disasters, or other emergencies, as well as to assist in the identification of vulnerabilities. PCII Authorized Users may include PCII Analysts within the Department's PCII Program Office and other authorized government users to include federal, state, local, or tribal agents and their contractors.

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

The PCII Program Office uses contact information to contact the submitting entity with questions related to the CII submission. Once protected, the PII and CII combine to form PCII. The PCII is disseminated only to PCII Authorized Users with the need to know. PCII Authorized Users are identified by their unique user number. Authorized Users' PII is maintained by PCIIMS solely to contact the individual for PCII Program office oversight activity.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

While PCII Analysts and others examine relationships between critical infrastructure sites in certain regions or sectors, submitter and Authorized User contact information is not analyzed in any way.

3.3 Are there other components with assigned roles and responsibilities within the system?

The PCII Program Office shares PCII with PCII Authorized Users, as necessary, to support mission requirements. All PCII Authorized Users must demonstrate a valid need to know before receiving any protected information. Additionally, any organization that develops a relationship with the PCII Program Office must develop programs for receiving, handling, and using PCII in their respective critical infrastructure programs. They also must complete certification to receive PCII. A list of components or directorates within the Department with which the information is shared is maintained by the PCII Program Office.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse of PII collected as part of a CII submission.

Mitigation: This risk is mitigated in that the entire submission (including PII), once validated, is protected as PCII. Therefore, any PII collected is afforded the same protection as PCII, and the uses of PCII are specifically defined in the Final Rule. DHS limits the use of the contact information to the coordination and validation of a PCII response. All PCII Authorized Users who receive PCII and, by necessity, process contact information, receive PCII training. All DHS employees are required to complete annual privacy training, which covers the appropriate use and handling of PII. Additionally, PCII Program users are authorized access to only the information necessary for the completion of their duties. These role-based access measures help to mitigate potential misuse of PII.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Entities that submit CII and associated business contact information to DHS do so voluntarily, and DHS requires that each submission is accompanied by a signed certification and express statement, ensuring the submitter acknowledges the voluntary nature of the program. Entities, including the individual submitters, are provided with specifics about the program in the Final Rule. The PCII Program Office provides notice at the time of collection to individuals applying to be authorized users in the form of a Privacy Act statement, in this PIA, and the DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882).

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The PCII Program Office may need to contact a submitter for additional information in order to complete a validation of submitted material. In such instances, the submitter can decline to provide any additional information or may withdraw the submission before it is validated. The PCII Program Office does not accept anonymous submissions. If a submitter declines to provide their contact information that would indicate that they choose not to participate in the PCII Program.

PCII Authorized Users are not provided ability to specifically consent to particular uses. Individuals who choose not to provide all the information necessary, may not be approved as a PCII Authorized User.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that submitters or PCII Authorized Users will not be provided with adequate notice as to how their PII will be used.

Mitigation: This risk is mitigated in that the PCII Program has a direct relationship with both submitters and PCII Authorized Users and ensures that notice provided to individuals is robust. For example, this PIA and the Final Rule provide detailed notice regarding the use of any PII provided to the PCII Program office. Once an entity chooses to submit information, they are aware of the extent of the information that is required, including the limited amount of contact information collected and the limited use of the contact information. Additionally, submitters of CII sign certification and express statements, certifying that information submitted to the PCII Program is done so voluntarily by the individual.

For Authorized Users, the PCII Program Office provides notice to individuals in the form of a Privacy Act statement at the time of collection, and further notice is provided in the DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882). This notice also ensures that individuals are aware of how to access and correct their records maintained within PCIIMS FOC.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

DHS worked with the National Archives and Records Administration (NARA) to develop a retention schedule for the records maintained within PCIIMS FOC. This retention schedule was designed to protect PCII maintained within the system to the maximum extent practicable and consistent with the CII Act. CII submissions that are validated as PCII are maintained indefinitely or until the PCII Program office determines that information may no longer be protected under the CII Act, in which case the status is changed from PCII to non-PCII. Status changes occur when: (1) the submitter requests in writing that the information no longer be protected under the CII Act; or (2) the PCII Program office determines that the information was, at the time of the submission, customarily in the public domain.

CII submissions that are rejected are removed from the system with the exception of the certification and express statements and reason for rejection, which are maintained for administrative tracking purposes. Similarly, when status changes occur, the substantive information from the submission is removed from the system, and only the certification and express statements, reason for removal, and submission metadata are retained, as outlined in the NARA guidelines. When information no longer requires protection, a submitter may request that the information be returned to them. Otherwise, it is removed from PCIIMS FOC and destroyed.

Per NARA guidance, the PCII Program maintains the following categories of information, and then retains them, as follows:

Per NARA Job No. N1-563-04-09:

Critical Infrastructure Information Submissions in all media formats that do not meet PCII criteria: 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.

Email and word processing documents related to Non-Protected CII submissions:

a. Copies that have no further value after the recordkeeping copy is made: Delete/destroy within 180 days after the recordkeeping copy has been produced

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy: Delete/destroy when dissemination, revision, and updating is complete.

Per NARA Job No. N1-563-08-36:

Critical Infrastructure Information Submissions: Return to submitter or destroy within 30 days of a change in submission status from PCII to non-PCII.

Workflow/Protected Subsystem: Destroy 20 years after the PCII has changed submission status from PCII to non-PCII.

Metadata Repository Subsystem: Destroy 20 years after the PCII has changed submission status from PCII to non-PCII.

Related Records: Destroy 20 years after either the initial status determination of the associated submission or the PCII submission has changed status from PCII to non-PCII.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that PII contained in a CII submission may be retained longer than necessary.

Mitigation: The above risk is mitigated in that information is only retained for as long as necessary and relevant to the PCII Program mission. Submitters can request that information no longer requiring protection be removed from the system. DHS follows NARA guidance regarding purging PII that is no longer relevant or necessary, as described in 5.1, and the PCII Program Office undergoes yearly compliance auditing. Additionally, all PCII Program Office personnel are required to follow the PCII Validation Standard Operating Procedure (SOP) when reviewing CII submitted for protection. By following this SOP and the PCII Procedures Manual, the PCII program office ensures that CII failing to qualify for PCII protections is returned (if requested by the submitter) and destroyed.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, local, and tribal government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The PCII Program shares PCII data with other federal, state, local, tribal, and territorial governments and their contractors, as necessary, to meet mission requirements through PCIIMS FOC and partnership systems. These partnership systems are systems managed by other federal agencies that collect, protect, and disseminate original PCII in a format that has been pre-approved by the PCII Program. Data from partnership systems is shared with the PCII Program by the partnership system granting access to the partnership system, sending a file by email, or by transmitting a CD or hardcopy of the information by mail, if necessary. Each partnership system is required to meet the PCII requirements of the Final rule and is covered by an individual memorandum of understanding (MOU) between the system owner and PCII Program, which details how information is collected, protected and disseminated from the partnership system (See Appendices A and B). A list of partnership systems is maintained by the PCII Program Office.

PCII Authorized User data is not shared outside of DHS as part of normal agency operations.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The purpose of the PCII Program is to protect and share PCII with federal, state, and local agencies when it is needed, as outlined in the CII Act. The purpose of collecting PII with the CII submissions is to communicate with the submitter.

The purpose of collecting PII for Authorized Users is to facilitate the maintenance of the PCII authorized user status and for the PCII Program Office to manage the PCII Authorized Users' PCII related activities. Authorized User information is shared in accordance with DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882).

6.3 Does the project place limitations on re-dissemination?

Information is re-disseminated and shared in accordance with the security defined in the Final Rule for Procedures for Handling Critical Infrastructure Information, 6 CFR Part 29. Limitations on re-dissemination include the requirement that all personnel receiving or viewing PCII have a need-to-know and also be a PCII Authorized User.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Information is only disclosed from PCIIMS to PCII Authorized Users via hardcopy, CD-ROM, or encrypted email. The PCII is shared through the PCII Program Office and is then electronically recorded in PCIIMS as the first level of dissemination. This record includes who received the data, the PCII identification number associated with the PCII, when the dissemination occurred, and the format in

which it was shared. Any subsequent dissemination is recorded by the responsible PCII Authorized User of that PCII, as indicated in the PCII authorized user training and Procedures Manual. Partnership systems are also required to follow this dissemination process.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that PCII data shared outside of DHS is lost or misused.

Mitigation: This risk is mitigated by processes in place whereby any external entity that develops a relationship with the PCII Program Office must first complete certification to receive PCII and then develop programs for receiving, handling, and using PCII in their respective critical infrastructure programs. PCIIMS PCII is only shared via hardcopy, encrypted CD-ROM, or encrypted email. All PCII Authorized Users are required to take PCII Authorized User training annually, which covers the consequences of loss or misuse of PCII data, including criminal and administrative penalties.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

As noted above, once the PCII and submitter's contact information is entered into PCIIMS FOC, it is designated as part of the entire PCII submission. As such, it is protected, and only PCII Authorized Users and the submitters themselves will have access to the submitted information. The PII associated with the submission is not covered by the Privacy Act because the information is not retrieved by personal identifier. PCII is exempt from release under the Freedom of Information Act (FOIA).

Submitters do not have direct access to their information, but can request updates or changes to their previously submitted information or can request that the status of their information be changed from PCII to non-PCII and retained, returned, or destroyed.

Authorized users may contact the PCII Program Manager for access to their information.

Individuals seeking access to any record containing information about themselves that is part of a DHS system of records, or seeking to contest the accuracy of its content, may submit a FOIA or Privacy Act request to DHS. The procedures for submitting FOIA requests are available in 6 CFR Part 5. Please write to "FOIA, U.S. Department of Homeland Security, National Programs and Protection Directorate, Attn: FOIA Officer, Washington, D.C. 20528-0380." Individuals may also make informal inquiries to NPPD.FOIA@dhs.gov.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals should notify the PCII Program Manager of any erroneous information found in the entity's contact information. Currently, the system provides two methods for correcting erroneous information: (1) deletion of the submission containing erroneous information and the creation of a new entry; or (2) by submitting an update to the erroneous submission.

7.3 How does the project notify individuals about the procedures for correcting their information?

Notice to the individual submitting CII information is described via communication with the PCII program office and in this PIA.

For Authorized Users, the PCII Program Office provides notice to individuals in the form of a Privacy Act statement at the time of collection, in this PIA, and the DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: As an individual cannot access their information once submitted, there is a risk that the PCIIMS FOC system may contain inaccurate information. The submitters and Authorized Users may be unaware of inaccuracies.

Mitigation: Once an individual submits CII and that information is protected, only the PCII, not the individual's personal information, is mission-critical. Therefore, if the personal information is inaccurate, it does not affect the overall PCII mission. Further, the individual's information is not analyzed or evaluated in any way and only needs to be correct at the time of submission, in the event the individual needs to be contacted to provide further clarification of the CII submission. If the PCII Program is unable to contact the submitter to clarify submission information within 30 days of receiving the submission, per the Final Rule, the CII submission is not validated as PCII and will be destroyed.

Authorized Users' PII will be verified yearly during their re-certification training, and they also have the ability to update their personal profiles, as necessary.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All uses of the information are specifically defined in the Final Rule for Procedures for Handling Critical Infrastructure Information, 6 CFR Part 29, as well as the DHS/ALL-004 General Information Technology Access Account Records System of Records (September 29, 2009, 74 FR 49882). The uses of the contact information are limited to the coordination and validation of a PCII response.

Additionally, PCIIMS users are authorized to see only the information necessary for the completion of their duties. Any access to PCII data is logged and regularly audited. Only PCII Authorized Users with a valid need to know can use PCII. PCII Authorized Users must maintain their PCII authorized status annually by completing training requirements, of which they are alerted by automated email from the system. If the requirement is not met, their PCII authorized status is revoked, and their information is removed from the system.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

PCII Authorized Users undergo computer-based PCII training that is necessary for any individual, internal or external to DHS, to handle PCII.

All DHS federal and contractor personnel with access to PCII within PCIIMS undergo DHS privacy training, which includes a discussion of Fair Information Practice Principles (FIPPs) and instructions on handling PII in accordance with FIPPs and DHS privacy policy. Additionally, all DHS federal and contractor personnel are required to complete annual privacy refresher training to retain system access. In addition, security training is provided on an annual basis, which will help to maintain the level of awareness for protecting PII. DHS will report on employees, including contractors, who receive IT security and privacy training, as required by FISMA.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

PCII may only be disseminated to PCII Authorized Users with a validated need to know. In order to become a PCII Authorized User, individuals must go through a vetting process, to include passing PCII Authorized User training and receiving certification for proper handling of PCII.

Statutory guidelines provide that the Under Secretary for NPPD 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 CII Act, other law, regulation, or legal authority. Any disclosure or use of PCII within the Federal government is limited by the terms of the CII Act.

The PCII Program Office Procedures Manual, PCII System Security Plan, and the Final Rule document the criteria, procedures, controls, and responsibilities regarding access.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All PCIIMS FOC system access requests and MOUs are reviewed by the PCII Program Office and the PCII Program Manager for approval. The PCIIMS FOC MOU template was written in coordination with the DHS Office of General Counsel.

Responsible Officials

Tammy Barbour
Protected Critical Infrastructure Information Program
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

MEMORANDUM OF AGREEMENT

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 and the Recipient are 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 fulfills that requirement. Furthermore, the PCII Program Office must accredit recipient entities as part of accessing 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 ;

(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) Nominating a PCII Officer

(d) Nominating a PCII PM designee, if applicable

(e) Ensuring that the PCII Officer and the PCII PM designee complete their training

(f) Completing and implementing a self-inspection plan in conjunction with Standard Operating Procedures for safeguarding, handling and disseminating PCII

(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 or Recipient 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

By: Laura L.S. Kimberly

Title: PCII Program Manager

_____
Signature

_____
Date

For _____
(Federal Agency)

By: _____
(Print Name)

Title: _____

_____
Signature

_____
Date

APPENDIX B

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

MEMORANDUM OF AGREEMENT

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 and the Recipient are 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 fulfills that requirement. Furthermore, the PCII Program Office must accredit recipient entities as part of accessing 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) Nominating a PCII Officer
(d) Ensuring that the PCII Officer complete his or her training
(e) Completing the self-inspection plan in conjunction with Standard Operating Procedures for safeguarding, handling and disseminating PCII
(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 or Recipient 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

By: _____
(Print Name)

Title: PCII Program Manager

Title: _____

_____
Signature

_____
Signature

_____
Date

_____
Date