Privacy Impact Assessment
for the

Protected Critical Infrastructure Information Program

DHS/CISA/PIA-034

December 13, 2019

Contact Point
Phillip W. Boggs
Program Manager, Protected Critical Infrastructure Information
Infrastructure Security Division
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
(703) 235-9511

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Protected Critical Infrastructure Information (PCII) Program, part of the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Infrastructure Security Division (ISD), Infrastructure Assessments and Analysis (IAA) Sub-Division, facilitates the sharing of PCII between the Government and the private sector. CISA has conducted this privacy impact assessment (PIA) to analyze and evaluate the privacy impact of the PCII Program's overall operations, including the PCII submission and validation process, and user access management. Most of this work occurs on the Protected Critical Infrastructure Information Management System (PCIIMS). PCIIMS is an Information Technology (IT) system and the means by which PCII submissions from non-federal critical infrastructure owners and operators are received and cataloged, and PCII Authorized Users are registered, trained, and managed. This system receives, provides validation processes, and securely stores critical infrastructure information (physical and cyber systems and assets) meeting the PCII program definition for validation. This PIA replaces DHS/NPPD/PIA-006 Protected Critical Infrastructure Information Management System, published July 13, 2011.

Overview

The vast majority of critical infrastructure within the United States is owned and operated by the private sector. Private sector owners and operators are not compelled to share their sensitive critical infrastructure information with DHS or with other federal agencies and may have disclosure concerns about sharing this information. To address these concerns, Congress passed the Critical Infrastructure Information Act of 2002 (6 U.S.C. § 671 *et seq.*) (CII Act), which provides the Secretary of Homeland Security with the authority to establish a program to receive and protect Critical Infrastructure Information (CII). Congress re-affirmed this authority with the passage of the Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4167. While also protecting CII from public release and disclosure, the CII Act charges DHS 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 enables 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 *Protected* Critical Infrastructure Information—*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]

Critical Infrastructure Owners/Operators who share CII with DHS, which can become protected under the CII Act once validated as PCII, include state and local government entities, private entities or individuals, 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 enables DHS and other authorized homeland security stakeholders access to information about the nation's critical infrastructure more expediently and completely. This comprehensive view of PCII also enables quick and effective planning, analysis, decision-making, and communication. Collecting administrative contact information from submitters of PCII supports the PCII Program mission of receipt, validation, protection, and dissemination of PCII to provide a mechanism to contact the submitter if additional information is needed about the submission. The PCII Program limits the contact information collected to the amount of information necessary to coordinate and validate a particular CII submission. The CII Act exempts validated submissions from the Freedom of Information Act (FOIA), state and local disclosure laws, use in civil litigation, and regulatory actions. 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 established procedures for the PCII Program through an implementing regulation, "Procedures for Handling Critical Infrastructure Information;" Final Rule, 6 CFR part 29 (Final Rule).[2] 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

[1] 6 U.S.C. § 671(3)(A)-(C).
[2] https://www.dhs.gov/sites/default/files/publications/pcii_final_rule_federal_register9-1-06-2_508_0.pdf.

Final Rule also requires the use of Protected Critical Infrastructure Information Management System (PCIIMS) to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of PCII.

PCIIMS exists as a stand-alone system within the accredited boundary of the Infrastructure Protection (IP) Gateway[3] architecture. PCIIMS shares an authentication token with the IP Gateway in order to confirm that the user is a PCII Authorized User. The token includes the PCII Authorized User's first and last name, email address, and PCII Authorized User Number. While PCIIMS sits on the IP Gateway infrastructure, it operates largely independently from the IP Gateway. PCIIMS gathers unique, validated submission metadata regardless of whether the submission originated via PCIIMS itself or from another source. In almost all cases, data is not shared from PCIIMS to IP Gateway or vice versa, except for the authentication token as described above and certain submissions as designated by the PCII Program manager.

PCIIMS offers users the opportunity to log into the system in two ways. Authorized users may access PCIIMS using their DHS Personal Identity Verification card through the DHS Chief Information Officer's AppAuth system.[4] AppAuth is a DHS authentication and credential verification capability. Authorized users whose organizations do not have the AppAuth system capability can access the system using a username and password.

PCIIMS provides the program with three main functions: (1) eSubmissions is a web-based portal enabling private sector and state, local, tribal, and territorial (SLTT) government critical infrastructure personnel to submit information electronically for protection; (2) PCIIMS-Management System (MS) is a function that enables validation and protection of the PCII; and (3) User Management is where PCII Authorized Users are registered, trained, authorized, and their accounts managed.

PCIIMS 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 PCIIMS to register for an account, receive PCII training, maintain their Authorized User status through annual refresher training, and verify others PCII Authorized User status. PCII Authorized Users use PCII for analyses, assessments, and other tasks in support of their homeland security duties (may include individuals outside of DHS). All personnel with access to PCIIMS are required to be PCII Authorized Users. Submitters, however, are not required to be PCII Authorized Users because they are submitting CII to be considered for protections as PCII and are not accessing validated PCII. Only PCII Program personnel have direct access to PCII maintained within PCIIMS, and through PCIIMS, PCII is disseminated to PCII Authorized

[3] *See* DHS/NPPD/PIA-023 Infrastructure Protection Gateway, *available at* www.dhs.gov/privacy.
[4] *See* DHS/ALL/PIA-060 Application Authentication System, *available at* www.dhs.gov/privacy.

Users by approved PCII Program personnel only after all sharing requirements are met, including the establishment of the PCII Authorized User's need-to-know.

As described in the CII Act and the Final Rule, PCII submissions will include PII from submitters. The PCII Program uses the contact information to coordinate and validate, as necessary, a particular CII submission. In addition, the PCII Program collects PII during the PCIIMS 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 through the eSubmissions functionality;[5] or (2) manually via email, regular mail, fax, orally, in-person, etc., or (3) through a pre-approved data collection.[6] Submissions collected outside of the eSubmissions process are required to provide metadata on each submission received that the PCII Program stores in PCIIMS. All tangible items will be immediately stored in lockable filing cabinets and may be prepared for shipment to and storage by the National Archives and Records Administration (NARA). All submissions the PCII Program receives must be accompanied by a signed 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 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.

[5] https://www.dhs.gov/electronic-submit-cii-pcii-protection.
[6] Per 6 CFR part 29.6(f) *Categorical Inclusions of Certain Types of Information*, "[t]he PCII Program Manager has discretion to declare certain subject matter or types of information categorically protected as PCII and to set procedures for receipt and processing of such information. Information within a categorical inclusion will be considered validated upon receipt by the Program Office or any of the Program Manager's designees without further review, provided that the submitter provides the express statement…"

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, the tracking of a CII submission begins with its receipt and is managed through the PCIIMS-MS application.

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 PCIIMS-MS 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.

PCIIMS-MS

The submission identification number follows the submission through the entire PCII submission, validation, approval, and storage process, which occurs in the PCIIMS-MS application. The PCIIMS-MS 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. The PCIIMS-MS application provides the ability to systematically generate letters to send to a submitter for various information requests or status updates regarding the submission. PCIIMS-MS 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 process, the PCII Program will either validate the submission as PCII, reject, or withdraw the submission upon the submitter's request. If the submission is validated as PCII, the PCIIMS-MS 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 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 as described in Section 5.0 of this PIA.

PCII Program personnel can perform limited search and reporting capabilities on the CII submissions, including the reporting of first-level dissemination of PCII retained in the application. This PCIIMS-MS functionality requires a separate login from eSubmissions and User Management functions. The search results and report information are only accessible to the PCII Program Office personnel. No other PCIIMS system users have access. Certain PCII submissions within PCIIMS-MS can be searched by an authorized federal user only using the IP Gateway's Digital Library search function. These submissions are approved by the PCII Program Manager before being placed in a "Share" folder allowing their discovery by a federal homeland security analyst.

User Management

The User Management functionality enables the PCII Program to manage the PCII Authorized Users. In order to maintain oversight and management of PCII Authorized Users, the PCII Program maintains a central repository of all users who are authorized to access PCII. 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 and complete annual refresher training requirements. The PCII Program relies heavily on a distributed user management framework consisting of PCII Officers within the many federal, state, local, tribal, and territorial government organizations that access PCII to oversee and manage the PCII Authorized User community.

The User Management application in PCIIMS aids the PCII Program Office 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 Office and Officer administrative tasks. All PCII Authorized Users are required to take PCII Authorized User training, which covers the access, marking, handling, dissemination and 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 with a need-to-know, 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 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). An additional capability PCIIMS provides as part of its User Management function is the authorized user search. Information provided as part of the search results includes: (1) PCIIMS Username, (2) First Name, (3) Last Name, (4) Email Address, (5) Authorized User Number, (6) account creation date, and (7) account expiration date. Upon signing into PCIIMS, users see the Privacy Notice (Attachment 1) and Authorization to Release and Consent to Exchange Information (Attachment 2). Users who agree to the authorization click "Agree and Continue" to access PCIIMS and users who do not agree to provide the information needed to establish the account may delay or prevent their registration or access to PCIIMS.

Partnership Systems

The PCII Program 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 from the PCII Program. These systems collect, protect, and disseminate original PCII in a format that has been pre-approved by the PCII Program Manager. PCII Officers in other federal agencies share their data with DHS either by granting the PCII Program Office 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 agreement (MOA) between the system owner and the PCII Program, which details how information is collected, protected, and disseminated from the partnership system (See Attachments 3 and 4).

PCII Program personnel may input PCII submission metadata records from approved PCII partnership systems into the PCIIMS-MS application in a standardized XML format. PCIIMS-MS stores these metadata records and enables the PCII Program analysts 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 U.S.C. § 121(d)), the CII Act[7], and the implementing regulation, "Procedures for Handling Critical Infrastructure Information;" Final

[7] 6 U.S.C. § 671 et seq.

Rule, 6 CFR part 29 (Final Rule), authorize CISA to collect PII necessary to manage PCIIMS and process CII submissions.

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

The PCII Program Office collects PII for the purpose of granting access to the PCIIMS 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).

Though PII submitted as part of the CII submission is covered by the Privacy Act, a system of records notice is not required because the information is not retrieved by personal identifier.

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

Because PCIIMS currently exists as an integrated capability on the IP Gateway infrastructure, it relies on the IP Gateway system security plan, which has been completed. The IP Gateway has been issued an Authority to Operate (ATO) through May 8, 2021 and has been granted admission into the ongoing authorization program.

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

The following records schedules cover PCIIMS and have been approved by National Archives and Records Administration (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."[8] However, the final rule

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

does not exempt partnership systems, and as such, collections by each partnership system may be required to follow PRA guidelines.

Section 2.0 Characterization of the Information

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

The eSubmissions functionality of PCIIMS collects limited contact information from individuals submitting CII to DHS. The contact information consists of full name, business title, business email address, business 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. Anonymous submissions are not accepted.

Information regarding the critical infrastructure itself comprises the rest of the submission and does not include PII. The types of information that PCIIMS collects may include the subject material (e.g., telecom, nuclear, chemical, commerce), plans related to a site (e.g., disaster, emergency response, security, buffer zone protection), 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.

Each submission requires an Express Statement and a Certification Statement (Attachment 5) from the submitter. This is usually referred to as the E&C statement and is signed by the submitting person or an authorized person on behalf of an entity and identifies the submitting person or entity. The statement affirms that the information is being voluntarily submitted in expectation of the protections provided by the CII Act and the certification statement must contain such contact information as is considered necessary by the PCII Program Manager and certify that the information being submitted is not customarily in the public domain.

The user management functionality of PCIIMS collects business contact information (e.g., name, email, business address, business phone, and organization) on personnel that are PCII Authorized Users. PCIIMS provides the Authorized User search function to its users. This capability allows for authorized users to enter names into a search function that queries whether the individuals whose names are entered are also authorized PCIIMS users. Information provided as part of the search results includes: (1) PCIIMS Username, (2) First Name, (3) Last Name, (4) Email Address, (5) Authorized User Number, (6) Account Creation Date, and (7) Account Expiration Date.

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 through the eSubmissions functionality; or (2) manually via email, regular mail, fax, orally, in-person, etc., in which case a PCII Program analyst inputs and uploads the submission into PCIIMS on the submitter's behalf. In the case of faxed or hard copy submissions, a PCII Program analyst scans and uploads the information to PCIIMS. Original, hard copy documents are stored securely in accordance with PCII safeguarding and records retention requirements.

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 Manager. The data is shared with the PCII Program 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 MOA between the system owner and the PCII Program Office, which details how information is collected, protected and disseminated from the partnership system (See Attachments 3 and 4).

Additionally, the User Management functionality of PCIIMS 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.

No. All information collected by PCIIMS is provided by the individual.

2.4 Discuss how accuracy of the data is ensured.

The PCII Program verifies the submitter's contact information at the time of the CII submission. PCII Program analysts review the information contained in the submitting entity's submission and E&C statements, as it is inputted into the eSubmissions functionality of PCIIMS. In the case of an oral submission, the submitter must follow up with written documents to memorialize the submission, which a PCII Program analyst then reviews. 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 his or her contact information.

Established standard operating procedures require that a trained PCII Program analyst review the information to ensure the submission either does or does not qualify for PCII protection and to check for accuracy. Once the employee processes the information, only the Program Manager of the PCII Program is authorized to validate the submission before it is stored as read-only in PCIIMS.

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 his or her information or to withdraw protections from the submissions. Notifications are also sent to PCII Authorized Users via email to conduct various PCIIMS user management activities, including training renewal notices and password resets. Responses to these notifications ensure that the contact information within PCIIMS is up to date. A non-response triggers PCIIMS 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: This risk has been mitigated. The PCII Program 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.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The PCII Program and PCII Authorized Users use 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 and other authorized government users to include federal, state, local, tribal, or territorial agents and their contractors.

PCII information is used by federal, state, local, tribal, and territorial governments in response to natural disaster recovery efforts. Using PII collected as part of a submission, the PCII Program may communicate requests to submitting entities in support of the PCII Program'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 uses the contact information provided as part of a CII submission to

contact the submitting entity with questions related to the submission. Once protected, the PII submitted with the CII submission will also be considered PCII, but it will not be shared by the PCII Program. The PCII is disseminated only to PCII Authorized Users with the need-to-know. In addition, the PCII Program collects PII during the PCIIMS user registration process to manage PCII Authorized Users with access to the system. Within PCIIMS, 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 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 Program 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 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 establishes a relationship with the PCII Program must develop programs for receiving, handling, and using PCII in their respective critical infrastructure programs. They must complete certification to receive PCII. A list of DHS components and directorates, as well as entities outside of DHS, with which the information is shared is maintained by the PCII Program.

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. Criminal and administrative penalties are identified in Section 214(f) of the CII Act for misuse of 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. Furthermore, 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

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 E&C statement, ensuring the submitter acknowledges the voluntary nature of the PCII Program. Entities, including the individual submitters, are provided with specifics about the program in the Final Rule. The PCII Program provides notice at the time of collection to individuals applying to be Authorized Users in the form of a Privacy Act Statement, prior to accessing PCIIMS, in this PIA, and DHS/ALL-004 General Information Technology Access Account Records System of Records (November 27, 2012, 77 FR 70792).

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 may need to contact a submitter for additional information when validating 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 does not accept anonymous submissions. If a submitter declines to provide his or her contact information that would indicate that he or she chooses not to participate in the PCII Program.

PCII Authorized Users are not provided the 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. The PCII Program has a direct relationship with both submitters and PCII Authorized Users and ensures that the 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. Once an entity chooses to submit information, it is 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 E&C

statements certifying that information submitted to the PCII Program is done so voluntarily by the individual.

For Authorized Users, the PCII Program provides notice to individuals in the form of a Privacy Act Statement at the time of collection, and further notice is provided in DHS/ALL-004 General Information Technology Access Account Records System of Records (November 27, 2012, 77 FR 70792). This notice also ensures that individuals are aware of how to access and correct their records maintained within PCIIMS.

Section 5.0 Data Retention by the project

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

DHS worked with NARA to develop a retention schedule for the records maintained within PCIIMS. 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 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 Manager 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 E&C 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, submitters may request that the information be returned to them. Otherwise, it is removed from PCIIMS and destroyed.

Per NARA guidance, the PCII Program Office 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.

PCIIMS-MS/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 risk is mitigated. CISA only retains information 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 Section 5.1. All PCII Program 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 ensures that CII failing to qualify for PCII protections is returned (if requested by the submitter) and destroyed.

Section 6.0 Information Sharing

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 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 Manager. Data from partnership systems is shared with the PCII Program Office 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 MOA between the system owner and the PCII Program, which details how information is collected, protected, and disseminated from the partnership system (See Attachments 3 and 4). A list of partnership systems is maintained by the PCII Program.

PCII Authorized User data is not shared outside of DHS as part of normal agency operations. PCII Authorized Users can use PCIIMS or reach out to the PCII Program to determine the user status of other PCII Authorized Users, though the only information that would be provided to the requesting Authorized User would be the other Authorized User's PCII Number and the expiration date of the requested Authorized User status.

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, local, tribal, and territorial 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 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 (November 27, 2012, 77 FR 70792).

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 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, 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.[9] Partnership systems are 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 must first complete certification to receive PCII and then develop programs for receiving, handling, and using PCII in its respective critical infrastructure programs. PCIIMS PCII is only shared via hardcopy, encrypted CD, 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

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, 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 CII submissions is not retrieved by personal identifier and therefore not subject to individual access provision of the Privacy Act.[10] In addition, PCII is exempt from release under the Freedom of Information Act (FOIA).[11]

Although submitters do not have direct access to the contact information in their submissions, they 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. PCIIMS Authorized Users may contact the PCII Program Manager for access to their information by emailing pcii-info@dhs.gov.

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

CISA FOIA Officer
245 Murray Lane SW

[9] https://www.dhs.gov/sites/default/files/publications/pcii-program-procedures-manual-508.pdf.
[10] 5 U.S.C. §552a(d)(1).
[11] The Freedom of Information Act is codified at 5 U.S.C. § 552. *See* 6 U.S.C. § 673 for the exemption.

Washington, D.C. 20528-0380

Individuals may also make informal inquiries to CISAFOIA@hq.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 by emailing pcii-info@dhs.gov. Currently, PCIIMS provides two methods for correcting erroneous or inaccurate 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 and in this PIA.

For Authorized Users, the PCII Program provides notice to individuals in the form of a Privacy Act statement at the time of collection, in this PIA, and DHS/ALL-004 General Information Technology Access Account Records System of Records (November 27, 2012, 77 FR 70792).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: As an individual cannot access his or her information once submitted, there is a risk that the individual cannot correct potentially inaccurate information in PCIIMS.

Mitigation: The risk is partially mitigated. The individual's information 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, including the contact information, is not validated as PCII and will be destroyed.

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

Section 8.0 Auditing and Accountability

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 DHS/ALL-004 General

Information Technology Access Account Records System of Records (November 27, 2012, 77 FR 70792). 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 user 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. Further, 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 the Federal Information Security Modernization Act (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 CISA Director or the Director'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 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 access requests and MOAs are reviewed by the PCII Program and the PCII Program Manager for approval. The PCIIMS MOA template was written in coordination with the DHS Office of General Counsel.

Responsible Officials

Phillip Boggs
Program Manager, Protected Critical Infrastructure Information
Infrastructure Security Division
Cybersecurity and Infrastructure Security Agency

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

ATTACHMENT 1

PCIIMS Privacy Notice

Authority: 5 U.S. C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.

Purpose: The primary purpose of this collection is to grant PCII Authorized Users access to the PCIIMS system.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 General Information Technology Access Account Records System of Records (November 27, 2012, 77 FR 70792).

Disclosure: Furnishing this information is voluntary; however, failure to furnish the requested information may delay or prevent your registration or access to PCIIMS.

ATTACHMENT 2

PCIIMS Authorization to Release and Consent to Exchange Information

The Protected Critical Infrastructure Information (PCII) Program Office maintains the Protected Critical Infrastructure Information Management System (PCIIMS) to record and manage among other things the receipt, acknowledgement, dissemination, and users of PCII.

By registering as a user, you are authorizing the PCII Program Office to allow other PCII authorized users to query PCIIMS by your first name, last name, user name, email address, authorized user number(s), and/or PCII authorized user expiration date.

I acknowledge that this consent is voluntary. If I cancel this consent at a later date, I must send written notification to the PCII Program Manager at PCII-Assist@hq.dhs.gov. If this consent is cancelled, I understand that information may have been released prior to the cancellation, and that action would not be considered a breach of confidentiality. I also acknowledge that recipients of this information could possibly re-release the information without proper authorization. Additionally, I understand that my access to PCIIMS will be terminated upon the cancellation of consent.

I understand that the information may be released electronically, and may include information related to my PCIIMS username; PCII authorized user number; and user expiration date.

I have read and understand this authorization and consent will remain effective until I revoke it by notifying the PCII Program Office in writing. This will stop the exchange of information authorized by this document. If I do not acknowledge this form, information will not be exchanged and will not be granted access to PCIIMS.

ATTACHMENT 3

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. §§ 671-674 ("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. § 673(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. § 673(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 reimbursable 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: Phillip W. Boggs

Title: PCII Program Manager

_____
Signature

For _____
(Federal Agency)

By: _____
(Print Name)

Title: _____

_____
Signature

_____
Date

_____
Date

ATTACHMENT 4

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. §§ 671-674 ("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. § 673(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. § 673(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 reimbursable 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: Phillip W. Boggs

Title: PCII Program Manager

_____
Signature

For _____
(State Agency)

By: _____
(Print Name)

Title: _____

_____
Signature

_____
Date

_____
Date

ATTACHMENT 5

Express and Certification Template

EXPRESS STATEMENT

This 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.

CERTIFICATION STATEMENT

To the best of my knowledge, information, and belief, the information being submitted is not customarily in the public domain.

I attest that I am not submitting this information in lieu of complying with a regulatory requirement.

I am authorized to submit this information to be considered for protection under the Critical Infrastructure Information Act of 2002.

Signature _____ Date _____

Please provide the following information:

Submitter:

Name:

Title:

Organization or Company Name (if applicable):

Mailing Address: City: State: Zip:

Office Telephone: Alternate Telephone: E-mail Address:

Alternate Contact Information:

Name:

Title:

Organization or Company Name (if applicable):

Mailing Address: City: State: Zip:

Office Telephone: Alternate Telephone: E-mail Address:

Please be aware that any knowing or willful false representations provided in this submission may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.