DEPARTMENT OF HOMELAND SECURITY (DHS)
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) PROGRAM

WORK PRODUCTS GUIDE

(APPENDIX TO PCII PROCEDURES MANUAL)

JANUARY 2012

Table of Contents

1. INTRODUCTION

This product guide is intended to provide authorized users with guidelines on how to identify and treat various work products that are based on Protected Critical Infrastructure Information (PCII). These guidelines are not meant to be all inclusive to determine how to mark or sanitize sensitive material but should be viewed as a quick reference tool for working with PCII.

2. TWO TYPES OF PCII WORK PRODUCTS

The two primary types of PCII work products are:

1. Derivative products: products derived from and containing PCII that should be marked, safeguarded, and handled as PCII; and
2. Sanitized products: advisories, alerts, and warnings that are not PCII and do not require PCII marking or handling.

2.1 DERIVATIVE PRODUCTS

Federal, State, or local entities frequently use PCII to conduct analysis on various assets, vulnerabilities, and sectors. The analysis results in an analytical derivative product(s). For example, at the Federal level, DHS analysts create derivative products that feature sector-wide or region-based analysis on common vulnerabilities or resilience issues.

Generally, if any sensitive material is taken from a PCII document, placed into or used directly in a new product, that new product is considered a PCII derivative product and must follow all PCII marking, safeguarding, and disclosure requirements.

Sensitive material will typically reveal security-related information or the vulnerability of specific infrastructure. For example, a risk evaluation concerning an asset, or details about an attempted or successful attack on infrastructure may be revealed, or information about a post-attack rebuilding plan is exposed. Any information that identifies the asset's submitter or reveals the information about the asset is PCII and will be considered sensitive and protected as PCII. Proprietary, business sensitive or trade secret information is also sensitive and treated as PCII.

The determination of what is "sensitive" or what is a "vulnerability" depends on the review of the content. Therefore, the topics below are only meant to be a guide to assist you with identifying sensitive material. If you are creating work products, please feel free to contact the DHS PCII Program on derivative product creation or sanitization efforts.

For the purposes of the PCII Program, a PCII derivative product is created when any of the following sensitive topics are taken from a PCII document and placed in a new product:

- Discussions of security-related vulnerabilities of (or risks to) critical infrastructure (or a protected system) related to a specific asset (i.e., the asset is identified by name);
- Information about attacks on infrastructure;
- Post-attack reconstruction and continuity plans;

- Proprietary, business-sensitive, or trade secret information; or
- Information revealing that a particular asset or submitter has made a PCII submission.

EXAMPLES

Below are examples to assist you with determining if a new analytical work product is a PCII derivative product:

A. Sample (identifies the submitter) within new work product:

"…John Smith, a Security Manager of a water treatment plant in Springfield county, entered information into the Automated Critical Asset Management System (ACAMS) describing his external security cameras …"

Evaluation:

PCII is present. The submitter surname is present, revealing his identity and participation in a PCII collection. A reference is made to the name of a PCII-approved categorical inclusion. Treat this as a derivative product that must be marked and safeguarded as PCII.

B. Sample (identifies an asset's vulnerability) within new work product:

"Jones Stadium and Smith Center both employ measures that mitigate most of the site assessment vulnerability-identified physical security deficiencies – with the exception of outer perimeter barriers at one facility and uninhibited avenues of approach at both facilities."

Evaluation:

PCII is present. A vulnerability is attributed to an asset and sensitive details were taken from an existing PCII document. Treat this as a derivative product that must be marked and safeguarded as PCII.

C. Sample (non-PCII) within new work product:

"Several vulnerabilities have been identified spanning the entire sector that indicate the sector is at an increased risk from a cyber attack".

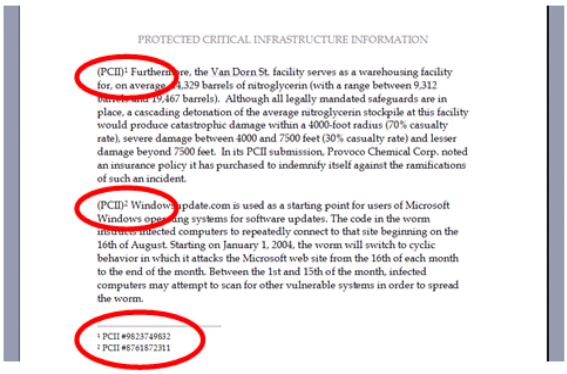
Evaluation:

No PCII is present. No specific details from any one submission were included, vulnerability and conclusion provided were from a strategic sector-wide view. No reference was made to a PCII-approved collection. This is not a derivative product and does not require PCII safeguarding (See Section 2.2.1 for more discussion.)

2.1.1 Unclassified Derivative Products

All users must follow these guidelines when preparing an *unclassified* PCII derivative product:

- Insert the text "Protected Critical Infrastructure Information" in the header and footer in a font larger than the document text.
- Mark each paragraph, table, graphic, figure, etc., containing verbatim or paraphrased PCII parenthetically as "PCII". (All other paragraphs, tables, graphics, figures, etc., are **not** portion-marked.) Insert a footnote superscript number as well.


PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

(PCII)[1] Furthermore, the Van Dorn St. facility serves as a warehousing facility for, on average, 14,329 barrels of nitroglycerin (with a range between 9,312 barrels and 19,467 barrels). Although all legally mandated safeguards are in place, a cascading detonation of the average nitroglycerin stockpile at this facility would produce catastrophic damage within a 4000-foot radius (70% casualty rate), severe damage between 4000 and 7500 feet (30% casualty rate) and lesser damage beyond 7500 feet. In its PCII submission, Provoco Chemical Corp. noted an insurance policy it has purchased to indemnify itself against the ramifications of such an incident.

(PCII)[2] Windowsupdate.com is used as a starting point for users of Microsoft Windows operating systems for software updates. The code in the worm instructs infected computers to repeatedly connect to that site beginning on the 16th of August. Starting on January 1, 2004, the worm will switch to cyclic behavior in which it attacks the Microsoft web site from the 16th of each month to the end of the month. Between the 1st and 15th of the month, infected computers may attempt to scan for other vulnerable systems in order to spread the worm.

[1] PCII #9823749832
[2] PCII #8761872311

- Include the Tracking Number for the PCII in a footnote to the paragraph (in most word processing applications this will automatically generate the required reference at the bottom of the page.)
  When there are numerous references and tracking numbers, a table may be used. Superscripts connecting the paragraph to a specific PCII document are not required when dealing with numerous references. However, the table should identify the asset or title of the PCII document being referenced. The table should also be present near the beginning of the document. A sample table is provided below.
- Affix a PCII Cover Sheet clearly marked with "PCII Derivative Product" in the "submission identification number" field. **NOTE**: PCII derived products will not have unique Tracking Numbers.

Sample PCII Reference Table

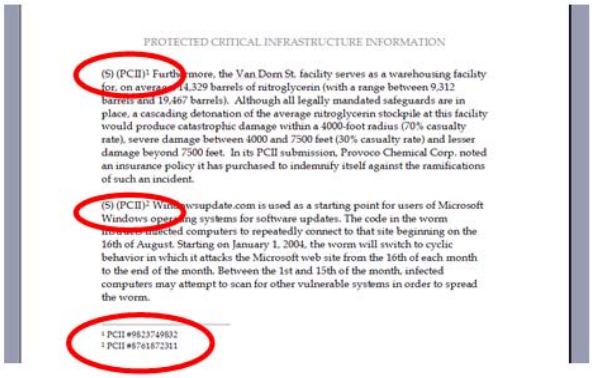
PCII Source Document	**Asset/System**	**PCII Source Document**	**Asset/System**
PCII-BZPP-12345-1234	Acme., Inc.	PCII-BZPP-12555-0001	Jones Chemical Plant
PCII-BZPP-56897-0001	Brooklyn Bridge	PCII-ECIP-33345-0001	Highway 66
PCII-SAV-12665-0001	Turner Pumping Station	PCII-BZPP-67845-0001	The Rodriguez Dam
PCII-BZPP-12555-0001	Jones Industrial Smoothing	PCII-BZPP-00045-0001	Peabody Towers

2.1.2 Classified Derivative Products

Classified PCII derivative products must be handled and protected in accordance with the safeguarding and handling requirements for **both** PCII and the highest level of classified designation within the product**.**

All users must follow these guidelines when preparing a *classified* PCII derivative product in addition to the procedures required by the classified designation:

- Insert the text "Protected Critical Infrastructure Information" in the header and footer in a font larger than the document text.
- Each paragraph, table, graphic, figure, etc., containing verbatim or paraphrased PCII must be parenthetically marked as "PCII". Where possible, separate Classified and PCII into separate paragraphs to assist in future sanitizing or releases of information. Where information in a paragraph, table, graphic, figure, etc., must be both PCII and Classified, it must be double-marked [e.g., (S) (PCII) or (TS) (PCII)]. This double marking is necessary because subsequent declassification will eliminate only the requirement for protecting the data as classified information. It will **NOT** eliminate the requirements for protecting PCII. Include the Tracking Number for the PCII in a footnote to the paragraph, table, figure, etc. When there are numerous references and tracking numbers, a table may be used (see section 2.1.1 for discussion and a sample table.).


PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

(S) (PCII)[1] Furthermore, the Van Dorn St. facility serves as a warehousing facility for, on average, 14,329 barrels of nitroglycerin (with a range between 9,312 barrels and 19,467 barrels). Although all legally mandated safeguards are in place, a cascading detonation of the average nitroglycerin stockpile at this facility would produce catastrophic damage within a 4000-foot radius (70% casualty rate), severe damage between 4000 and 7500 feet (30% casualty rate) and lesser damage beyond 7500 feet. In its PCII submission, Provoco Chemical Corp. noted an insurance policy it has purchased to indemnify itself against the ramifications of such an incident.

(S) (PCII)[2] Windowsupdate.com is used as a starting point for users of Microsoft Windows operating systems for software updates. The code in the worm instructs infected computers to repeatedly connect to that site beginning on the 16th of August. Starting on January 1, 2004, the worm will switch to cyclic behavior in which it attacks the Microsoft web site from the 16th of each month to the end of the month. Between the 1st and 15th of the month, infected computers may attempt to scan for other vulnerable systems in order to spread the worm.

[1] PCII #9823749832
[2] PCII #8761872311

  Affix the PCII cover sheet immediately behind the classified cover sheet clearly marked with "PCII Derivative Product" in the "submission identification number" field. **NOTE**: PCII derived products will not have unique Tracking Numbers.

2.2 SANITIZED PRODUCTS

There are different reasons for the need to create a sanitized product, such as:

- The creation of a database that only features information in the public domain ; or
- Creation of a general advisory, alert or warning that can be disseminated to a large and varied audience.

2.2.1 Sanitized Work Products

A work product may be developed that includes only asset names and geographic descriptors. As seen above, if the work product names the asset and discusses a security-related or proprietary characteristic, then the product is a PCII derivative product. However, if the **only** information extracted from an existing PCII document is the **asset name** and **publicly available information**, such as the asset address or geographical coordinates, the product is not a PCII derivative product.

In order to be considered a sanitized product, the information:

- cannot reveal that the submitter made a PCII submission;
- cannot include data from PCII submissions;

- cannot include references to PCII-approved collections or submission data from such collections;
- cannot reveal any sensitive infrastructure information as discussed in Section 2.1;

For example, lists of assets, that feature addresses, are compiled by government entities in order to create catalogs of infrastructure. For these lists, ensure that the product does not feature any reference to the fact that any information was obtained from PCII. No reference should be made to the name of a PCII-approved categorical inclusion, e.g., a Site Assistance Visit Report. Nor should any markings, headers/footers, etc., be present. The requirement is to protect the submitter's identity and their participation in PCII-related submissions or collections.

The following graphic, a snapshot from a fictitious local government infrastructure cataloguing tool, provides an example of an acceptable sanitized work product that does not have to be treated as PCII.. This list is comprised of addresses from assets that were obtained from more than one collection effort. This Listing System identifies the collections of origin under the "Dataset" column. Some datasets do not involve PCII protections at all, whereas others are PCII collections. However, addresses and other types of geographic location data can be duplicated from sources in the public domain. Although this is technically a work product because some of the asset names and addresses were taken from PCII reports, the product is not PCII because the quoted material exists in the public domain.

NOTE:

- Please note that there are no PCII headers or footers;
- The dataset of origin for those results with PCII origins (those datasets were PCII categorical inclusions) are intentionally given the non-attributable label of "Other", to avoid using the "PCII" label, and .
- There are no labels connecting the submitting asset to a PCII submission.

Smithtown Pennsylvania Infrastructure Facility Listing System

Website Search Query Results: …10 results

Select Box	Asset Name	Address	City	County	State	Zip	Latitude	Longitude	Sector	Subsector	Dataset
[ ]	Jones Pipeline – Junction Breakout Tankage	34 Beryl Court	Port Heading	Accomack	PA	3678	55.48528	-86.7489	Energy	Petroleum	Other
[ ]	Pearlman Electricity Plant	1313 Mockingbird Lane	Smithtown	Albemarle	PA	3699	55.8546	-86.4788	Energy	Electricity	IAL
[ ]	Exxon Gas distribution plant	461 Ryders Lane	Jones City	Caroline	PA	3622	55.5874	-86.5688	Energy	Petroleum	IAL
[ ]	Mack-Cali Office	2 Savage Road	Fort Kyle	Amelia	PA	3644	55.6987	-86.5444	Commercial Facilities	Office Buildings	Other
[ ]	NJ Transit Line	8876 Myers Street	Phillipsburg	Amherst	PA	3611	55.1147	-86.8585	Transportation	Rail	Other
[ ]	Brown Fertilization Co.	121 Sycamore Street	Richardton	Arlington	PA	3678	55.6698	-86.7474	Critical Manufacturing	Fertilizers	Other
[ ]	Crystal Clear Water Treatment Plant	880 Route 23	New Brunswick	Campbell	PA	3621	55.6677	-86.1111	Water	Wastewater	IAL
[ ]	Dallas Pumping LLC	248 Landing Lane	Springfield	Augusta	PA	3655	55.1158	-86.5588	Energy	Petroleum	IAL
[ ]	Quakerbridge Mall	119 Broadway Blvd.	Alexandria	Bath	PA	3609	55.6987	-86.7458	Commercial Facilities	Shopping Malls	Other
[ ]	I-95 Overpass at Dayton	I-95 at Dayton	Newark	Bedford	PA	3602	55.6699	-86.7888	Transportation	Highways	Other

2.2.2 Sanitized Advisories, Alerts and Warnings

Federal, State, or local entities may use PCII to prepare advisories, alerts, and warnings regarding potential threats and vulnerabilities to critical infrastructure for dissemination to individuals outside of the PCII Authorized User community such as public and private sector individuals or foreign governments. When an advisory, alert or warning is produced, the product must be sanitized to remove all PCII. When appropriate, it is recommended that the PCII Officer or preparer of the advisory, alert or warning contact the submitting person (or an authorized person on behalf of a submitting entity) to ensure that the advisory, alert, or warning does not contain proprietary, business sensitive, or trade secret information. PCII Officers are responsible for ensuring that advisories, alerts, and warnings are sufficiently sanitized. The PCII Program is also available to provide advice and review of advisories, alerts or warnings as needed.

Further to the discussion of "sensitive" material in Section 2.1, sanitizing involves ensuring no reference to a PCII submission or identity-centric elements such as the submitter surname, asset name, address, coordinates, and the site-specific vulnerability information associated with that asset. The following is an example of an advisory that could be considered sanitized:

A. Sample (non-PCII) within new work product:

"IF THE BARRIER IS OVERRUN, HOUSING AND COMMERCIAL PROPERTIES IN THE PROVIDENCE RIVER BASIN MAY EXPERIENCE SEVERE FLOODING...DAMAGE TO INFRASTRUCTURE MAY ALSO RESULT, INCLUDING COMPROMISE OF ANY STRUCTURE IN THE AREA WITH A 6 FOOT PERIMETER WALL OR SHORTER."
Evaluation:
No PCII is present. No specific details from any one submission were included, vulnerability and conclusion provided were from a strategic sector-wide view. No reference was made to a PCII-approved collection. This is not a derivative product and does not require PCII safeguarding

As you can see from the example above, a sanitized product can be produced while still mentioning a vulnerability. The example identifies a vulnerability by itself, without revealing the asset or any identity-centric characteristics that originated from a PCII source.

Unless exigent circumstances require otherwise, any advisory/alert/warning to the general public that is not sanitized in accordance with the directions above must be authorized by the DHS Secretary, the Under Secretary for National Protection and Programs, the Assistant Secretary for Cyber Security and Communications, or the Assistant Secretary for Infrastructure Protection.

Such exigent circumstances exist only when authorization from the parties named above cannot be obtained within a reasonable time necessary to issue an effective advisory, alert, or warning. The PCII Officer, or other authorized PCII individual such as the Designee, must coordinate with the PCII Program to issue these warnings in accordance with the PCII Final Rule (6 CFR Part 29). In issuing advisories, alerts, and warnings, DHS must—

- Consider the exigency of the situation, the extent of possible harm to the public or to critical infrastructure, and the necessary scope of the advisory, alert, or warning;
- Take appropriate actions to protect from disclosure any information that is proprietary; business sensitive; or is not otherwise appropriately in the public domain; or relates specifically to or might be used to identify the submitting person or entity, any persons or entities on whose behalf the critical infrastructure information was submitted.;

DHS may consult or cooperate with the submitter in issuing such advisories, alerts, or warnings. A State or local government entity that has submitted CII validated as PCII, is not required to consult DHS in the issuance of an advisory, alert, or warning based on the PCII provided that the State or local entity either (a) uses its own copy of the information that does not bear the PCII marking or, (b) if it is using a PCII copy, has sanitized the advisory, alert, or warning such that it does not contain any PCII.

2.2.2.1 Using a Derivative Product as the Source

When a PCII derivative product is used as the basis for developing an advisory, alert, or warning for public release, following the sanitization principles discussed in section 2.1 will ensure that the subsequent advisory, alert, or warning **does not** contain any PCII.

If the PCII derivative product that provides the basis for the advisory, alert, or warning includes "Third party information" (e.g., Company A independently submits information about a product made by, or a service provided by, Company B), the advisory, alert, or warning must **NOT** include any information that explicitly or implicitly identifies specific products or services from the third party.

However, analysts may use any information they obtain from open sources that may potentially contain the same information found in a PCII derivative product.

2.3 THE PCII COVER SHEET

The PCII Cover Sheet is a warning that alerts observers that the document contains PCII.

The PCII Cover Sheet must be affixed to all documents containing PCII, including derivative products, and must remain with the document at all times. PCII materials should always be protected by the PCII Cover Sheet, whether in storage, transit, or when in use, even in an environment with existing rigorous access controls in place.

3. DISSEMINATION OF DERIVATIVE PRODUCTS

Derivative products can only be disseminated to authorized users with homeland security responsibilities and a “need-to-know”. If you need to disseminate a product to unauthorized users or the general public, you are responsible for adequately sanitizing the product and issuing it in the form of an advisory, alert, or warning.

4. DESTRUCTION OF DERIVATIVE PRODUCTS

The PCII Program encourages destruction of PCII derivative products and copies of PCII when no longer needed. No approval is required from the PCII Program Manager to destroy copies of PCII materials or PCII derivative products, but approved destruction methods must be used. Destruction of *original* PCII materials is not permitted at any time.

Table 4-1. Approved Destruction Methods

Approved Destruction Methods	
Paper	Shred or Burn
Electronic File	Delete and empty recycle bin
Magnetic Media	Degauss or shred
Compact Discs	Shred and grind
Thumb Drives/Memory Sticks	Wipe and erase data
Microfiche: Audio/Video Tapes	Chemical (e.g., acetone bath) or shred
System Backups	Contact the PCII Program Office
Other (e.g., databases or hard drives)	

5. PCII TRACKING REQUIREMENTS

PCII Officers are strongly encouraged to track the generation, dissemination, and destruction of all PCII derivative products and all copies of PCII within the entity for which they are responsible. Additional information on tracking may be found in the PCII Procedures Manual, Section 8.3, Tracking.

Overview Outline

Derivative Products

- If any sensitive material taken from a PCII document is placed into a new product, that new product is considered a PCII derivative product and must follow all PCII rules.
- The most common type of "sensitive" information is when a security-related vulnerability is attributed to, and combined with, a specific asset.
- You can destroy PCII derivative products and copies of PCII when no longer needed. No approval is required. Destruction of *original* PCII materials is not permitted at any time.
- Officers are strongly encouraged to track the generation, dissemination, and destruction of all derivative products.

How to Mark an Unclassified Derivative Product

- Insert the PCII header and footer.
- Mark each PCII-containing paragraph with "(PCII) ".
- Use a footnote and superscript system for products with only a few quotations.
- Use a reference table for products with numerous quotations.
- Affix a PCII cover sheet.

Derivative Products featuring Classified Information

- Insert the PCII header and footer.
- Separate the Classified from the PCII into separate paragraphs if possible.
- Mark each any paragraph containing both PCII and classified material with a dual marking such as "(TS)(PCII)."
- Use a footnote and superscript system for products with only a few quotations.
- Use a reference table for products with numerous quotations.
- Affix a PCII cover sheet.

Sanitized Product – Public Domain Work Product

- An asset name, taken from a PCII document, used alone, or with publically available location fields, is not PCII.
- "Asset address lists" are not PCII.

Sanitized Product – Advisories/Alerts/Warnings (AAWs)

- AAWs cannot contain combinations of identity or location elements, nor site-specific vulnerabilities (amongst other sensitivities).
- If the submitting government entity is not sure if their attempt to sanitize an AAW is in compliance, the AAW must go through DHS approval.
- A SLT entity does not have to submit its AAW to DHS for compliance if it uses its own, non-PCII marked, copy.