KENTUCKY OFFICE OF HOMELAND SECURITY
READY AND PREPARED

# Nonprofit Organization Vulnerability Assessment

Facility Name:

Facility POC:

Assessor Name/Organization:

Date of Assessment:

**If you use this document, you MUST provide a narrative of the identified vulnerabilities, not just a YES or NO answer. Incomplete responses can result in the application not being funded.**

*This assessment will be voluntarily submitted as Protected Critical Infrastructure Information (PCII) under the Critical Infrastructure Information Act of 2002. Once submitted, PCII cannot be disclosed through a Freedom of Information Act (FOIA) request or through a request under a similar State, local, tribal, or territorial disclosure law; be disclosed in civil litigation; or be used for regulatory purposes.*

# CERTIFICATION STATEMENT AND EXPRESS STATEMENT FORM

Submitters may voluntarily submit critical infrastructure information for PCII protection under the Critical Infrastructure Information Act of 2002. All submissions must be accompanied by a Certification Statement and an Express Statement which initiates the protection of the critical infrastructure information throughout the review and validation process.

## CERTIFICATION STATEMENT

I am authorized to submit this information as one of the following (*please initial*):

_____Owner (or a representative) of a privately or publicly owned company;
_____Representative from an industry association;
_____Individual providing an informed observation of the critical infrastructure;
_____State/local/tribal/territorial government official (that can attest to voluntary participation);
_____Other: _____

*(Please initial)*:
_____To the best of my knowledge the information submitted is not customarily in the public domain. I am not submitting this information to comply with a regulatory requirement. I am not required to provide this information to a Federal regulatory entity.

## EXPRESS STATEMENT *(Please initial):*

_____I am submitting this information voluntarily. I am submitting this information to the Federal Government in expectation of protection from disclosure as provided by the provisions of U.S. Code Title 6, Chapter 1, Subchapter II, Part B, Section 133, and the Critical Infrastructure Information Act of 2002.

## ACCESS DISCLOSURE *(Please initial)*:

_____Individuals eligible to access PCII include Federal, State, local, tribal, or territorial government employees or contractors who meet the following requirements:

- Assigned to homeland security duties related to critical infrastructure; and Demonstrate a valid need-to-know; and
- Current authorized user (to include completion of all required authorized user training); and
- Such individuals must comply with the requirements stated in the Critical Infrastructure Information Act of 2002 and the Regulation (6 C.F.R. Part 29).

Submitter Signature_____Date _____

Protected Critical Infrastructure Information (PCII) Submission Form

## Submitter Contact Information:

Name *(please print)*: _____

Title:_____

Organization or Company Name: _____

Mailing Address: _____

City:_____State:_____Zip:_____

Office Telephone: _____

E-mail Address: _____

## Alternate Submitter Contact Information:

Name (please print): _____

Title:_____

Organization or Company Name: _____

Office Telephone: _____

E-mail Address: _____

Learn more about the DHS PCII Program at www.dhs.gov/pcii

## For PCII Program Office Only

Assessor Name: _____

Title: _____

Organization Name: _____

Office Telephone: _____

E-mail Address: _____

*DHS Form #: pending*
*Revised 08-05-14*
*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.*

# Protected Critical Infrastructure Information (PCII) Submission Requirements

**The Submitter (owner/operator) should be familiar with the Certification Statement and the PCII Express Statement, which are required for a proper submission.**

The Submitter should affirm one of the following:

- An owner (or a representative) of a privately or publicly owned company;
- A representative from an industry association;
- An individual providing an informed observation of the critical infrastructure; or
- A State/local/tribal/territorial government official (that can attest to voluntary participation).

The Submitter should read the following statements and affirm, to the best of his or her knowledge, that they are true:

- To the best of my knowledge the information submitted is not customarily in the public domain.
- I am not submitting this information to comply with a regulatory requirement. I am not required to provide this information to a Federal regulatory entity.
- I am submitting this information voluntarily.
- I am submitting this information to the Federal Government in expectation of protection from disclosure as provided by the provisions of U.S. Code Title 6, Chapter 1, Subchapter II, Part B, Section 133, and the Critical Infrastructure Information Act of 2002.

The Submitter should read the following statements and understand that:

- Individuals eligible to access PCII include Federal, State, local, tribal, or territorial government employees or contractors who are assigned to homeland security duties related to critical infrastructure, are trained in PCII rules, and demonstrate a valid need-to-know.
- Such individuals must comply with the requirements stated in the Critical Infrastructure Information Act of 2002 and 6 C.F.R. Part 29. They are required to take PCII Authorized User training and fulfill other access requirements.

Learn more about the DHS PCII Program at www.dhs.gov/pcii.

## Security Management Profile

- Does the facility have a written physical security plan? ○ Yes ○ No
    - Are personnel trained on the plan? ○ Yes ○ No
    - Is the plan exercised at least once a year? ○ Yes ○ No
- Is there a manager/department in charge of security management? ○ Yes ○ No
- Does the facility have procedures for suspicious packages? ○ Yes ○ No
- Does the facility participate in any security working groups? ○ Yes ○ No
- Are background checks conducted? ○ Yes ○ No
    - On all employees? ○ Yes ○ No
    - Are recurring background checks conducted? ○ Yes ○ No

# Security Force Profile

- Does the facility have a security force? ○ Yes ○ No
    - Is the security force armed? ○ Yes ○ No
    - Is the security force on site? ○ Yes ○ No
    - Are there static posts? ○ Yes ○ No
        - What percentage of the facility is covered?
            - ○ 1 – 25%
            - ○ 26 – 50%
            - ○ 51 – 75%
            - ○ 76 – 99%
            - ○ 100%
    - Are there roving patrols?
        - What percentage of the facility is covered?
            - ○ 1 – 25%
            - ○ 26 – 50%
            - ○ 51 – 75%
            - ○ 76 – 99%
            - ○ 100%

# Physical Security Profile

- Is the 100% of the facility enclosed in fencing? ○ Yes ○ No
- Is there a clear zone around the perimeter (an area that allows for clear sight of fence perimeter with no vegetation, objects or privacy slats)? ○ Yes ○ No
- Does the facility use vehicle gates? ○ Yes ○ No
- Does the facility use pedestrian gates? ○ Yes ○ No
- Does the facility have ground floor windows (less than 18 feet from the ground)? ○ Yes ○ No
    - Are there protective measures on the ground floor windows for the facility? ○ Yes ○ No
- Does facility have an air handling system with an external air intake less than or equal to 10 feet from the ground with unrestricted access? ○ Yes ○ No
- Does the facility utilize video surveillance? ○ Yes ○ No
    - Does a trained security staff monitor the video surveillance? ○ Yes ○ No
- For each of the following groups, are controls in place that limit entry?
    - Employees ○ Yes ○ No
    - Visitors ○ Yes ○ No
    - Contractors/Vendors ○ Yes ○ No
    - Customer/Patron/Public ○ Yes ○ No
- Can any vehicle be placed (legally or illegally) within 400 feet of the facility? ○ Yes ○ No
- Does the facility have one or more avenues of high-speed approach? ○ Yes ○ No
    - Does the facility use barriers to mitigate a high-speed avenue of approach? ○ Yes ○ No
- Does the facility use barriers to enforce standoff? ○ Yes ○ No

- Is the illumination of fences, gates, and parking areas similar and uniform in type with overlapping light patter coverage in most areas? ○ Yes ○ No
- Is the illumination of building entrance and delivery areas similar and uniform in type with overlapping light pattern coverage in most areas? ○ Yes ○ No
- Are illumination systems controlled by software applications? ○ Yes ○ No
- Does the facility utilize an interior intrusion detection method or application? ○ Yes ○ No
    - Are the intrusion detection systems controlled by software applications? ○ Yes ○ No
- Does the facility have a written agreement with entities other than emergency responders? ○ Yes ○ No
- Does the facility participate in security exercises or tabletops with outside agencies? ○ Yes ○ No

## Resilience Management Profile

- Is there a manager/department in charge of business continuity? ○ Yes ○ No
- Does the facility have a written business continuity plan? ○ Yes ○ No
    - Does the plan include both physical and cyber assets? ○ Yes ○ No
    - Are personnel trained on the plan? ○ Yes ○ No
    - Is the plan exercised at least once a year? ○ Yes ○ No
- Does the facility have a written Emergency Operation/Emergency Action Plan? ○ Yes ○ No
    - Does the plan include both physical and cyber assets? ○ Yes ○ No
    - Are personnel trained on the plan? ○ Yes ○ No
    - Is the plan exercised at least once a year? ○ Yes ○ No

## Information Sharing

- Does the facility receive threat information, security-related bulletins, advisories, and/or alerts from an external source? ○ Yes ○ No
- Does the facility share threat and/or security-related information with outside organizations? ○ Yes ○ No
- Does the organization receive threat information, to include cyber-security-related bulletins, advisories, and/or alerts on cyber attacks and actors, from an external source? ○ Yes ○ No
- Does the organization receive vulnerability information, to include cyber-security-related bulletins, advisories, and/or alerts on technical vulnerabilities, from an external source? ○ Yes ○ No
- Does the organization share cyber-security information with outside organizations? ○ Yes ○ No

## Cyber Security Management

- Is there a manager/department in charge of cyber security management? ○ Yes ○ No
- Is there an inventory of all critical cyber assets for this system? ○ Yes ○ No
- Is there a documented security architecture that includes each of the identified critical cyber security assets? ○ Yes ○ No
- Does the organization use system configuration monitoring procedures and/or tools that measure secure configuration elements and report configuration vulnerability information? ○ Yes ○ No
- Does the organization have a documented and distributed cyber change management policy and supporting procedures? ○ Yes ○ No
- Does the organization employ measures to address system and data confidentiality, integrity, and availability requirements throughout their life cycle (design, procurement, installation, operation, and disposal)? ○ Yes ○ No
- Does your organization implement at least one cyber-security standard(s) of practice (e.g., NIST SP800 series, NERC CIP, HIPAA, ISO/IEC 27000 series, etc.)? ○ Yes ○ No
- Is there a Cyber Security Plan covering the critical cyber security assets? ○ Yes ○ No
    - Are personnel trained on the plan? ○ Yes ○ No
    - Is the plan exercised at least once a year? ○ Yes ○ No
- Does the organization conduct cyber security exercises? ○ Yes ○ No

## Cyber Security Forces

- Are the following positions formalized within your organization?
    - Cyber Security Incident Response Team Lead/Incident Commander ○ Yes ○ No
    - Security Operations Personnel (i.e., Security Administrators, Security Analysts) ○ Yes ○ No
    - Security Architect ○ Yes ○ No
- Do cyber security personnel involved in day-to-day operations receive cyber training? ○ Yes ○ No

## Cyber Security Controls

- Has the organization established a process for identity proofing and authentication to limit access to the critical cyber systems to only authorized persons? ○ Yes ○ No

- Does the organization practice the concept of least privileges (i.e., users are only granted access to the information, file, and applications required to fulfill their roles and responsibilities)? ○ Yes ○ No

- Does the organization allow remote access to critical cyber services/assets? ○ Yes ○ No

- Which of the following cyber security measures does the organization employ for monitoring of networks related to the critical cyber system? Near-real-time monitoring for:

    - Malicious code ○ Yes ○ No

    - Unauthorized access ○ Yes ○ No

    - Intrusion detection ○ Yes ○ No

- Does the organization maintain security and event logs? ○ Yes ○ No

- Does the organization provide training on cyber security for critical cyber systems users? ○ Yes ○ No

## Incident Response

- Does the organization have predefined plans for responding to cyber security incidents? ○ Yes ○ No

- Should your site become inoperable, do you have access to an alternative location? ○ Yes ○ No

## Dependencies – Cyber

- Is the facility's core function dependent on data processing systems (mainframes, cloud providers, server farms, etc.)? ○ Yes ○ No
- Where is the location of the primary data processing systems and services? ○ Yes ○ No
    - Within the boundaries of the physical facility (on-site)? ○ Yes ○ No
    - At a data center located away from the facility (off-site data center, cloud service provider, etc.)? ○ Yes ○ No
        - Name
        - Address
        - City
        - State
        - ZIP
- Are your data processing and cyber security functions managed by a third-party service provider, vendor or contractor? ○ Yes ○ No
- Is the data storage required for the critical cyber system? ○ Yes ○ No
- Does the organization have alternative or backup storage capabilities that can be used in case of loss of the primary storage? ○ Yes ○ No
- If the primary mode of communication service is lost, is there a backup mode of communication? ○ Yes ○ No

# Dependencies – Electric

- Who is the facility's provider of electrical power?
    - Name
- What is the primary substation that the facility is dependent upon?
    - Name
    - Address
    - City
    - State
    - ZIP
- Is there a secondary or alternate substation for this facility? ○ Yes ○ No
    - Name
    - Address
    - City
    - State
    - ZIP
- Does the facility possess and maintain a backup generator(s) capable of running mission critical services for 72 hours? ○ Yes ○ No

# Dependencies – Natural Gas

- Is the facility's core function dependent on access to natural gas? ○ Yes ○ No
    - Who is the facility's provider of natural gas?
        - Name
    - What is the facility's primary source of natural gas?
        - Name
        - Address
        - City
        - State
        - ZIP
    - Is there a secondary source of natural gas? ○ Yes ○ No
        - Name
        - Address
        - City
        - State
        - ZIP
    - What is the delivery mechanism of the gas supply?
        - Pipeline ○ Yes ○ No
        - Truck ○ Yes ○ No

# Dependencies – Water

- Who is the facility's provider of water?
    - Name
- What is the facility's primary source of water?
    - Name
    - Address
    - City
    - State
    - ZIP
- Is there a secondary source of water? ○ Yes ○ No
    - Name
    - Address
    - City
    - State
    - ZIP
- Does the facility maintain onsite water storage capability capable of sustaining operations? ○ Yes ○ No

# Dependencies – Wastewater

- Is the facility's core function dependent on continuous access to wastewater discharge services? ○ Yes ○ No

    - Who is the facility's provider of wastewater discharge services?

        - Name

    - What is the facility's primary source of wastewater discharge services?

        - Name
        - Address
        - City
        - State
        - ZIP

    - Is there a secondary source of wastewater discharge services? ○ Yes ○ No

        - Name
        - Address
        - City
        - State
        - ZIP

## Dependencies – Communications

- Is the facility's core function dependent on continuous access to communications infrastructure (e.g., wired phone, wired data, cell phone, etc.)? ○ Yes ○ No

    - Name
    - Address
    - City
    - State
    - ZIP

# Dependencies – Transportation

- Is the facility's core function dependent on access to roadways, bridges, tunnels and highway infrastructure? ○ Yes ○ No
    - What are the key structures?
    - How long can a facility operate if these structures are compromised?

- Is the facility's core function dependent on access to any of the following transportation systems?
    - Rail ○ Yes ○ No
    - Air ○ Yes ○ No
    - Shipping ○ Yes ○ No
    - Waterways ○ Yes ○ No
    - Pipeline ○ Yes ○ No

## Dependencies – Critical Products

- Is the facility's core function dependent on access to chemicals and/or fuels? ○ Yes ○ No
    - What are the names of the chemical and/or fuel providers?
    - In the event of a disruption affecting your suppliers, do you have contracts with alternate suppliers? ○ Yes ○ No
- Is the facility's core function dependent on byproduct and waste removal? ○ Yes ○ No
- Is the facility's core function dependent on reliable access to raw materials such as metals, plastics, rubber, lumber, etc.? ○ Yes ○ No

## Dependencies – General

- If you are a supplier of critical goods or services to other entities please list them below.

- If your facility experiences an unplanned service interruption, what are the impacts or consequences to your customers, the public, or other suppliers in the subsector/segment?

    - Loss of operations or serviced
    - Significant impact
    - No impact
    - Minor impact

## Consequence

- Is the facility a lifeline critical infrastructure (e.g., a utility provider/asset)? ○ Yes ○ No

- Can other competitors or similar sister companies/facilities provide the product or service without major price impacts or delivery delays? ○ Yes ○ No

- What is the maximum facility population at any one time (include special events, employees, contractors and visitors)?

- Is the facility considered a Chemical, Biological, Radiological, Nuclear, or Explosive facility? ○ Yes ○ No

- What is the maximum offsite population that will be impacted by a reasonable worst case scenario at the facility (human impact such as death or injury, not economic impact)?

- Would an incident at the facility cause an immediate mass evacuation of the facility and a large population (over 20,000 people) within the surrounding area? ○ Yes ○ No

- Is the facility part of a designated system (e.g., electric grid, pipeline, railroad, or mass transit system)? ○ Yes ○ No

- What is the asset replacement value?

  ○ Less than $5,000,000
  ○ $5,000,001 to $20,000,000
  ○ $20,000,001 to $100,000,000
  ○ $100,000,001 to $500,000,000
  ○ $500,000,001 or greater

- What is the business interruption cost?
  ○ Less than $10,000,000
  ○ $10,000,001 to $100,000,000
  ○ $100,000,001 to $500,000,000
  ○ $500,000,001 to $1,000,000,000
  ○ $1,000,000,001 or greater

# Threat Identification

**Natural Hazards**

- ☐ Avalanche
- ☐ Animal Disease Outbreak
- ☐ Drought
- ☐ Earthquake
- ☐ Flood
- ☐ Hurricane
- ☐ Landslide
- ☐ Pandemic
- ☐ Tornado
- ☐ Tsunami
- ☐ Volcanic Eruption
- ☐ Wildfire
- ☐ Winter Storm
- ☐ Other
  Please specify:

**Technological (Accident)**

- ☐ Airplane Crash
- ☐ Dam Failure
- ☐ Levee Failure
- ☐ Mine Accident
- ☐ Hazardous Materials Release
- ☐ Power Failure
- ☐ Radiological Release
- ☐ Train Derailment
- ☐ Urban Conflagration
- ☐ Other
  Please specify:

**Human-Caused (Intentional)**

- ☐ Biological Attack
- ☐ Chemical Attack
- ☐ Cyber Incident
- ☐ Explosives Attack
- ☐ Radiological Attack
- ☐ Sabotage
- ☐ School and Workplace Violence
- ☐ Other
  Please specify:

**Cyber (Intentional)**

- ☐ Access via Wireless, Mobile, or Personal Devices
- ☐ Cloud Security
- ☐ Cyber Crime/Blackmail
- ☐ Data Breach/Loss
- ☐ Intellectual Property Theft/Corp Espionage
- ☐ Malware
- ☐ Distributed Denial of Service (DDOS)
- ☐ Code Injection
- ☐ Exploit Kits
- ☐ Social Media
- ☐ Targeted Cyber Attacks
- ☐ Other
  Please specify: