OMB Control Number: 1660-NEW
FEMA Form Number: 089-23
Expiration Date: XX-XX-XXXX

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Requirements for Use

Public reporting burden for this form is estimated to average 8 hours per response. The burden estimate includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and submitting the form. You are not required to respond to this collection of information unless it displays a valid OMB control number. Send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: Information Collections Management, Department of Homeland Security, Federal Emergency Management Agency, 500 C Street, SW, Washington, DC 20472, Paperwork Reduction Project (1660-NEW) NOTE: Do not send your completed form to this address.

Nondisclosure

This document contains PCII. In accordance with the provisions of 6 C.F.R. Part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq., the implementing Regulation at 6 C.F.R. Part 29 and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

Assigned to homeland security duties related to this critical infrastructure; and

Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the Critical Infrastructure Information Act of 2002 found at 6 U.S.C. § 131 et seq. and the implementing Regulation at 6 C.F.R. Part 29.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended**.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

> **Hand Delivery**: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.
>
> **Email**: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment**.**
>
> **Mail**: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER.**" Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Tracking Number(s) of the source document(s) must be included on the derivatively created document in the form of an endnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Tracking Number:

This page is intentionally left blank.

EXPRESS AND CERTIFICATION STATEMENT

Instructions: For all submissions requesting PCII protection, the Express and Certification Statement included in the template should be completed and signed by an authorized State Administrative Agency (SAA) official, which may be the SAA Buffer Zone Protection Program (BZPP) point of contact (POC). Please note that electronic signatures are allowed.

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 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:

Office Telephone: Alternate Telephone:

E-Mail Address:

Alternate Contact Information

Name:

Title:

Organization or Company Name (if different from submitter):

Mailing Address: City: State:

Office Telephone: Alternate Telephone:

E-Mail Address:

Please be aware that 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.

Buffer Zone Plan

(Facility Name)

,

(Location: City/County, State)

,

(Date Completed by Responsible Jurisdiction: Month DD, YYYY)

Insert ".jpg" site photo

This Plan was developed based on a cooperative effort among (Critical Infrastructure/Key Resource Name), (Responsible Jurisdiction Name),
and the U.S. Department of Homeland Security.

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

BZP	Buffer Zone Plan
BZPP	Buffer Zone Protection Program
CBRN	Chemical, Biological, Radiological, Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure/Key Resources
CPU	Central Processing Unit
DHS	(U.S.) Department of Homeland Security
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GIS	Geographic Information System
HAZMAT	Hazardous Materials
HSAS	Homeland Security Advisory System
HSGP	Homeland Security Grant Program
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IT	Information Technology
JTTF	Joint Terrorism Task Force
LLE	Local Law Enforcement
LVIED	Large-Vehicle Improvised Explosive Device
MARSEC	Maritime Security
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
N/A	Not Applicable
NADB	National Asset Database
NCIC	National Crime Information Center
NIC	NIMS (National Incident Management System) Integration Center
NIMS	National Incident Management System
NRP	National Response Plan
PCII	Protected Critical Infrastructure Information
POC	Point of Contact
PPE	Personal Protective Equipment
PSA	Protective Security Advisor
PSCD	Protective Security Coordination Division
SAA	State Administrative Agency
SCADA	Supervisory Control and Data Acquisition
SOP	Standard Operating Procedure
SSP	Sector-Specific Plan
SWAT	Special Weapons and Tactics
TIC	Toxic Industrial Chemical
TSGP	Transit Security Grant Program
U.S.C.	United States Code
VBIED	Vehicle-Borne Improvised Explosive Device
VIP	Very Important Person
VRPP	Vulnerability Reduction Purchasing Plan

1.0 INTRODUCTION

The Protective Security Coordination Division (PSCD) of the U.S. Department of Homeland Security (DHS) is responsible for leading the Department's efforts to reduce the Nation's vulnerability to terrorism and deny the use of U.S. critical infrastructure and key resources (CI/KR) as a weapon. In support of this objective, PSCD is developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize, and protect CI/KR in cooperation with all levels of government and partners in the private sector.

In coordination with the DHS Federal Emergency Management Agency (FEMA), PSCD has developed a Buffer Zone Protection Program (BZPP) to provide targeted grants that enhance the protection of CI/KR across the country. The purpose of the Program is to make it more difficult for terrorists to conduct planning activities or successfully launch attacks from the immediate vicinity of CI/KR targets. The program is based on the premise that State and local law enforcement (LLE) agencies and first responders are first preventers on the front lines in preparing, preventing, defending against, and mitigating the impacts of terrorist attacks against our Nation. To this end, the BZPP was conceived to increase the general awareness, protective capacity and preparedness of State law enforcement, LLE, and other first responders as first preventers in communities surrounding CI/KR facilities by: 1) establishing buffer zones around individual assets, 2) developing Vulnerability Reduction Purchasing Plans (VRPPs) to identify planning activities and equipment shortfalls needed to mitigate vulnerabilities and/or capability gaps identified in the individual Buffer Zone Plans (BZPs) and protect these assets effectively, 3) providing the financial resources necessary to execute approved VRPP procurements, and 4) verifying and validating that expenditures will adequately mitigate vulnerabilities and/or capability gaps identified in the individual BZPs.

The purpose of a BZP is to assist State law enforcement, LLE, and other first responders in the analysis of threats and vulnerabilities to a CI/KR site and its significant assets in order to develop effective site-specific preventive and protective measures that make it more difficult for terrorists to target and attack CI/KR sites successfully. Specifically, a BZP will assist in:

- Identifying significant assets at a particular site that may be targeted by terrorists for attack;
- Identifying specific threats and vulnerabilities associated with the site and its significant assets;
- Developing an appropriate buffer zone extending outward from the facility in which protective measures can be employed to make it more difficult for terrorists to conduct site surveillance, engage in other preliminary activities, or initiate attacks;
- Identifying all responsible law enforcement jurisdictions—to include Federal, State, and local agencies—with a role in the prevention of, protection against, and response to terrorist threats or attacks specific to the CI/KR site and identifying the appropriate points of contact within these organizations;
- Evaluating the capabilities of the responsible law enforcement jurisdictions with respect to terrorism prevention and response; and
- Identifying specific planning, equipment, training, and/or exercise capabilities needed by the responsible jurisdictions to mitigate the threats and vulnerabilities of the site and its buffer zone.

A BZP is designed to complement, and not supersede, existing site plans developed for response to terrorist threats or attacks. It is intended to foster a cooperative environment in which Federal, State, and local authorities, along with private industry, can carry out their respective prevention and protection responsibilities for our Nation's CI/KR more efficiently and effectively. Additionally, in developing and implementing BZPs, security and preparedness officials at all levels should seek opportunities to coordinate and leverage funding from multiple sources, including Federal, State, and local resources.

A BZP is required as documentation to justify resource requests and expenditures from responsible jurisdictions for grants under the Fiscal Year (FY) 2009 BZPP.

2.0 SITE IDENTIFICATION

*** NOTE: Some information may be provided by DHS in the initial background package. If so, it must be verified prior to submission of this document to ensure it is current and accurate.**

2.1 Site-Specific Information

SPECIFICS	COMPLETE THE FOLLOWING:
Site Name	
Site Address	
Site Owner/Operator Name	
Site Owner/Operator Address	
Site POC Name	
Site POC Phone Number	

2.2 Site General Characteristics

Critical Infrastructure Sector	
Critical Infrastructure Segment	
Critical Infrastructure Attribute	
Description of Site	
Area: Acreage or Square Footage	• Acres, Total: • Acres, Developed: • Acres, Undeveloped: Describe: • Acres, Wooded: Describe: • Square Footage:
Number of Structures	• Buildings: Describe: • Other:
Elevation: Number of Floors Above Ground	• Highest structure on site by number of floors above ground level: Describe:
Elevation: Number of Floors Below Ground	• Deepest structure on site by number of floors below ground level: Describe:
Number of Employees	
Total Number	(total)
Permanent	(employees)
Contractor	(on site)
Temporary	(temp agency-sourced)
Seasonal	(type and number)

Hours of Operation **If more than one shift, include the number and timing of shifts, and the number of employees on each shift.**	Hours: Number of Shifts: Timing of Shifts: Number of Employees on Each Shift:
Number of Visitors as applicable: **1. Per Day** **2. Per Year** **3. Per Event**	* (e.g.: Including vendors and delivery people, there are approximately 30-40 visitors per day. All visitors are logged in upon arrival and logged out before exiting.) 1. 2. 3.

2.3 Overview

Provide Geographic Information System (GIS) maps, street maps, satellite imagery, aerial photographs, and/or other maps, detailed schematic drawings, or other pictorial representations of the site/facility as appropriate.

2.3.1 General Location Map

Use a GIS map format to identify the general location of the BZP site at the city or county level.

Insert “.jpg” Image Here

Action: Insert map that shows the general location of the BZP site at the city or county level.
(Background package may include maps for this section)

Insert Caption for Image

2.3.2 Street-Level Location Map

Insert “.jpg” Image Here

Action: Insert map that shows named streets and roadways.
(Background package may include maps for this section)

Insert Caption for Image

2.3.3 Overhead Aerial/Satellite Photographs, Map Images, Detailed Schematic Drawings, and/or Other Pictorial Representations of Site/Facility

Insert ".jpg" Image(s) Here

Action: Insert Overhead Aerial/Satellite Photographs, Map Images, Detailed Schematic Drawings, and/or Other Pictorial Representations of Site/Facility.

Insert caption(s) for photos

3.0 IDENTIFICATION OF CRITICAL SITE OPERATIONS AND SIGNIFICANT ASSETS

3.1 Description of Site Operations

Purpose of Site	
Key Products/Services	
Key Customers or Industries Supported	
Type, Quantity, and Storage Medium of Hazardous Materials (HAZMAT), if applicable	
Other Activities Posing Public Health/Environmental Hazards	

3.2 Criticality of Site or Site Operations

Proximity to Heavily Populated Areas or Other Areas of Strategic Interest	
Production of Resources Critical to National or Regional Needs	
National/Regional Economic Impacts	
Environmental Consequences	
National Security Impacts	
Symbolic Importance	
Other Socio-Political Impacts	
Support to Other Critical Infrastructure	

3.3 Standard Operating Procedures

Documented Standard Operating Procedures (SOPs) exist for the following emergencies:

Break-Ins	□ No □ Yes
HAZMAT Spills/Releases	□ No □ Yes
Hostage Situations	□ No □ Yes
Natural Disasters	□ No □ Yes
Terrorist Incidents	□ No □ Yes

3.4 Consequences of Attack on Facility

Likely consequences of an attack upon the facility—to include impacts to facility operations, the economy, and to environment, safety, and health—are identified in the table below.

*** NOTE: Check the most appropriate box applicable to each category. Mark only one response.**

CONSEQUENCES OF ATTACK ON FACILITY	RESPONSE
Loss of Operations, Estimated Costs (24 hours)	□ $1,000,000 and higher □ $500,000 – $999,999 □ $250,000 – $499,999 □ $100,000 – $249,999 □ Less than $100,000
Replacement Cost of Facility	□ $10,000,000,000 and higher □ $1,000,000,000 – $9,999,999,999 □ $500,000,000 – $999,999,999 □ $100,000,000 – $499,999,999 □ Less than $100,000,000

CONSEQUENCES OF ATTACK ON FACILITY	RESPONSE
Economic Impact	□ International □ National □ Regional □ Local (Note: Select only the highest applicable category; e.g., national impacts are presumed to include lesser regional and local impacts.)
Environmental, Safety, and Health Impacts (Worst-Case Scenario)	□ Extend off site with population impacts > 100,000 □ Extend off site with population impacts of 50,000 – 99,999 □ Extend off site with population impacts of 10,000 – 49,999 □ Extend off site, with population impacts of < 10,000 □ Extend off site, with no population impacts □ Limited to on site

3.5 Infrastructure Dependencies

INFRASTRUCTURE DEPENDENCIES	DEFINE WHAT THE SITE'S CONSEQUENCES OF LOSS ARE AND IDENTIFY ANY REDUNDANCIES IN PLACE.
Energy	
Telecommunications	
Transportation	
Water	
Other	

3.6 Identification of Significant Areas/Assets

The following site areas and/or assets are determined to be significant to site operations and/or public safety and thus warrant enhanced preventive and protective measures against terrorist attack.

SIGNIFICANT AREA/ASSET	CHARACTERISTICS	DESCRIPTION OF LOCATION AND LATITUDE/LONGITUDE
	Describe: Consequence of loss:	Location: Latitude: Longitude:
	Describe: Consequence of loss:	Location: Latitude: Longitude:
	Describe: Consequence of loss:	Location: Latitude: Longitude:
	Describe: Consequence of loss:	Location: Latitude: Longitude:
	Describe: Consequence of loss:	Location: Latitude: Longitude:
	Describe: Consequence of loss:	Location: Latitude: Longitude:

3.7 Photographs of Significant Areas/Assets

Insert ".jpg" Photo(s) of Significant Areas/Assets at Facility

Insert Caption

3.8 Security Implementation Table

Overall security within and surrounding this CI/KR site will be significantly increased through implementation of the buffer zone protection measures recommended below. These protective measures reduce the risk associated with specific operational based threats.

HOMELAND SECURITY ADVISORY SYSTEM (HSAS) LEVEL	PROTECTIVE MEASURE	PURPOSE (Devalue, Detect, Deter, Defend)	AGENCY / DEPARTMENT	STATUS (In Place or Option for Consideration)
GREEN (Low)	At this time, normal operating condition is no lower than YELLOW.			
BLUE (Guarded)				
YELLOW (Elevated)				
ORANGE (High)				
RED (Severe)				

3.9 Correlation of Threat Levels

Does the facility utilize HSAS?	□ No □ Yes
If applicable, other threat level systems used at this facility and their correlation to HSAS are identified below. **Ex: Maritime Security (MARSEC) Level 1 = HSAS Green, Blue, Yellow**	
Does the facility receive sector-specific threat information and trends from the State or regional Fusion Center?	□ N/A □ No □ Yes
Does the facility receive notification of changes to sector-specific or national HSAS threat levels from the State or regional Fusion Center?	□ No, Describe how notifications are received: □ Yes

4.0 THREAT IDENTIFICATION

Terrorists have a variety of weapons and tactics available to achieve their objectives. Attacks can be carried out by individuals, small teams of perpetrators, or larger groups acting in a coordinated fashion. Significant site assets should be evaluated for their vulnerability to each of the following six threat streams based on the vulnerability factors presented below.

*** NOTE: Complete and accurate information is critical to the BZPP. Therefore, describe each "Yes" response in full detail.**

4.1 Improvised Explosive Device (IED) – Worn, Carried, Placed Bomb, and Vehicle-Borne

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR IED ATTACK	VULNERABILITY
Uninhibited avenues of approach exist that would enable the transport of an IED. (Note: e.g., sidewalks, roads, parking lots, and public forms of transportation are abundant in the vicinity.)	□ N/A □ No □ Yes, Describe:
High-speed avenues of approach exist for a vehicle-borne IED (VBIED). (Note: e.g., wide sidewalks, roads, adjacent parking lots)	□ N/A □ No □ Yes, Describe:
Parking is permitted (above or below ground) near key assets, thus enabling a VBIED attack.	□ N/A □ No □ Yes, Describe:
Concealed drop-off points exist to hide an IED (e.g., mail boxes, garbage cans).	□ N/A □ No □ Yes, Describe:
There are multiple entry/exit points to/from the facility.	□ N/A □ No □ Yes, Describe: (Note: Include all, regardless of condition, as locked/barred or obstructed. Specify if operational and/or how door use is restricted, e.g., broken or chained, etc.)

FACTORS FOR IED ATTACK	VULNERABILITY
Identifiable physical security measures exist at the facility that are obvious to the casual observer. (Note: e.g., fence, closed-circuit television (CCTV), uniformed guards.)	□ N/A □ No □ Yes, Describe:
The facility is normally open to the public.	□ N/A □ No □ Yes, Describe: (Note: Conditional situations that exist such as time constraints or specific times of exclusion should be noted.)
The facility is periodically open to the public.	□ N/A □ No □ Yes, Describe: (Note: Conditional situations that exist such as the existence of planned open house activities or civic event times and duration should be defined.)
LLE response time to facility is more than 5 minutes.	□ N/A □ No □ Yes, Describe:
Identifiable unique structures, colors, location, or signage exist at the facility that are obvious to the casual observer and call attention to the facility or its assets.	□ N/A □ No □ Yes, Describe:
Large numbers of people congregate at the facility and/or its assets.	□ N/A □ No □ Yes, Describe:
Detection devices or measures are in place to identify an adversary or potential IED/VBIED. (Note: e.g., magnetometers or mail pre-screening.)	□ N/A □ No □ Yes, Describe:
There is a readily accessible staging area for surveillance and direct lines of sight.	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:

4.2 Biological Weapon/Chemical Weapon/Radiological Dispersion Device

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR CHEMICAL, BIOLOGICAL, RADIOACTIVE, NUCLEAR (CBRN) ATTACK	VULNERABILITY
Exhaust ducts exist at street level in the immediate vicinity of high-value targets, thus allowing a biological/chemical agent to be disseminated to a broader population.	□ N/A □ No □ Yes, Describe:
Air intakes are easily accessible to high-value targets, thus allowing biological/chemical agent induction to the site. (Note: e.g., ground level or open access from the roof)	□ N/A □ No □ Yes, Describe:
Food and water systems are accessible for contamination. (Note: e.g., at point of entry, food is prepared off site, etc)	□ N/A □ No □ Yes, Describe:
There is an enclosed system capable of spreading a biological/chemical agent great distances. (Note: e.g., consider tunnel networks, sewer systems, service races, etc.)	□ N/A □ No □ Yes, Describe:
There are areas where there is the ability to deliberately contaminate surfaces with biological toxins.	□ N/A □ No □ Yes, Describe:
There are large open spaces where people gather.	□ N/A □ No □ Yes, Describe:
Detection devices or measures are in place to identify biological/chemical/radioactive agents through delivery of packages and mail. (Note: e.g., bio-detection, x-ray, ion-scan systems, etc.)	□ N/A □ No □ Yes, Describe:
The facility has accessible biological/chemical/ radioactive agents on site (e.g., in a research and development lab).	□ N/A □ No □ Yes, Describe:
Loss of facility areas for re-entry would cause mass chaos and loss of operations for a long period of time.	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:

4.3 Toxic Industrial Chemicals (TICs)/HAZMAT Release

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR TIC/HAZMAT ATTACK	VULNERABILITY
There is significant population density in the area that could be impacted by a release. (i.e., population density greater than 200,000)	□ N/A □ No □ Yes, Describe:
Presence of TIC/HAZMAT on site is readily apparent. (Note: e.g., recognizable items are visible such as chemical tanks/vessels that are labeled or constructed to indicate toxic or hazardous contents; chemical monitors or workers in personal protective equipment (PPE) indicate on-site toxic hazards.)	□ N/A □ No □ Yes, Describe:
First responders are adequately equipped or trained to respond to a TIC or HAZMAT release.	□ N/A □ No, Describe: □ Yes, Describe:
Facility TIC/HAZMAT response times are adequate.	□ N/A □ No, Describe: □ Yes
On-site response capability for a TIC/HAZMAT release exists.	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:
Caveats and exceptions or anomalies exist to the statements above.	□ N/A ☒ No □ Yes, Describe:

4.4 Airborne Attack (Use of Aircraft as a Weapon)

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR AIRBORNE ATTACK	VULNERABILITY
There are uninhibited avenues of approach to the facility by air. (Note: e.g., no-fly zones, airports in the vicinity)	□ N/A □ No □ Yes, Describe:
The facility is obviously identifiable from the air during the day. (Note: e.g., by virtue of unique structure, color, location, signage, shape or size)	□ N/A □ No □ Yes, Describe:
The facility is obviously identifiable from the air at night. (Note: e.g., by virtue of lighting, shape, or size)	□ N/A □ No □ Yes, Describe:
Local response capability includes coordination of civil combat air patrol and/or LLE aircraft.	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:

4.5 Maritime Attack (Use of Watercraft as a Weapon)

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR WATERBORNE ATTACK	VULNERABILITY
The facility is near a navigable waterway.	□ No (Skip to Section 4.6.) □ Yes, Describe:
There are uninhibited avenues of approach to the facility by water.	□ N/A □ No □ Yes, Describe: (Note: List all types and sizes. Include mitigating factors such as current flow.)
Significant asset(s) are located on or in close proximity to the water's edge and are visible from	□ N/A □ No

the waterway. (Note: e.g., by virtue of unique structure, color, location, or signage.)	□ Yes, Describe:
There are navigable routes with acceptable depths in and around the facility or significant assets. (Note: high and low tides, minimum depth, currents, etc.)	□ N/A □ No □ Yes, Describe:
Navigable waterways exist that are usable 24/7. Travel access times are unlimited. (Note: e.g., by tides and currents)	□ N/A □ No □ Yes, Describe:
Man-made or natural barriers in the waterway exist that impede direct access to the facility.	□ N/A □ No □ Yes, Describe:
Stand off in or around significant assets exists.	□ N/A □ No □ Yes, Describe:
Discernable perimeter security exists in and around the facility.	□ N/A □ No □ Yes, Describe:
Lighting is such that critical asset(s) are easily recognizable from the water during evening hours.	□ N/A □ No □ Yes, Describe:
Perimeter security is well defined, but factors such as clutter and vegetation on shore provide cover and concealment for staging waterborne attacks. (Note: e.g., able to stage vessel-borne IED attack or insert assaulters near asset)	□ N/A □ No □ Yes, Describe:
Waterborne response agencies exist. (e.g., Coast Guard, LLE)	□ N/A □ No □ Yes, Describe: (Include responders and estimated response times.)
Unsecured communications can be monitored via marine band radio.	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:

4.6 Hostage Barricade, Abduction/Kidnapping, and/or Assault/Assassination

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR HOSTAGE BARRICADE, ABDUCTION/ KIDNAPPING, AND/OR ASSAULT/ASSASSINATION	**VULNERABILITY**
Key individuals who are likely targets work/reside in this facility.	□ N/A □ No □ Yes (Note: Identify/describe in boxes below.)
Key individuals in this facility who are likely targets include: (Note: e.g., designers, researchers, technicians, scientists, visitors during special events)	1. □ Executives 2. □ Members of the Board of Directors 3. □ Key Knowledge Workers 4. □ Children of Very Important Persons (VIPs)/High-Profile Individuals 5. □ Dignitaries. Describe: 6. □ High-Profile Individuals. Describe: 7. □ Persons of International Relevance. Describe:
High-priority groups that are likely targets work/ reside in this facility. (Note: e.g., Technical Development Teams etc.)	□ N/A □ No □ Yes (Note: Identify/describe in boxes below.)
High-priority groups that are likely targets in this facility include:	□ Groups of children. Describe: (e.g., schools, churches, day care centers) □ Groups of personnel. Describe: (e.g., religious, political, organizational) □ Others. Describe:
There is a readily accessible staging area for surveillance with a direct line of sight to the facility.	□ N/A □ No □ Yes, Describe:
Key individuals who are likely targets visit this facility.	□ N/A □ No □ Yes, Describe:
High-priority groups who are likely targets visit this facility. (Note: e.g., Technical Development Teams etc.)	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:

4.7 Cyber Attack

Vulnerability assessment: Identification of the vulnerabilities associated with this threat stream. (Note: Identify if it is the facility as a whole, or specific Significant Areas/Assets in particular, which are vulnerable to this specific attack.)	□ This threat stream is not applicable. (Explain.) □ Facility □ Significant Areas/Assets 1. 2. 3.

FACTORS FOR CYBER ATTACK	VULNERABILITY
Information technology (IT) systems are critical to facility operations.	□ N/A □ No □ Yes, Describe:
The facility has a cyber security plan.	□ N/A □ No □ Yes, Describe:
The facility has a remote access system or modem connection.	□ N/A □ No □ Yes, Describe:
The facility has a Supervisory Control and Data Acquisition (SCADA) system.	□ N/A □ No □ Yes, Describe:
Other (Please describe.)	□ No □ Yes, Describe:

5.0 SECURITY CHECKLISTS

The purpose of this section is to assist in determining those characteristics of the facility and/or its buffer zone that render it vulnerable to terrorist attack or exploitation. The information gathered from these checklists will be used to determine site vulnerabilities, as well as the preventive and/or protective measures to be taken during the various HSAS threat level changes.

5.1 Facility Management Security

This checklist assesses facility security, human resources, and other management practices that may affect facility security.

FACILITY MANAGEMENT	DESCRIPTION
Formal documented security plan(s) exist.	□ N/A □ No □ Yes, Describe:
Formal documented security plan(s) are available to all employees.	□ N/A □ No, Describe: □ Yes
Formal documented threat definition and assessment statement(s) exist.	□ N/A □ No □ Yes, Describe:
Formal documented threat definition and assessment statement(s) are available to all employees.	□ N/A □ No, Describe: □ Yes
Initial security awareness training is provided to all employees.	□ N/A □ No, Describe: □ Yes, Describe:
Refresher security awareness training is provided annually.	□ N/A □ No, Describe: □ Yes, Describe:
The facility has a security force.	□ N/A □ No □ Yes, Describe: (Note: Specify whether these are company or contractor employees.)
How many individuals comprise the security force?	(Note: Include shifts and number of personnel per shift.)
Additional security force personnel are used during heightened threat levels.	□ N/A □ No □ Yes, Describe:
Members of the security force have arrest authority.	□ N/A □ No □ Yes, Describe: (Note: Include number of or percentage of the force with this authority.)
Security-related SOPs exist and are documented.	□ N/A □ No □ Yes, Describe:

FACILITY MANAGEMENT	DESCRIPTION
Security force personnel train and employ documented SOPs.	□ N/A □ No □ Yes, Describe:
Initial background checks are made on all new employees.	□ N/A □ No □ Yes, Describe:
Security force personnel are reinvestigated yearly.	□ N/A □ No □ Yes, Describe:
Preliminary background checks are made on all temporary employees.	□ N/A □ No □ Yes, Describe:
Initial background checks are made on all temporary employees and contractors.	□ N/A □ No □ Yes, Describe:
Reinvestigations are made on all temporary employees and contractors annually for long-term contracts.	□ N/A □ No □ Yes, Describe:
Executive protection program(s) exist for senior executives/managers.	□ N/A □ No □ Yes, Describe:
Memoranda of understanding (MOUs) and/or memoranda of agreement (MOAs) regarding security measures are in place with adjacent facilities for mutual support.	□ N/A □ No □ Yes, Describe:

5.2 Surveillance Security

This checklist assesses the facility's vulnerability to surveillance and the existence or effectiveness of measures in place to protect against surveillance.

SURVEILLANCE	DESCRIPTION
Locations outside the facility exist that allow viewing of sensitive operations.	□ N/A □ No □ Yes, Describe:
Higher elevation areas around the facility exist that enhance the probability for surveillance and attack scenarios (e.g., hills, buildings, parking structures, other facilities, etc.).	□ N/A □ No □ Yes, Describe:
Commercial, public, or private buildings exist that allow long-term surveillance to go undetected.	□ N/A □ No □ Yes, Describe:
Bus stops, taxi stands/drops, or other areas used for public transportation exist that can be used as staging areas with lines of sight to the facility.	□ N/A □ No □ Yes, Describe:

SURVEILLANCE	DESCRIPTION
Normal activities occur outside the facility that allow for close proximity to restricted areas and/or the facility's perimeter by unauthorized personnel.	□ N/A □ No □ Yes, Describe:
Counter-surveillance teams are utilized during elevated threat levels.	□ N/A □ No □ Yes, Describe:
Trained counter-surveillance teams are available to the facility. (Note: e.g., LLE may provide if available.)	□ N/A □ No □ Yes, Describe:
Pedestrian and/or auto traffic has uninhibited access to routes allowing moving surveillance of the facility.	□ N/A □ No □ Yes, Describe:
Known deficiencies exist in the facility's security perimeter.	□ N/A □ No □ Yes, Describe:
Adjacent facilities have mutual/comparable security measures in place to prevent, limit, or monitor access to shared boundaries.	□ N/A □ No □ Yes, Describe:
Procedures exist that identify and verify disabled vehicles, personnel, etc. found in close proximity to the facility's security perimeter or critical facility components.	□ N/A □ No □ Yes, Describe:
Measures exist to visually record vehicles or personnel who approach or cross into the facility.	□ N/A □ No □ Yes, Describe:
"Warning" signs exist and are placed where clearly visible (e.g., no trespassing, beware of dog, cameras in use, video surveillance in use).	□ N/A □ No □ Yes, Describe:
Opportunities exist for contractors, vendors, visitors, etc. to obtain unrestricted access to the facility or restricted areas.	□ N/A □ No □ Yes, Describe:
Procedures exist for reporting suspicious personnel or activities.	□ N/A □ No □ Yes, Describe:

5.3 Buffer Zone Security

The following checklist assesses the security of the facility's buffer zone.

BUFFER ZONE SECURITY	DESCRIPTION
An exclusive buffer zone currently exists outside of the external physical perimeter to the facility or critical component.	□ N/A □ No □ Yes, Describe:
Critical components/assets exist outside of the facility's physical perimeter.	□ N/A □ No □ Yes, Describe: (Note: Include proximity to and/or distance from perimeter. e.g., located adjacent to, in the vicinity of, or remote at some specified distance)
Public roads exist that allow access to critical facility components outside of the facility's physical perimeter.	□ N/A □ No □ Yes, Describe:
Additional avenues of approach for pedestrian or auto traffic exist that allow access to critical facility components outside of the facility's physical perimeter.	□ N/A □ No □ Yes, Describe:
Waterways that flow through the facility's grounds and/or within the buffer zone are monitored/patrolled.	□ N/A □ No □ Yes, Describe:
Parking is allowed within the established buffer zone.	□ N/A □ No □ Yes, Describe:
Loaded trucks and/or railcars stop or park at or near the facility.	□ N/A □ No □ Yes, Describe:
Vehicle parking areas within the buffer zone are observed and monitored from security checkpoints or other occupied security offices.	□ N/A □ No □ Yes, Describe:
Vehicle parking areas in the buffer zone are illuminated.	□ N/A □ No □ Yes, Describe:
Buffer zone areas have sufficient lighting for security. (Note: e.g., parking lots, walkways, roads etc.)	□ N/A □ No, Describe: □ Yes, Describe:

BUFFER ZONE SECURITY	DESCRIPTION
Passive vehicle barriers are employed to prevent vehicles from entering the buffer zone. (Note: e.g., Jersey barriers, buried ties, concrete planters, cables)	□ N/A □ No □ Yes, Describe:
Active barriers are employed to exclude vehicles from entering the buffer zone. (Note: e.g., hydraulic lift gates)	□ N/A □ No □ Yes, Describe:
Temporary barriers are employed to exclude vehicles from entering the buffer zone. (Note: e.g., vehicles, portable wheel spikes, water-filled Jersey barriers)	□ N/A □ No □ Yes, Describe:
Dumpster and trash receptacles exist as vehicle barriers within the buffer zone.	□ N/A □ No □ Yes, Describe:

5.4 Physical Security

PHYSICAL SECURITY	DESCRIPTION
Fences and gates exist within the buffer zone.	□ N/A □ No □ Yes, Describe:
Fence and gate components of the facility perimeter are in good repair.	□ N/A □ No, Describe: □ Yes
Fence and gate components of the facility perimeter have alarms.	□ N/A □ No □ Yes, Describe:
Fence and gate components of the facility perimeter are reinforced or are otherwise protected against vehicle intrusion. (Note: e.g., trench line precedes the fence.)	□ N/A □ No □ Yes, Describe:
Fence and gate components of the facility perimeter are clear of vegetation.	□ N/A □ No, Describe: □ Yes
Fence and gate components of the facility perimeter are clearly marked with visibly well placed “warning” signs along the perimeter.	□ N/A □ No □ Yes, Describe:

PHYSICAL SECURITY	DESCRIPTION
Gates control vehicular and/or pedestrian access to the facility.	□ N/A □ No □ Yes, Describe:
Gates are manned 24/7.	□ N/A □ No □ Yes, Describe: (Note which are and are not.)
Gates are controlled by a card reader system and/or other automated access control system.	□ N/A □ No □ Yes, Describe: (Note which are and are not.)
Fence and gate components of the facility perimeter are adequately illuminated.	□ N/A □ No, Describe: □ Yes
Vehicle barriers exist within the buffer zone.	□ N/A □ No □ Yes, Describe:
Speed control obstacles are employed to prevent vehicles from running checkpoints or vehicle search areas during elevated alert levels.	□ N/A □ No □ Yes, Describe:
Passive vehicle barriers are employed to protect critical components from Large-Vehicle Improvised Explosive Devices (LVIEDs). (Note: e.g., Jersey barriers, buried ties, concrete planters, cables)	□ N/A □ No □ Yes, Describe:
Vehicle searches are performed within the buffer zone.	□ N/A □ No □ Yes, Describe:
Delivery vehicles are routinely screened and inspected upon entry to the facility.	□ N/A □ No □ Yes, Describe:
During elevated threat levels, passenger vehicles are searched prior to being permitted to enter the facility.	□ N/A □ No □ Yes, Describe:
Explosives detection canines are available for facility security sweeps.	□ N/A □ No □ Yes, Describe: (Note: Identify applicable conditions.)

PHYSICAL SECURITY	DESCRIPTION
Intrusion detection systems (IDSs) exist within the buffer zone.	□ N/A □ No □ Yes, Describe:
The facility employs an exterior IDS.	□ N/A □ No □ Yes, Describe:
The facility's IDS provides specific dedicated coverage for significant facility assets.	□ N/A □ No, Describe: □ Yes, Describe:
The facility employs CCTV.	□ N/A □ No □ Yes, Describe: (Include the total number of cameras and key assets monitored.)
All significant facility assets are under CCTV coverage.	□ N/A □ No, Describe: □ Yes, Describe:
Security patrols are performed within the buffer zone.	□ N/A □ No □ Yes, Describe:
Daily after-hours security checks are made of all facility access points.	□ N/A □ No □ Yes, Describe:
The perimeter is checked routinely by the facility security force.	□ N/A □ No □ Yes, Describe:
Security force checks are all recorded.	□ N/A □ No □ Yes, Describe: (Note: Include intervals)
Access control exists within the buffer zone.	□ N/A □ No □ Yes, Describe:
Identity badges are used to authenticate employees and authorized personnel.	□ N/A □ No □ Yes, Describe: (Note: Identify frequency of verification.)

PHYSICAL SECURITY	DESCRIPTION
Facility access passes and/or decals are used to identify authorized vehicles.	□ N/A □ No □ Yes, Describe:
Access control devices are used to gain entry to the facility. (Note: e.g., employee badges, swipe/proximity cards, biometric devices)	□ N/A □ No □ Yes, Describe:
Access control devices are used to gain entry to critical assets and/or areas of interest within the facility. (Note: e.g., employee badges, swipe/proximity cards, biometric devices)	□ N/A □ No □ Yes, Describe:
Screening devices are used to detect the presence of weapons, explosives, and/or other unauthorized items. (Note: e.g., dogs, metal detectors, X-rays)	□ N/A □ No □ Yes, Describe:
Visitor access control exists within the buffer zone.	□ N/A □ No □ Yes, Describe:
Visitors are required to sign in with security.	□ N/A □ No □ Yes, Describe:
Visitors are issued temporary badges that identify them as visitors.	□ N/A □ No □ Yes, Describe:
Visitors must be escorted at all times everywhere in the facility.	□ N/A □ No, Describe: □ Yes, Describe:
Visitors must be escorted in sensitive facility locations only.	□ N/A □ No □ Yes, Describe:
Radio communications exist within the buffer zone.	□ N/A □ No □ Yes, Describe:
Radio communications within the buffer zone are clear and unrestricted.	□ N/A □ No, Describe: □ Yes, Describe:
Other communications exist within the buffer zone.	□ N/A □ No □ Yes, Describe:

PHYSICAL SECURITY	DESCRIPTION
Other communications within the buffer zone are clear and unrestricted.	□ N/A □ No, Describe: □ Yes, Describe:
A designated command center exists within the facility.	□ N/A □ No □ Yes, Describe:
Designated direct communication channels exist between the facility and LLE.	□ N/A □ No, Describe how LLE is contacted in the event of an emergency: □ Yes, Describe:
Alternative communication channels exist between the facility and LLE other than 911 emergency phone services.	□ N/A □ No □ Yes, Describe:

6.0 BUFFER ZONE DEVELOPMENT

Based on the threats and vulnerabilities identified in the preceding sections, the following buffer zone, extending outward from the facility, has been defined as the appropriate area for the implementation of preventive and protective security measures. The buffer zone includes all areas that would allow effective surveillance of or launch of an attack against the facility. The area also incorporates other nearby critical infrastructure and transportation assets—to include roads, rail lines, bridges, and waterways—as appropriate.

A description of the buffer zone is provided in Section 6.1. Relevant maps and photographs follow.

*** NOTE: Some information may be provided in the background package.**

6.1 Buffer Zone Description

BUFFER ZONE DESCRIPTION	DESCRIPTIVE DETAILS
General Description of the Buffer Zone (Note: e.g., industrial, commercial, residential, agricultural, rural; approximate size)	
Boundaries of the Buffer Zone	N: S: E: W:
County or Counties	
Local Government(s)	
Populated Areas Around Facility	
Major Transportation Routes (Note: e.g., roads, rail lines, waterways)	
Surrounding Critical Infrastructure	
Location and Response Times of Nearest Police/Fire/Rescue to Facility	Police: Fire: Rescue: (Note: include cardinal direction, distance, and response time to facility.)

6.2 Map Delineating Buffer Zone Boundaries

*** NOTE: Outline the buffer zone within a map or image that clearly defines the critical boundaries. Identify and label surveillance points, possible attack points, ingress/egress routes, and notable buffer zone features. Use computer-based graphics to support this process. Save as a .jpeg file and insert below.**

Insert ".jpg" Image Here

6.3 Buffer Zone Images

*** NOTE: Include photographs or overhead imagery documenting perimeter security concerns, views of significant assets from the buffer zone, etc. as appropriate. Identify and label surveillance points, staging areas, potential stand-off weapon locations, and avenues of approach or assault. Include a legend to any descriptive markings. Use computer-based graphics to support this process. Save as a .jpeg file and insert below.**

Insert “.jpg” Image(s) Here

7.0 BZPP AGENCY POINTS OF CONTACT

The following agencies and individuals have responsibilities associated with the implementation of this BZP and related terrorism protection and response duties in support of this facility. This list includes applicable law enforcement agencies; State, regional, and/or urban area fusion centers; emergency response assets, to include bomb disposal and HAZMAT units; public works; other Federal, State, and local government agencies; and facility security officials.

***NOTE: This section must be completed by LLE to ensure accurate and current data is provided. Affected agencies include:**

Site/Facility Management

Security Force, HAZMAT Team

LLE, Emergency Response, and other Homeland Security Agencies

Police Departments, Sheriff's Offices, Bomb Disposal, Special Weapons and Tactics (SWAT)

Fire Departments, Rescue Squads, HAZMAT Teams

Public Works and/or Public Health

State, Regional, or Local Agencies

State Homeland Security Advisor, State Police, State Emergency Management Agencies, National Guard

Fusion Center

Federal Agencies

Federal Bureau of Investigation (FBI), Joint Terrorism Task Force (JTTF), DHS, Coast Guard

Other Enforcement Agencies (e.g., transit, railroad, and/or port police, etc.)

7.1 BZPP Agency POC List

AGENCY	POC NAME & TITLE	ADDRESS	PHONE	CELL	FAX	E-MAIL

8.0 GAP ANALYSIS OF LOCAL TERRORISM PREVENTION AND PROTECTION CAPABILITIES

To ensure that adequate levels of support are available to prevent, protect against, and respond to acts of terrorism affecting this CI/KR site and its surrounding communities, the responsible law enforcement jurisdiction(s) and/or emergency services providers for this site were asked to provide an overview of their operations and a self-evaluation of their organization's readiness and capabilities. This evaluation is designed to gauge each responsible jurisdiction's ability to effectively prevent and respond to certain emergency situations, to include having an adequate force of trained personnel and the necessary tools and equipment to perform their assigned missions.

*** NOTE: Explain answers as necessary.**

8.1 General LLE Protective Force Support

Name and Address of Agency	
Agency BZPP POC	
Size of Force	
Estimated Response Time to Site	
Patrols	Is the area around the facility regularly patrolled by officers? Yes □ No □ If yes, how often?
Mutual Aid Agreements	Yes □ No □ If yes, please describe the following: 1. Are the agreements written or verbal? Written □ Verbal □ 2. List the agencies involved, describe how aid is requested, and identify the types/levels of support to be provided. 3. Are radio communications interoperable? Yes □ No □ If yes, explain how: (Note: e.g. specified channels, command center)
Participation in Visits/Exercises/ Training Affecting Site	Yes □ No □ If yes, please describe:
Ability to Operate in a Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) Environment	Yes □ No □ 1. Describe the types of CBRNE equipment LLE currently possesses. 2. Describe the types of CBRNE equipment LLE currently lacks.

What types of training does LLE currently lack to operate in a preventive or protective capacity at this site?	Describe:
What types of equipment does LLE currently lack to operate in a preventive or protective capacity at this site?	Describe:

8.2 Bomb Disposal Support

Name and Address of Agency		
Agency BZPP POC		
Size of Unit		Full-Time □ Part-Time □
Estimated Response Time to Site		
Mutual Aid Agreements	Yes □ No □ If yes, please describe the following: Are the agreements written or verbal? Written □ Verbal □ List the agencies involved, describe how aid is requested, and identify the types/ levels of support to be provided. Are radio communications interoperable? Yes □ No □ If yes, explain how: (Note: e.g. specified channels, command center)	
Participation in Visits/Exercises/ Training Affecting This Site	Yes □ No □ If yes, please describe:	
Does the unit have bomb detection K-9 dogs?	Yes □ No □ If yes, how many:	
Ability to Operate in a CBRNE Environment	Yes □ No □ Describe the types of CBRNE equipment the Bomb Squad currently possesses. Describe the type of CBRNE equipment the Bomb Squad currently lacks.	
What types of training does the bomb squad currently lack to operate in a protective or preventive capacity at this site?	Describe:	
What types of equipment does the bomb squad currently lack to operate in a preventive or protective capacity at this site?	Describe:	

8.3 SWAT Support

Name and Address of Agency		
Agency BZPP POC		
Size of Unit		Full-Time □ Part-Time □
Unit Members	Number of Tactical Medics: Number of Bomb Technicians:	
Estimated Response Time from Initial Notification to Fully Operational Command Post		
Unit Capabilities (Include explosive breaching, aerial insertion, waterborne introduction, etc.)		
Mutual Aid Agreements	Yes □ No □ If yes, please describe the following: Are the agreements written or verbal? Written □ Verbal □ List the agencies involved, describe how aid is requested, and identify the types/ levels of support to be provided. Are radio communications interoperable? Yes □ No □ If yes, explain how: (Note: e.g. specified channels, command center)	
Participation in Visits/Exercises/ Training Affecting This Site	Yes □ No □ If yes, please describe:	
Ability to Operate in a CBRNE Environment	Yes □ No □ Describe the types of CBRNE equipment the SWAT unit currently possesses. Describe the type of CBRNE equipment the SWAT unit currently lacks.	
What types of training does the SWAT unit currently lack to operate in a protective or preventive capacity at this site?	Describe:	
What types of equipment does the SWAT unit currently lack to operate in a protective or preventive capacity at this site?	Describe:	

8.4 Additional Emergency Services Prevention and Protection Support

*** NOTE: <u>IMPORTANT</u>: Only include an agency if it has a role in <u>PREVENTION</u> or <u>PROTECTION</u>, not response.**

Do any additional emergency services agencies (e.g., fire departments, rescue squads/emergency medical services, public works, public health or safety agencies) have any preventive or protective roles with regard to the subject site? Yes □ No □

If yes, please complete the following table for each applicable agency. The table may be copied as necessary.

Name and Address of Agency		
Agency BZPP POC		
Size of Force		Full-Time □ Part-Time □
Estimated Response Time to Site		
Mutual Aid Agreements	Yes □ No □ If yes, please describe the following: 1. Are the agreements written or verbal? Written □ Verbal □ 2. List the agencies involved, describe how aid is requested, and identify the types/ levels of support to be provided. 3. Are radio communications interoperable? Yes □ No □ If yes, explain how: (Note: e.g. specified channels, command center)	
Participation in Visits/Exercises/ Training Affecting This Site	Yes □ No □ If yes, please describe:	
Ability to Operate in a CBRNE Environment	Yes □ No □ Describe the types of CBRNE equipment the agency currently possesses. Describe the types of CBRNE equipment the agency currently lacks.	
Description of the Protection and/or Prevention Role the Agency Would Provide at This Site		
What types of training does the agency currently lack to operate in a preventive or protective capacity at this site?	Describe:	
What types of equipment does the agency currently lack to operate in a preventive or protective capacity at this site?	Describe:	

8.5 Other Agencies

Do any other Federal, State, or local agencies have any preventive or protective roles with regard to the subject site? **Yes □ No □** **If yes, please complete the following table for each applicable agency. The table may be copied as necessary.**		
Name and Address of Agency		
Agency BZPP POC		
Size of Force		Full-Time □ Part-Time □
Estimated Response Time to Site		
Mutual Aid Agreements	Yes □ No □ If yes, please describe the following: 1. Are the agreements written or verbal? Written □ Verbal □ 2. List the agencies involved, describe how aid is requested, and identify the types/ levels of support to be provided. 3. Are radio communications interoperable? Yes □ No □ If yes, explain how: (Note: e.g. specified channels, command center)	
Participation in Visits/ Exercises/Training Affecting This Site	Yes □ No □ If yes, please describe:	
Ability to Operate in a CBRNE Environment	Yes □ No □ Describe the types of CBRNE equipment the agency currently possesses. Describe the types of CBRNE equipment the agency currently lacks.	
Description of the Protection and/or Prevention Role the Agency Would Provide at This Site		
What types of training does the agency currently lack to operate in a preventive or protective capacity at this site?	Describe:	
What types of equipment does the agency currently lack to operate in a preventive or protective capacity at this site?	Describe:	

8.6 Mutual Aid Agreements with Supporting Agencies

List agencies in the order in which they would be contacted.

LLE SUPPORT	BOMB SUPPORT	SWAT SUPPORT	FIRE SUPPORT	HAZMAT SUPPORT
Agency: **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No
Agency: **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No
Agency: **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No
Agency: **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No
Agency: **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No	**Agency:** **Mutual Aid Agreement:** □ Yes □ No **Written?** □ Yes □ No

9.0 RECOMMENDED RESOURCES ENHANCEMENTS

*** NOTE: Should any questions or concerns arise regarding this section, LLE should contact their local Protective Security Advisor (PSA).**

Based on: 1) the analysis of threats and vulnerabilities associated with this facility and its buffer zone and 2) the results of the gap analysis of existing law enforcement and emergency services capabilities to prevent, protect against, and respond to terrorist incidents affecting this site, the following is a comprehensive list of recommended planning, equipment, training, and exercises enhancements that have been identified to improve the security around this site and its buffer zone.

All requested equipment enhancements **must** specifically reference as its purpose either: 1) the site-specific threat or vulnerability that the equipment is intended to mitigate or 2) an agency-specific capability gap that the equipment will address, as it pertains to the protection of the identified site.

The total value of the planning, equipment, training, and exercises enhancements identified in this section may exceed the total amount of the applicable FY 2009 BZPP grant funds and/or the identified enhancements may include items that are not eligible for purchase using this grant. Other grant programs, such as the Homeland Security Grant Program (HSGP), may be leveraged to support activities or equipment purchases that may not be funded through FY 2009 BZPP grants.

The specific planning activities and equipment items that the responsible jurisdiction(s) is proposing to procure for this site utilizing the FY 2009 BZPP grant are documented in the VRPP that accompanies this document. All items identified in the VRPP **must** also be listed below.

Please review the FY 2009 Program Guidelines and Application Kit to identify specific planning activities and equipment eligibility for funding.

• Planning	ALLOWABLE
• Equipment	ALLOWABLE
• Training	NOT ALLOWABLE
• Exercises	NOT ALLOWABLE

9.1 Planning Activities

In FY 2009, BZPP funds may be used for a range of homeland security and CI/KR protection planning activities. Allowable planning activities include, but are not necessarily limited to, the following:

Developing and implementing homeland security and CI/KR support programs and adopting DHS national initiatives limited to the following:

- Implementing the National Preparedness Guidelines, as they relate to implementation of the National Infrastructure Protection Plan and Sector-Specific Plans (SSPs).
- Building or enhancing preventive radiological and nuclear detection programs.
- Modifying existing incident management and Emergency Operating Plans (EOPs) to ensure proper alignment with the National Response Plan (NRP) and the National Incident Management System (NIMS) coordinating structures, processes, and protocols.
- Establishing or enhancing mutual aid agreements or MOUs to ensure cooperation with respect to CI/KR protection.
- Developing communications and interoperability protocols and solutions with the BZPP site.
- Developing or enhancing radiological and nuclear alarm resolution reachback relationships across local, State, and Federal partners.
- Developing or updating resource inventory assets in accordance to typed resource definitions issued by the NIMS Integration Center (NIC).
- Designing State and local geospatial data systems.

Developing related terrorism prevention and protection programs including:

- Planning to enhance preventive detection capabilities, security, and population evacuation in the vicinity of specified CI/KR during heightened alerts and terrorist incidents and/or to support mitigation efforts.
- Multi-discipline preparation and integration across the homeland security community.
- Developing or enhancing radiological and nuclear alarm resolution protocols and procedures.
- Developing and planning for information/intelligence sharing groups and/or fusion centers.
- Acquiring systems allowing connectivity to Federal data networks, such as the National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS), as appropriate.

Developing and enhancing plans and protocols, limited to:

- Developing or enhancing EOPs and operating procedures.
- Developing terrorism prevention/deterrence plans.
- Developing or enhancing cyber security plans.
- Developing or enhancing cyber risk mitigation plans.
- Developing public/private sector partnership emergency response, assessment, and resource sharing plans.
- Developing or updating local or regional communications plans.
- Developing plans to support and assist special needs jurisdictions, such as port authorities and rail and mass transit agencies.
- Developing and/or updating plans and protocols to support evacuation planning efforts.

The VRPP must clearly show how any funds identified for planning activities support the implementation of prevention and protection capabilities of the responsible jurisdiction, as they are related to the identified CI/KR site(s).

ACTIVITY	DETAILED JUSTIFICATION FOR PROPOSED PLANNING ACTIVITY	TOTAL COST	REQUESTING AGENCY	ARE FUNDS FROM OTHER FEDERAL, STATE, OR LOCAL SOURCES OR GRANT PROGRAMS BEING LEVERAGED FOR THIS ACTIVITY? IF SO, IDENTIFY THE SOURCE (E.G., HSGP, TRANSIT SECURITY GRANT PROGRAM (TSGP), ETC.).

9.2 Equipment Shortfalls

*** NOTE: The equipment identified in Section 9 is intended to be a comprehensive list of all equipment needed by the responsible jurisdictions to mitigate vulnerabilities associated with the site and its buffer zone and/or to address agency-specific capability gaps. The list generated may include items that are not eligible for purchase under the FY08 BZPP. The total value of equipment listed may exceed the amount of available FY08 BZPP funding. Responsible jurisdictions are encouraged to leverage resources that may be available under other homeland security grant programs to fund needed enhancements.**

ITEM (INCLUDING QUANTITY)	DETAILED JUSTIFICATION FOR PROPOSED USE OF EQUIPMENT (SITE-SPECIFIC THREAT/VULNERABILITY MITIGATION OR AGENCY GAP)	TOTAL COST	REQUESTING AGENCY	ARE FUNDS FROM OTHER FEDERAL, STATE, OR LOCAL SOURCES OR GRANT PROGRAMS BEING LEVERAGED FOR THIS EQUIPMENT NEED? IF SO, IDENTIFY THE SOURCE (E.G., HSGP, TSGP, ETC.).

9.3 Training Shortfalls

*** NOTE: Training identified and listed in this section should focus on strengthening anti-terrorism efforts by means of enhancing prevention and protection capabilities for appropriate designated jurisdictions. Inclusion of training needs and priorities in the BZP enables State and local jurisdictions to gain a full perspective of needed training and capability gaps relevant to a particular jurisdiction or CI/KR site. Funding from other DHS grant programs *may* be available to support the design and delivery of and/or attendance at necessary training. Identification of training shortfalls also alerts DHS to areas where future additional training may need to be developed and/or made available.**

TRAINING	DETAILED JUSTIFICATION FOR REQUESTED TRAINING	REQUESTING AGENCY	ARE FUNDS FROM OTHER FEDERAL, STATE, OR LOCAL SOURCES OR GRANT PROGRAMS BEING LEVERAGED FOR THIS EQUIPMENT NEED? IF SO, IDENTIFY THE SOURCE (E.G., HSGP, TSGP, ETC.).

9.4 Exercises

*** NOTE: Exercise funding is available through a variety of DHS grant programs, including the HSGP. Exercise scenarios may be threat- or performance-based. Those needs identified in this section should relate to:**

Prevention of and protection against terrorist attacks, including physical security activities and the sharing of intelligence and information;
Reduction of vulnerability to terrorism;
Minimizing the damage of terrorist attacks;
Enhancing the ability to respond to terrorist attacks; and/or
Providing a snapshot of the ability and preparedness level of State and local officials to deal with terrorist attacks.

ACTIVITY	DETAILED JUSTIFICATION FOR REQUESTED ACTIVITY	REQUESTING AGENCY	ARE FUNDS FROM OTHER FEDERAL, STATE, OR LOCAL SOURCES OR GRANT PROGRAMS BEING LEVERAGED FOR THIS EQUIPMENT NEED? IF SO, IDENTIFY THE SOURCE (E.G., HSGP, TSGP, ETC.).

10.0 IDENTIFICATION OF COLLATERAL BENEFICIARIES

10.1 Critical Infrastructure Sites (CI/KR Additions and/or Recommended Nominations)

The following sites, although not listed in the National Asset Database (NADB), have been identified by State or local officials as critical infrastructure in the same jurisdiction as the subject BZPP site that will also benefit from activities and equipment purchases requested in Section 9.

*** NOTE: The inclusion of these locally identified sites allows State or local jurisdictions to add infrastructure considered regionally critical. This listing may be used to feed the NADB as appropriate.**

FACILITY NAME	SECTOR	SEGMENT	ATTRIBUTE	ZIP CODE

11.0 INFORMATION ON BZP PREPARATION

11.1 BZP Preparer Contact Information

Name and Title of BZP Preparer(s):	
Agency Name:	
Address:	
Phone:	
FAX:	
E-Mail:	

11.2 DHS Technical Assistance

Did representatives from DHS provided technical assistance in the evaluation of threats and vulnerabilities of this CI/KR site and the corresponding development of this plan?

□ No

□ Yes

If yes, submit contact information for individuals involved who assisted in this BZP's development.

Name(s):	
Agency Name:	
Address:	
Phone:	
FAX:	
E-Mail:	

11.3 Facility Officials Participating in Site Visit/Plan Development

The following site representatives were interviewed for and/or otherwise participated in the development of this plan.

NAME	TITLE	PHONE	E-MAIL

11.4 Supporting Security Assessments, Emergency Plans and Directives, and Related Documents

The following documents and/or information sources—including pertinent security plans, emergency response plans, SOPs, continuity of operations plans, and vulnerability assessments —were used in the development of this BZP:

SECURITY DOCUMENT	SOURCE

FOR DHS USE ONLY

IP/PSCD APPROVAL:	NAME/TITLE:	/
	PHONE NUMBER & E-MAIL ADDRESS:	Phone: E-mail:
	DATE:	(dd/mm/yyyy)

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Requirements for Use

Nondisclosure

This document contains PCII. In accordance with the provisions of 6 C.F.R. Part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administra penalties. It is to be safeguarded and disseminated in accordance with the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 1 seq., the implementing Regulation at 6 C.F.R. Part 29 and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals witho following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of re of this information. You will receive an email containing the PCII user training. Follow the instructions included in the ema

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must m the following requirements:

Assigned to homeland security duties related to this critical infrastructure; and

Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the Critical Infrastructure Information Act of 2002 found at U.S.C. § 131 et seq. and the implementing Regulation at 6 C.F.R. Part 29.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do n leave this document unattended**.

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements list above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in tra

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular channels. If encryption is not available, send PCII as a password protected attachment and provide the password under se cover. **Do not send PCII to personal, non-employment related e-mail accounts.** Whenever the recipient forwa disseminates PCII via email, place that information in an attachment**.**

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to p inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking or identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addr Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return ad "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER**." Adhere to the aforementioned requiremen interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstance

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty re bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom o page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly create documents containing PCII. The PCII Tracking Number(s) of the source document(s) must be included on the derivatively crea document in the form of an endnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Tracking Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION