# Vancouver Energy
# Construction Security Plan

Plan No. C.08 | Revision 00

**Approved by:**

Name, Title: Kelly Flint, Senior Vice President and Corporate Counsel, Savage Companies
Designated Agent for EFSEC Application No. 2013-01
Date: 30 April 2015

**This page left blank intentionally.**

# Vancouver Energy
# Construction Security Plan

EFSEC Application for Site Certification No. 2013-01
Docket No. EF131590
30 April 2015

Prepared for

Tesoro Savage Petroleum Terminal LLC
5501 NW Old Lower River Road
Vancouver, Washington 98660

Prepared by

Mark A. Burris
Regional Security Manager, NW
Tesoro Companies Inc. LLC

**Revision Summary**

| No. | Date | Edits/Comments |
|---|---|---|
| 00 | 30 April 2015 | Submittal for Application Review |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Vancouver Energy
# Construction Security Plan

## Table of Contents

### Section

**1. Introduction ..... 3**
1.1 Purpose of Plan ..... 3
1.2 Regulatory Requirements ..... 3
1.3 Related Plans and Documents ..... 6
**2. Threat Assessment ..... 6**
**3. Site Security ..... 6**
3.1 Site Security ..... 6
3.2 Area 200 - Unloading ..... 6
3.3 Area 300 - Storage ..... 7
3.4 Area 400 - Marine Terminal ..... 7
3.5 Access Control ..... 7
3.6 Screening ..... 7
3.7 Traffic Control/Blockage of Roadways ..... 8
3.8 Monitoring ..... 8
3.9 Incident Procedures and Emergency Response ..... 8
**4. List of Acronyms and Abbreviations ..... 9**

### List of Figures

Figure 1. Vicinity Map ..... 4
Figure 2. Site Plan ..... 5

### List of Appendices

Appendix A. 49 CFR 1520 SSI
Appendix B. Crime Cast Report (CAP)
Appendix C. Emergency Contacts
Appendix D. Bomb Threat

**This page left blank intentionally.**

# 1. Introduction

Vancouver Energy (Facility) provides transloading services for pipeline quality crude oil from railcars to marine vessels. The Facility is located at 5501 NW Old Lower River Road, Vancouver, Washington; it is situated at the Port of Vancouver USA (Port) on the north bank of the Columbia River at approximately River Mile 103.5. The Facility site is approximately 47.4 acres in size and comprises elements within the following "area" groupings, as illustrated in Figure 1 and Figure 2.

- Area 200 – Rail Unloading – located at Terminal 5 of the Port
- Area 300 – Storage – located at Parcel 1A of the Port
- Area 400 – Marine Terminal – located at berths 13 and 14 at the Port
- Area 500 – Transfer Pipelines – located in locations between areas 200, 300, and 400
- Rail Infrastructure – located at Terminal 5 of the Port

The Facility receives an average of four unit trains per day and unloads an average of 360,000 barrels (bbl) of crude oil per day. Six nominal capacity 400,000 bbl tanks are used to store crude oil on site. A transfer pipeline system is used to convey crude oil from Area 200 to Area 300 for storage, and from Area 300 to Area 400 for vessel loading. The transfer pipeline system can also be operated to move crude oil from Area 200 directly to Area 400. The Facility operates 24 hours per day, 7 days per week.

## 1.1 Purpose of Plan

This construction security plan describes the security measures to be implemented during the construction phase of the Facility. [1]. All Facility and contractor personnel comply with applicable security requirements.

## 1.2 Regulatory Requirements

The Marine Terminal (Area 400) lies within the Maritime Transportation Security Act (MTSA)-regulated area of the Port and subject to the Port Facility Security Plan on file with the U.S. Coast Guard (USCG) in accordance with 33 CFR 105.

Security plans for facilities subject to these regulations are considered Security Sensitive Information (SSI) under 49 CFR 1520 and subject to protection from general release. See Appendix A for 49 CFR 1520 requirements.

This security plan is drafted to comply with federal statutory and regulatory requirements under the MTSA of 2002, 46 U.S.C. § 70101, et seq. This federal statute and implementing federal regulations preempt any conflicting state and local regulations or requirements.

[1] This plan has been prepared in response to the review of the Application for Site Certification (ASC). It is a preliminary plan based on the Applicant's current understanding of the Facility, as described in the ASC submitted to EFSEC. It is a draft and subject to change as the project develops. Changes in engineering and construction may impact later versions and editions of this security plan. This plan is current as of the date as listed in the footer.

Further, the Port is a vibrant dynamic economic engine with multiple tenants and customers. The Port makes changes to physical and procedural security to facilitate their various customers and tenants. The Facility would be only one of these tenants. Changes to physical and procedural security are subject to change and may impact later versions and editions of this plan. For example, perimeter fencing or gates may be changed or added. Security routes may be changed or added.

## Figure 1 - Vicinity Map

**LEGEND**

- Project Boundary
- Vancouver_WA
- Portland,_Oregon

VANCOUVER ENERGY

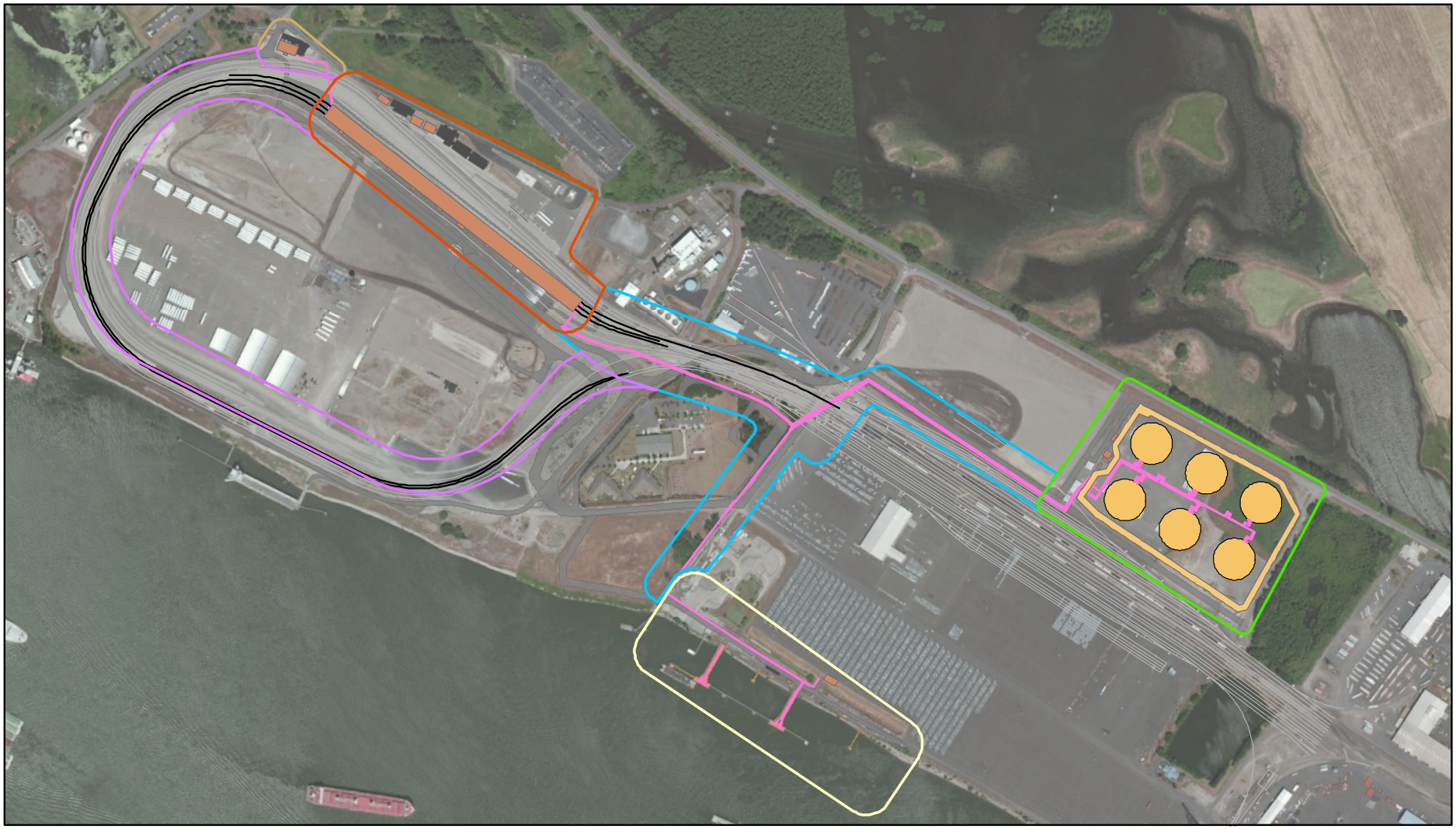
Tesoro Savage Petroleum Terminal LLC

Date: February 2015

**Map Notes:** Aerial photo dated July 2010, courtesy of ESRI World Imagery service

N

EX-0001-005318-PCE



## Figure 2 - Site Plan

VANCOUVER ENERGY

Tesoro Savage Petroleum Terminal LLC

**Proposed Project Facilities**

- Containment Berm
- Rail
- Parking
- Building
- Transfer Pipeline
- Storage Tank
- Roads
- Marine Terminal

**TSPT Improvement Areas**

- 200 - Unloading and Office
- 300 - Storage
- 400 - Marine Terminal
- 500 - Transfer Pipelines
- 600 - West Boiler
- Rail Infrastructure

0 250 500 1,000 Feet

N

Date: February 2015

**Map Notes:** Aerial photo dated July 2010, courtesy of ESRI World Imagery service

EX-0001-005319-PCE

## 1.3 Related Plans and Documents

Other plans prepared for the Facility construction that address site security measures include the following.

- Construction Traffic Management Plan – This plan identifies how haul trucks will access various areas of the Facility construction site. Such access will be conducted in accordance with the security measures described in the Construction Security Plan.

# 2. Threat Assessment

The basis for measures and mitigations proposed in this security plan is a result of a basic local threat assessment of the Facility location at the Port.

Vancouver Police Department crime statistics and Crime Map were referenced for historical criminal threat data. A Crimecast CAP index report for 2014 for the Port was reviewed. Past incident data for the Port was reviewed. The Facility is located in an area with statistically average general crime threats. General property crimes are the most common but at national averages. The general crime threat has been evaluated as low severity and low likelihood. See Appendix B. The protest threat has been evaluated as likely but with a low level of severity.

With no specific threat, mitigations and measures as required by MTSA are deemed adequate mitigations to general threats to critical energy infrastructure. General crime and protest disruption mitigation measures are exceeded by the regulatory requirements of MTSA.

# 3. Site Security

## 3.1 Site Security

The perimeter of the Port is fenced and gated to prevent unauthorized access to the Port. The overpass from Terminal 4 to Terminal 5 provides access to the rail loop at Terminal 5. Gates and traffic schemes are in effect to restrict access to the rail loop at the east base of the overpass. Proposed enhancements to physical security include increased fencing, gates, and possible staffed gate house with powered gates.

The Port has a professional full-time proprietary security force. This security force monitors Port property via roving random vehicle patrols, staffed gates, and monitored closed-circuit television (CCTV). The security force maintains a strong liaison with Vancouver Police Department (VPD) for security-related response.

Construction sites are secured via a combination of temporary fencing, portable lighting, and 24/7 security officers. Security officers are be hired from the Port or an outside vendor. Security officers have redundant communications with the Port to report suspicious activity and to contact VPD for response. Security officers work with Port security to provide mobile coverage of active construction sites.

## 3.2 Area 200 - Unloading

This construction site is located in the Terminal 5 rail loop. The rail loop may be in use by the Port and other tenants during construction. Potential threats include property crimes related to equipment and materials. Mitigations include existing perimeter fencing, existing Port lighting, existing random Port security patrols. Additional mitigations include temporary fencing, portable lighting to enhance existing Port lighting, and 24/7 staffing by a contract security officer. Day/construction security officer duties

include access control in addition to monitoring. Afterhours duties include patrols and monitoring of the site, construction equipment, and materials.

## 3.3 Area 300 - Storage

This construction site is located in Parcel 1A East. Potential threats include property crimes related to equipment and materials. Mitigations include existing perimeter fencing, existing Port lighting, existing random Port security patrols. Additional mitigations include temporary fencing, portable lighting to enhance existing Port lighting, and 24/7 staffing by a contract security officer. Day/construction security officer duties include access control in addition to monitoring. Afterhours duties include patrols and monitoring of the site, construction equipment, and materials.

## 3.4 Area 400 - Marine Terminal

This construction site is located in Terminal 4, berths 13 and 14. Potential threats include property crimes related to equipment and materials. Mitigations include the berths 13 and 14 that lie within the MTSA-regulated footprint of the Port. The Port controls access to the MTSA area via perimeter fencing, staffed entrance gates, Port lighting, random Port security patrols, and monitoring via security staff and CCTV. Additional mitigations are considered to include portable lighting to enhance existing Port lighting, and 24/7 staffing by a contract security officer. Day/construction duties include access control in addition to monitoring. Afterhours duties include patrols and monitoring of the site, construction equipment, and materials.

## 3.5 Access Control

Access control to the construction sites are the primary function of security during day/construction hours. Access control measures serve to mitigate unauthorized access to the sites for safety, security, and loss control risks. Access lists are coordinated with construction supervision to accommodate dynamic scheduling of construction. A Facility-specific decal is provided to individuals who have completed the Facility-specific orientation. This decal is required for unescorted access within the defined Facility boundaries.

Visitors and guests are admitted to the site only after preapproval or coordination with construction supervision. All entrants are required to initially provide a government issued photo identification to match with access lists or to record visitor guest information. Visitor guest access and escort requirements are determined by construction supervision weighing active construction and security risks.

Transportation Workers Identification Credential (TWIC) escorts are required for non-TWIC visitors and guests at Area 400 – Marine Terminal in accordance with Port procedures. A TWIC is required for individuals working the marine loading construction area because this area is within the Port MTSA-regulated footprint. Although not required at the rail unloading construction site, nor for the storage tanks construction site, consideration is given to requiring TWIC for other construction areas for construction crew flexibility.

## 3.6 Screening

Random entry screening of personnel and vehicles are conducted by contract security to prevent the introduction of unauthorized individuals, substances, and devices to the construction sites. Screening rates are coordinated with the Port to be in alignment with current Port security posture. Random exit screening are conducted by contract security to mitigate potential loss of materials and tools. Any tools, materials, or equipment being brought out of the Facility require an authorized Material Gate Pass. These passes may be obtained from the Facility HSSE lead. All items are subject to inspection prior to release. Coordination with construction supervision is conducted to manage deliveries and demobilizations.

## 3.7 Traffic Control/Blockage of Roadways

If a roadway managed by a public or private entity must be blocked or access restricted as a result of Facility work, advanced planning and notification to stakeholders is required. All road closures and traffic control activities are coordinated through the Facility HSSE lead or his delegate, and taking into consideration the Construction Traffic Management Plan.

## 3.8 Monitoring

Monitoring and random patrols of the construction sites is the primary function after hours. Monitoring and random patrols serves to mitigate loss control and general crime risks. Monitoring and random patrols encompass active constructions sites, materials staging areas, equipment and tool storage areas, and any flammable or hazardous materials storage areas. Locked storage, trailers, ConEx, cabinets, etc. are used for storage when tools and materials are not in use.

## 3.9 Incident Procedures and Emergency Response

Site familiarization visits are coordinated with construction supervision, contract security, Port security, Vancouver Police Department, and Vancouver Fire Department. These visits are conducted preconstruction and at major construction milestones to ensure safe and timely response to any emergent situation. Safe and timely access and egress routes are clearly established. Standard clear nomenclature is established to describe the construction site and site hazards. These visits include a review of current threat status of the construction site, high value items and their storage strategies, and site hazards. Emphasis is given to potential risks to responders, including construction and flammable and/or hazardous materials on site. General site plot plans are used to illustrate these visits. This plot plan is updated with each major construction milestone or significant hazard change. A laminated portable copy is provided to contract security.

A security incident reporting call list is established to ensure timely and comprehensive notification of any security incident. Current 24-hour contact numbers with name and title are included in the reporting procedure. See Appendix C.

On-duty security initiate incident reporting and prepare a laminated plot plan with location of the incident clearly marked for emergency responders.

Telephonic threats or bomb threats are reported to law enforcement. A bomb threat record sheet is kept near the public or main listed telephone for the construction site. See Appendix D.

Post incident procedures include a root cause review of the incident to determine lessons learned and any possible modification to this plan.

# 4. List of Acronyms and Abbreviations

CCTV: closed-circuit television

CFR: Code of Federal Regulations

MTSA: Maritime Transportation Security Act

Port: Port of Vancouver USA

SSI: Security Sensitive Information

TWIC: Transportation Workers Identification Credential

USCG: U.S. Coast Guard

VPD: Vancouver Police Department

**This page left blank intentionally.**

# Vancouver Energy
# Construction Security Plan

EFSEC Application for Site Certification No. 2013-01
Docket No. EF131590

## Appendix A
## 49 CRF 1520 SSI

WARNING: This record contains SSI that is controlled under 49 CFR, Parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know,” as defined in 49 CFR, Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR, Parts 15 and 1520.

# SUBCHAPTER B—SECURITY RULES FOR ALL MODES OF TRANSPORTATION

## PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.
1520.1 Scope.
1520.3 Terms used in this part.
1520.5 Sensitive security information.
1520.7 Covered persons.
1520.9 Restrictions on the disclosure of SSI.
1520.11 Persons with a need to know.
1520.13 Marking SSI.
1520.15 SSI disclosed by TSA or the Coast Guard.
1520.17 Consequences of unauthorized disclosure of SSI.
1520.19 Destruction of SSI.

AUTHORITY: 46 U.S.C. 70102–70106, 70117; 49 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

SOURCE: 69 FR 28082, May 18, 2004, unless otherwise noted.

### § 1520.1 Scope.

(a) *Applicability*. This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information, as defined in § 1520.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation*. The authority of TSA and the Coast Guard under this part may be further delegated within TSA and the Coast Guard, respectively.

### § 1520.3 Terms used in this part.

In addition to the terms in § 1500.3 of this chapter, the following terms apply in this part:

*Administrator* means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

*Coast Guard* means the United States Coast Guard.

*Covered person* means any organization, entity, individual, or other person described in § 1520.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in § 1520.7.

*DHS* means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

*DOT* means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

*Federal Flight Deck Officer* means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

*Maritime facility* means any facility as defined in 33 CFR part 101.

*Rail facility* means ''rail facility'' as defined in 49 CFR 1580.3.

*Rail hazardous materials receiver* means ''rail hazardous materials receiver'' as defined in 49 CFR 1580.3.

*Rail hazardous materials shipper* means ''rail hazardous materials shipper'' as defined in 49 CFR 1580.3.

*Rail secure area* means ''rail secure area'' as defined in 49 CFR 1580.3.

*Rail transit facility* means ''rail transit facility'' as defined in 49 CFR 1580.3.

*Rail transit system* or *Rail Fixed Guideway System* means ''rail transit system'' or ''Rail Fixed Guideway System'' as defined in 49 CFR 1580.3.



EX-0001-005327-PCE

*Railroad* means ''railroad'' as defined in 49 U.S.C. 20102(1).

*Railroad carrier* means ''railroad carrier'' as defined in 49 U.S.C. 20102(2).

*Record* includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term *record* also includes any draft, proposed, or recommended change to any record.

*Security contingency plan* means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

*Security screening* means evaluating a person or property to determine whether either poses a threat to security.

*SSI* means sensitive security information, as described in § 1520.5.

*Threat image projection system* means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

*TSA* means the Transportation Security Administration.

*Vulnerability assessment* means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, or vessel; aircraft; railroad; railroad carrier, rail facility; train; rail hazardous materials shipper or receiver facility; rail transit system; rail transit facility; commercial motor vehicle; or pipeline; or a transportation-related automated system or network to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions or countermeasures to address security concerns.

[69 FR 28082, May 18, 2004, as amended at 70 FR 41599, July 19, 2005; 73 FR 72172, Nov. 26, 2008; 74 FR 47695, Sept. 16, 2009]

**§ 1520.5 Sensitive security information.**

(a) *In general.* In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the security of transportation.

(b) *Information constituting SSI.* Except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including any comments, instructions, or implementing guidance, including—

(i) Any aircraft operator, airport operator, fixed base operator, or air cargo security program, or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—

(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation, maritime, or rail transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation, maritime, or rail transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(iv) Any armed security officer procedures issued by TSA under 49 CFR part 1562.

(9) *Security screening information.* The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property



EX-0001-005329-PCE

screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out aviation, maritime, or rail transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.* (i) Lists of the names or other identifying information that identify persons as—

(A) Having unescorted access to a secure area of an airport, a rail secure area, or a secure or restricted area of a maritime facility, port area, or vessel;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation, maritime, or rail infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or rail transportation system (including rail hazardous materials shippers and rail hazardous materials receivers) that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under



EX-0001-005330-PCE

49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) *Loss of SSI designation.* TSA or the Coast Guard may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria set forth in paragraph (a) of this section.

[69 FR 28082, May 18, 2004, as amended at 70 FR 41599, July 19, 2005; 71 FR 30507, May 26, 2006; 73 FR 72172, Nov. 26, 2008; 74 FR 47695, Sept. 16, 2009]

### § 1520.7 Covered persons.

Persons subject to the requirements of part 1520 are:

(a) Each airport operator, aircraft operator, and fixed base operator subject to the requirements of subchapter C of this chapter, and each armed security officer under subpart B of part 1562.

(b) Each indirect air carrier (IAC), as described in 49 CFR part 1548; and each certified cargo screening facility and its personnel, as described in 49 CFR part 1549.

(c) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.

(d) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107–295), 46 U.S.C. 70101 *et seq.*, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.*

(e) Each person performing the function of a computer reservation system or global distribution system for airline passenger information.

(f) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(g) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(h) DHS and DOT.

(i) Each person conducting research and development activities that relate to aviation or maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in § 1520.11.

(k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

(m) Each person receiving SSI under § 1520.15(d) or (e).

(n) Each railroad carrier, rail hazardous materials shipper, rail hazardous materials receiver, and rail transit system subject to the requirements of part 1580 of this chapter.

[69 FR 28082, May 18, 2004, as amended at 70 FR 41600, July 19, 2005; 73 FR 72173, Nov. 26, 2008; 74 FR 47695, Sept. 16, 2009; 76 FR 51867, Aug. 18, 2011]

### § 1520.9 Restrictions on the disclosure of SSI.

(a) *Duty to protect information.* A covered person must—

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in § 1520.13.

(5) Dispose of SSI as specified in § 1520.19.

(b) *Unmarked SSI.* If a covered person receives a record containing SSI that is not marked as specified in § 1520.13, the covered person must—

(1) Mark the record as specified in § 1520.13; and



EX-0001-005331-PCE

(2) Inform the sender of the record that the record must be marked as specified in § 1520.13.

(c) *Duty to report unauthorized disclosure.* When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) *Additional Requirements for Critical Infrastructure Information.* In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

**§ 1520.11 Persons with a need to know.**

(a) *In general.* A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) *Federal, State, local, or tribal government employees, contractors, and grantees.* (1) A Federal, State, local, or tribal government employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties, on behalf or in defense of the interests of the Federal, State, local, or tribal government.

(2) A person acting in the performance of a contract with or grant from a Federal, State, local, or tribal government agency has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) *Background check.* TSA or Coast Guard may make an individual's access to the SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI that are satisfactory to TSA or the Coast Guard.

(d) *Need to know further limited by the DHS or DOT.* For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

[69 FR 28082, May 18, 2004, as amended at 70 FR 1382, Jan. 7, 2005; 73 FR 72173, Nov. 26, 2008]

**§ 1520.13 Marking SSI.**

(a) *Marking of paper records.* In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) *Protective marking.* The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) *Distribution limitation statement.* The distribution limitation statement is:

*WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ''need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies,

public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(d) *Other types of records*. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

### § 1520.15 SSI disclosed by TSA or the Coast Guard.

(a) *In general*. Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does TSA or the Coast Guard release such records to persons without a need to know.

(b) *Disclosure under the Freedom of Information Act and the Privacy Act*. If a record contains both SSI and information that is not SSI, TSA or the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) *Disclosures to committees of Congress and the General Accounting Office*. Nothing in this part precludes TSA or the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) *Disclosure in enforcement proceedings*—(1) *In general*. TSA or the Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of TSA or the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by TSA or the Coast Guard.

(2) *Security background check*. Prior to providing SSI to a person under paragraph (d)(1) of this section, TSA or the Coast Guard may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of TSA or the Coast Guard, a security background check.

(e) *Other conditional disclosure*. TSA may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by TSA that disclosure of such records or information, subject to such limitations and restrictions as TSA may prescribe, would not be detrimental to transportation security.

(f) *Obligation to protect information*. When an individual receives SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under § 1520.7 and is subject to the obligations of a covered person under this part.

(g) *No release under FOIA*. When TSA discloses SSI pursuant to paragraphs (b) through (e) of this section, TSA makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) *Disclosure of Critical Infrastructure Information*. Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

### § 1520.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

### § 1520.19 Destruction of SSI.

(a) *DHS*. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve



EX-0001-005333-PCE

records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function.

(b) *Other covered persons*—(1) *In general.* A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

(2) *Exception.* Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.



EX-0001-005334-PCE

# Vancouver Energy
# Construction Security Plan

EFSEC Application for Site Certification No. 2013-01
Docket No. EF131590

## Appendix B
## Crime Cast Report (CAP)

# CRIMECAST® basic

## Site Information

Vancouver Terminal
2111 St. Francis Ln.
Vancouver, WA 98660

**Coordinates** Latitude: 45.638678, Longitude: -122.699294

## Report Contents

About CAP Index, Inc. ..... 2

CRIMECAST Map - 1:3 Methodology ..... 3

CRIMECAST Scores - 1:3 Methodology ..... 4

Appendices ..... 5

*About the CRIMECAST Map & Scores* ..... 5



CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://crimecast.capindex.com/terms.aspx. ©2015 CAP Index, Inc. All Rights Reserved.

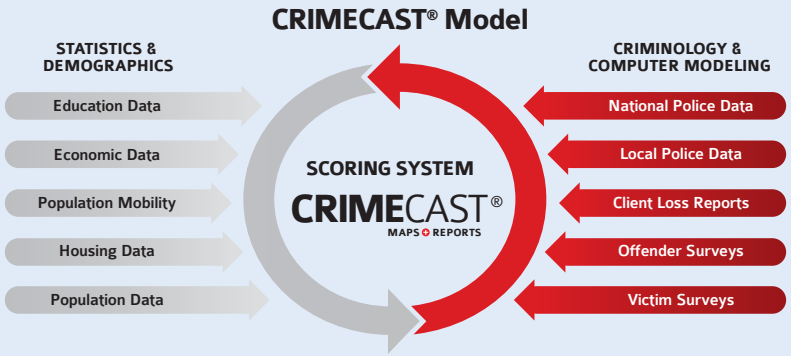
# About CAP Index, Inc.

CRIMECAST® basic

## Address-Specific Crime and Loss Forecasting

The CAP Index® CRIMECAST Model is based upon the strong relationship that exists between a neighborhood's "social disorganization" and the amount of crime that is perpetrated there. Our advanced evaluation system identifies the risk of personal and property crimes at any location in the United States.

Objective, address-specific CRIMECAST Scores are calculated by correlating a broad array of demographic variables (excluding race, religion and gender) with historical crime data, survey information and other known indicators of crime.




**The result?** CRIMECAST Reports provide data-driven scores that place any location within the United States in context with national, state and county levels of crime risk.

## About CAP Index, Inc.

As the world leader in crime and risk forecasting, CAP Index provides innovative solutions for companies and government agencies looking to minimize losses including shrink, general liability, fraud, lawsuits and crimes against persons and property. CAP Index is a trusted partner to 81 of the Fortune® 100 Companies.

CAP Index's CRIMECAST products are derived from an advanced evaluation system designed to identify the risk of personal and property crimes at any location in the United States, the United Kingdom and Canada. Address-specific CRIMECAST Reports assist clients in ranking and comparing multiple locations, site selection, security resource allocation, litigation and underwriting.

Going beyond CRIMECAST Scores, CAP Index's team of consultants can analyze external CAP Index information in tandem with internal company-specific data in order to create an objective, operationally feasible, cost-effective and fully customized risk identification model.


**Corporate Headquarters**
The Commons at Lincoln Center
150 John Robert Thomas Drive
Exton, PA 19341

**U.S. and Canada**
1-800-CAP-RISK
(1-800-227-7475)

**Outside U.S. and Canada**
+1 610-903-3000

info@capindex.com
www.capindex.com





CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://crimecast.capindex.com/terms.aspx. ©2015 CAP Index, Inc. All Rights Reserved.

# CRIMECAST Map - 1:3 Methodology

Tesoro Corporation

CRIMECAST® basic

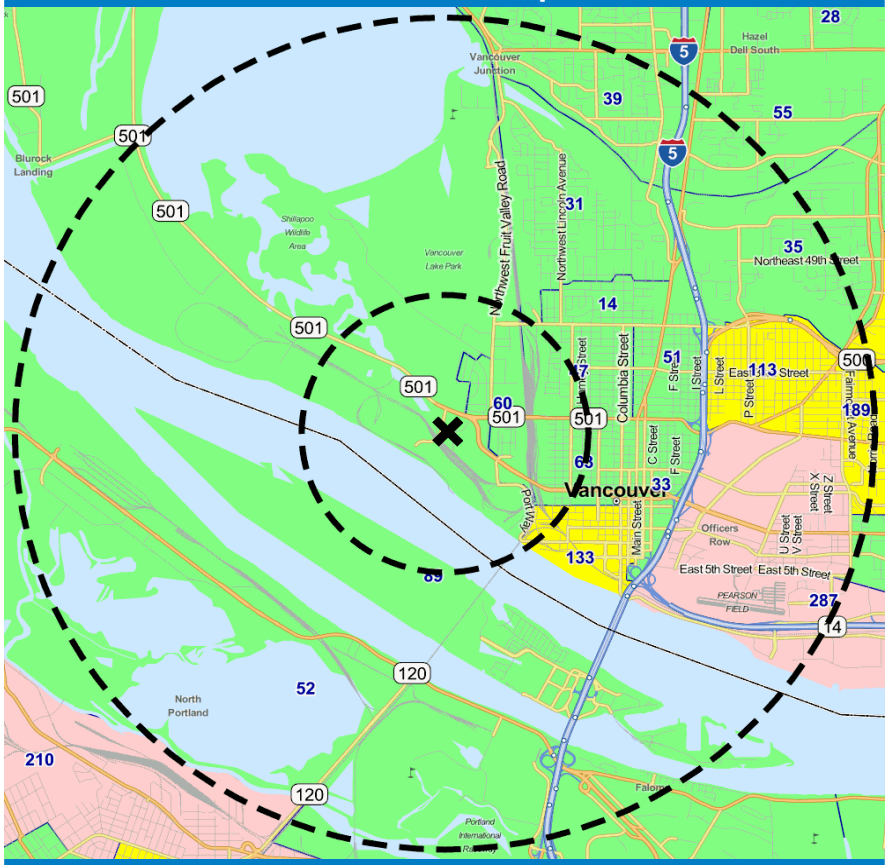
This site's Current 2014 National CAP Index Score is

# 134

Vancouver Terminal
2111 St. Francis Ln.
Vancouver, WA 98660

Lat: 45.638678, Long: -122.699294

## CRIMECAST Map




Inner Radius: 1.0 mi • Outer Radius: 3.0 mi

**Score Ranges:** 0-99 | 100-199 | 200-399 | 400-799 | 800-2000

1.2 mi

## National

| CRIMECAST CATEGORY | This Site's Scores CURRENT 2014 |
|---|---|
| CAP Index | 134 |
| Homicide | 84 |
| Rape | 187 |
| Robbery | 123 |
| Aggravated Assault | 151 |
| **Crimes Against Persons** | **144** |
| Burglary | 149 |
| Larceny | 248 |
| Motor Vehicle Theft | 207 |
| **Crimes Against Property** | **239** |

| CAP INDEX SCORE | NATIONAL |
|---|---|
| Past – 2010 | 135 |
| Current – 2014 | 134 |
| Projected – 2019 | 123 |

*CRIMECAST Scores are based on a scale of 0 to 2000, with 0 representing the lowest risk and 2000 the highest - 100 is average. A score of 600 is 6 times higher than average, and a score of 25 indicates that the risk is 1/4 the average.*

**Creation Date:** January 05, 2015

CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://crimecast.capindex.com/terms.aspx. ©2015 CAP Index, Inc. All Rights Reserved.

CAPIndex®



EX-0001-005339-PCE

# CRIMECAST Scores - 1:3 Methodology

Tesoro Corporation

CRIMECAST® basic

This site's Current 2014 National CAP Index Score is

# 134

Vancouver Terminal
2111 St. Francis Ln.
Vancouver, WA 98660

Lat: 45.638678, Long: -122.699294

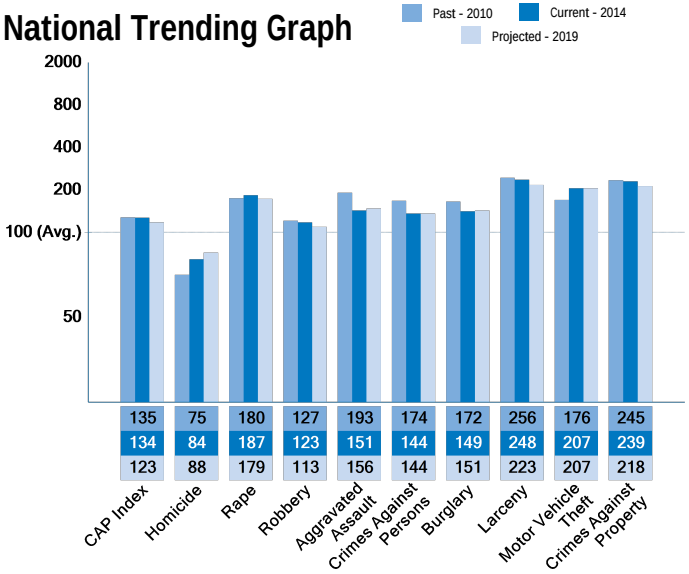
## National

| CRIMECAST CATEGORY | This Site's Scores PAST 2010 | CURRENT 2014 | PROJECTED 2019 |
|---|---|---|---|
| CAP Index | 135 | 134 | 123 |
| Homicide | 75 | 84 | 88 |
| Rape | 180 | 187 | 179 |
| Robbery | 127 | 123 | 113 |
| Aggravated Assault | 193 | 151 | 156 |
| **Crimes Against Persons** | **174** | **144** | **144** |
| Burglary | 172 | 149 | 151 |
| Larceny | 256 | 248 | 223 |
| Motor Vehicle Theft | 176 | 207 | 207 |
| **Crimes Against Property** | **245** | **239** | **218** |

## State

| CRIMECAST CATEGORY | This Site's Scores PAST 2010 | CURRENT 2014 | PROJECTED 2019 |
|---|---|---|---|
| CAP Index | 179 | 180 | 169 |
| Homicide | 172 | 200 | 208 |
| Rape | 175 | 188 | 183 |
| Robbery | 178 | 174 | 163 |
| Aggravated Assault | 248 | 202 | 212 |
| **Crimes Against Persons** | **229** | **196** | **200** |
| Burglary | 172 | 155 | 162 |
| Larceny | 210 | 210 | 191 |
| Motor Vehicle Theft | 140 | 158 | 159 |
| **Crimes Against Property** | **205** | **206** | **191** |

## National Trending Graph




## County*

| CRIMECAST CATEGORY | This Site's Scores PAST 2010 | CURRENT 2014 | PROJECTED 2019 |
|---|---|---|---|
| CAP Index | 311 | 302 | 278 |
| Homicide | 310 | 341 | 348 |
| Rape | 326 | 311 | 297 |
| Robbery | 295 | 283 | 260 |
| Aggravated Assault | 391 | 306 | 310 |
| **Crimes Against Persons** | **376** | **311** | **306** |
| Burglary | 308 | 271 | 267 |
| Larceny | 557 | 535 | 462 |
| Motor Vehicle Theft | 301 | 317 | 311 |
| **Crimes Against Property** | **531** | **512** | **453** |

*CRIMECAST Scores are based on a scale of 0 to 2000, with 0 representing the lowest risk and 2000 the highest - 100 is average. A score of 600 is 6 times higher than average, and a score of 25 indicates that the risk is 1/4 the average.*

*Clark County, WA

**Creation Date:** January 05, 2015

CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://crimecast.capindex.com/terms.aspx. ©2015 CAP Index, Inc. All Rights Reserved.

CAPIndex®



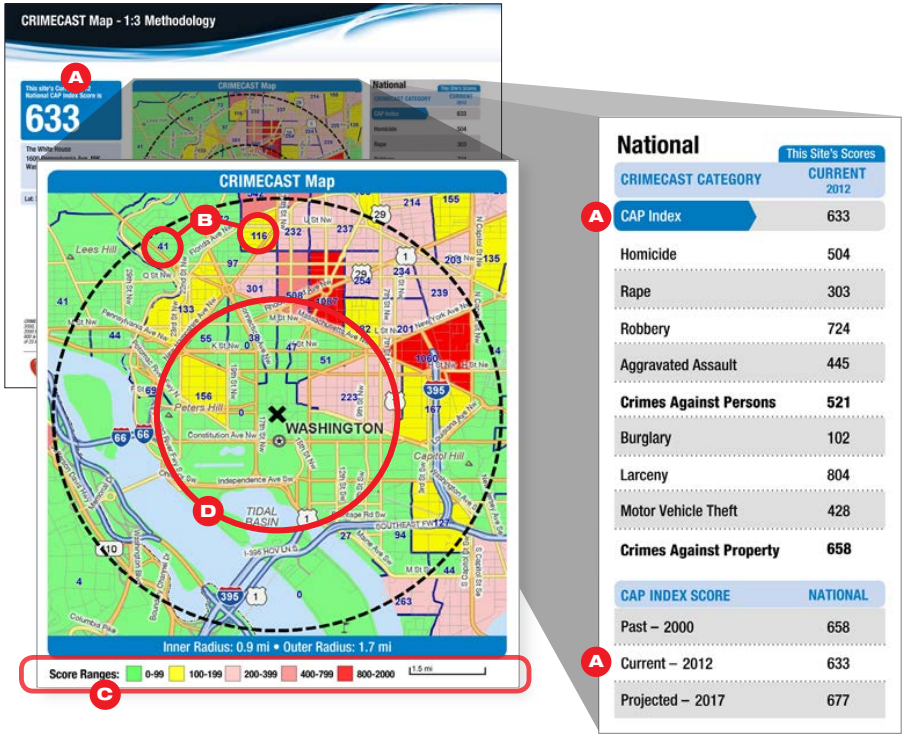
EX-0001-005340-PCE

# About the CRIMECAST Map & Scores

CRIMECAST® basic

## CRIMECAST Reports

With a detailed, color-coded map and a spreadsheet of risk scores, users can identify potential asset protection concerns surrounding an address. A quick glance at the map shows the site in relation to its environment. The CRIMECAST Scores allow for an in-depth analysis of the overall crime risk.




## CRIMECAST Scores

**A** The CAP Index Score represents the overall risk of crime at the address.

- CRIMECAST Scores are based on a scale of 0 to 2000, with 0 representing the lowest risk and 2000 the highest – 100 is average.
- A score of 600 is 6 times higher than average, and a score of 25 indicates that the risk is ¼ the average.
- Each CRIMECAST Report contains 90 risk scores provided for 3 geographic levels and 3 time periods:

1. **National** scores provide the site's risk in comparison to the entire U.S.
2. **State** scores compare the site to the average risk of the state in which it resides.
3. **County** scores compare the site to the average risk of the county in which it resides.
4. **Past, Current** and **Projected** risk scores are provided to allow for trending.

## CRIMECAST Map

**B** Census tracts are outlined in blue. There are over 72,000 census tracts in the United States. Each tract contains several thousand residents with similar socioeconomic characteristics. Every census tract is assigned a numeric risk score and a coinciding risk shading.

**C** The site map is color-coded to depict the level of risk within each tract and identify the potential origin of criminal behavior. CAP Index Score ranges are used to assign risk shading similar to that of the green, yellow and red color scheme found on a traffic light.

**D** A radius threshold analysis is used to determine a site's overall risk. The inner radius represents 1 mile or a population of 25,000, equaling 2/3 of the overall score. The outer radius represents 3 miles or a population of 100,000, providing the remaining 1/3. In addition to the 1:3 methodology shown to the left, a 2:6 methodology is also available. This methodology applies an inner radius of 2 miles or a population of 100,000 and an outer radius of 6 miles or a population of 400,000.




CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://crimecast.capindex.com/terms.aspx. ©2015 CAP Index, Inc. All Rights Reserved.

# About the CRIMECAST Map & Scores (cont.)

CRIMECAST® basic

National

| CRIMECAST CATEGORY | This Site's Scores PAST 2000 | CURRENT 2012 | PROJECTED 2017 |
|---|---|---|---|
| CAP Index | 658 | 633 | 677 |
| Homicide | 404 | 504 | 551 |
| Rape | 344 | 303 | 281 |
| Robbery | 713 | 724 | 780 |
| Aggravated Assault | 414 | 445 | 426 |
| **Crimes Against Persons** | **499** | **521** | **505** |
| Burglary | 129 | 102 | 105 |
| Larceny | 911 | 804 | 743 |
| Motor Vehicle Theft | 252 | 428 | 484 |
| **Crimes Against Property** | **738** | **658** | **610** |

State

| CRIMECAST CATEGORY | This Site's Scores PAST 2000 | CURRENT 2012 | PROJECTED 2017 |
|---|---|---|---|
| CAP Index | 199 | 264 | 303 |
| Homicide | 135 | 208 | 216 |
| Rape | 251 | 364 | 393 |
| Robbery | 196 | 267 | 308 |
| Aggravated Assault | 166 | 242 | 262 |
| **Crimes Against Persons** | **179** | **254** | **274** |
| Burglary | 262 | 299 | 320 |
| Larceny | 772 | 829 | 812 |
| Motor Vehicle Theft | 252 | 327 | 359 |
| **Crimes Against Property** | **694** | **751** | **727** |

National Trending Graph



County*

| CRIMECAST CATEGORY | This Site's Scores PAST 2000 | CURRENT 2012 | PROJECTED 2017 |
|---|---|---|---|
| CAP Index | 199 | 264 | 303 |
| Homicide | 135 | 208 | 216 |
| Rape | 251 | 364 | 393 |
| Robbery | 196 | 267 | 308 |
| Aggravated Assault | 166 | 242 | 262 |
| **Crimes Against Persons** | **179** | **254** | **274** |
| Burglary | 262 | 299 | 320 |
| Larceny | 772 | 829 | 812 |
| Motor Vehicle Theft | 171 | 327 | 359 |
| **Crimes Against Property** | **694** | **751** | **727** |

*This site is located in District Of Columbia County

## CRIMECAST Scores

This page contains 90 risk scores provided for 3 geographic levels and 3 time periods.

- **A** **National** scores provide the site's risk in comparison to the entire U.S. and are broken down by CRIMECAST Category. **Past, Current** and **Projected** risk scores are provided to allow for trending.
- **B** **State** scores compare the site to the average risk of the state in which it resides and are broken down by CRIMECAST Category. **Past, Current** and **Projected** risk scores are provided to allow for trending.
- **C** **County** scores compare the site to the average risk of the county in which it resides and are broken down by CRIMECAST Category. **Past, Current** and **Projected** risk scores are provided to allow for trending.
- **D** The **National Past**, **Current** and **Projected** risk scores for the CAP Index Score and each CRIMECAST Category are graphed in order to provide a visual representation of the site's risk pattern over an extended period of time.




CRIMECAST is a trademark of CAP Index, Inc. Please note terms and conditions as presented on http://crimecast.capindex.com/terms.aspx. ©2015 CAP Index, Inc. All Rights Reserved.

# Vancouver Energy
# Construction Security Plan

EFSEC Application for Site Certification No. 2013-01
Docket No. EF131590

## Appendix C
## Emergency Contacts

# Appendix C
# Emergency Contacts

| IMPORTANT PHONE CONTACTS | | | |
|---|---|---|---|
| **Affiliation** | **Phone Number** | **Name of Person Contacted** | **Time Contacted** |
| Manager | XXX-XXX-XXXX (office)<br>XXX-XXX-XXXX (cell) | | |
| Company Security Officer<br>Director Corporate Security<br>Tesoro Companies Inc. LLC | XXX-XXX-XXXX (office)<br>XXX-XXX-XXXX (cell) | | |
| USCG National Response Center | (800) 424-8802 | | |
| USCG MSO, Portland | (503) 240-9301 | | |
| State of Washington Department of Emergency Management | (800) 258-5990 | | |
| Clark County Emergency Preparedness | (360) 737-1911 | | |
| Vancouver Police/Fire/Emergency Services | 911 | | |
| | | | |
| | | | |
| **NEIGHBORING AREA FACILITIES** | | | |
| Port of Vancouver USA | (360) 693-3611 | | |
| | | | |
| | | | |
| **OUTSIDE AGENCY PHONE CONTACTS** | | | |
| FBI Portland | (503) 224-4181 | | |
| Washington State Highway Patrol | (360) 449-7900 | | |
| Washington State Fire Marshall | (360) 596-3900 | | |
| | | | |
| | | | |

# Vancouver Energy
# Construction Security Plan

EFSEC Application for Site Certification No. 2013-01
Docket No. EF131590

## Appendix D
## Bomb Threat

# Appendix D
# Bomb Threat Procedures

If You Receive a Telephone Bomb Threat

TIME _____ DATE _____

Be calm – listen carefully – pretend difficulty with hearing – write exact message.

_____

_____

_____

_____

SEX: MALE ☐ FEMALE ☐ ADULT ☐ JUVENILE ☐

| VOICE CHARACTERISTICS | | SPEECH | | LANGUAGE | |
|---|---|---|---|---|---|
| ☐ LOUD | ☐ SOFT | ☐ FAST | ☐ SLOW | ☐ EXCELLENT | ☐ GOOD |
| ☐ HIGH PITCH | ☐ DEEP | ☐ DISTINCT | ☐ DISTORTED | ☐ FAIR | ☐ POOR |
| ☐ RASPY | ☐ PLEASANT | ☐ STUTTER | ☐ NASAL | ☐ FOUL | |
| ☐ INTOXICATED | | ☐ SLURRED | ☐ LISP | | ☐ OTHER |
| | ☐ OTHER | | | | |
| | | | ☐ OTHER | | |

| ACCENT | | MANNER | | BACKGROUND NOISES | |
|---|---|---|---|---|---|
| ☐ LOCAL | ☐ NOT LOCAL | ☐ CALM | ☐ ANGRY | ☐ FACTORY | ☐ TRAINS |
| ☐ FOREIGN | ☐ REGION | ☐ RATIONAL | ☐ IRRATIONAL | ☐ MACHINES | ☐ ANIMALS |
| ☐ Other | | ☐ COHERENT | ☐ INCOHERENT | ☐ BEDLAM | ☐ QUIET |
| | | ☐ DELIBERATE | ☐ EMOTIONAL | ☐ MUSIC | ☐ VOICES |
| | | ☐ RIGHTEOUS | ☐ LAUGHING | ☐ OFFICE | ☐ AIRPLANES |
| | | | | ☐ MACHINES | ☐ PARTY |
| | | | | ☐ MIXED | ☐ ATMOSPHERE |
| | | | | ☐ STREET TRAFFI | |

Keep caller talking—if caller seems agreeable to further conversation, ask questions like:

When will it go off? Certain hour _____ Time remaining _____

Where is it located? Building _____ Area _____

What kind of bomb? _____ Where are you now? _____

How do you know so much about the bomb? _____

What is your name and address? _____

If the building is occupied, inform caller that detonation could cause injury or death.

Did caller appear familiar with plant or building by his description of the bomb location? _____