
Critical Infrastructure Protection Plan Portland / Vancouver Urban Area

Submitted to
City of Portland, Oregon

Prepared by



August 2007

Critical Infrastructure Protection Plan

Portland/Vancouver Urban Area

This initial version of the Portland/Vancouver Area critical Infrastructure Protection Plan represents the first-ever attempt by public and private infrastructure owners and operators in the urban area to define, identify, and prioritize regionally-critical infrastructure. Although labeled as a plan, the document represents both a report on the process used to begin plan development and a guide for future development of the plan.

This document was prepared under a grant from the Office of State and Local Government Coordination and Preparedness (SLGCP), United States Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of SLGCP or the U.S. Department of Homeland Security.

The plan will be further developed and maintained by the group or organization responsible for management of the Urban Areas Security Initiative (UASI) Grant program in the Portland/Vancouver area.

Executive Summary

Background:

The team managing implementation of the Department of Homeland Security's Urban Areas Security Initiative (UASI) grant program for the Portland/Vancouver urban area, called the Urban Area Points of Contact (UAPOC) Group, initiated an effort to prepare a Portland/Vancouver Urban Area Critical Infrastructure Protection Plan (CIPP). CH2M HILL was selected to facilitate the process and prepare the plan.

The Portland/Vancouver Urban Area was defined as the city of Portland, and the five surrounding counties of Clackamas, Columbia, Multnomah, and Washington in the state of Oregon and Clark in the state of Washington.

Results:

The Critical Infrastructure Protection Plan development process yielded several positive results.

- First, a definition of critical infrastructure for the region was established. Thresholds for each sector and sub-sector were adopted with the consensus of plan development participants.
- Next, a methodology for assessing infrastructure criticality was developed and was used to score and prioritize the critical infrastructure assets. A total of 375 critical infrastructure assets of an identified 777 assets within the urban area were scored and prioritized.
- Finally, an infrastructure interdependencies workshop was conducted for regionally critical infrastructure owners/operators. The workshop enhanced the understanding of interdependencies and their importance to infrastructure planning.

Plan Gaps:

This effort was very ambitious. It broke new ground regionally and perhaps nationally in the development of a comprehensive methodology for the identification, categorization, and prioritization of critical assets within a region. Gaps in the plan include:

- **Inconsistent Participation:** Some sectors had gaps in participation. For example, the Banking, Healthcare, and Food/Agriculture sectors were poorly represented. As a result, the information received and asset inventory for these sectors is incomplete.
- **Inconsistent Asset Scoring:** All asset owners/representatives were asked to score their respective assets. This resulted in inconsistent scores for similar assets in some cases.

Follow-on Recommendations:

- Convene a meeting with the participating organizations and agencies to announce the findings and results of the plan. Solicit ideas and formulate next-step actions for further progress and refinement of the plan.
- Continue obtaining completed prioritization questionnaires. There are gaps within certain sectors.

- Normalize questionnaire scoring. Review and adjust scoring results. Some groups have unusually high (or low) scores. This may have been caused by confusion or uncertainty by the respondents in filling out the questionnaires, particularly in the interdependency section of the questionnaire. Questionable high scores were noted for one telecom central office, one dam, and several levees. Questionable low scores were noted for several aviation and maritime facilities.
- Establish more consistent interdependency scores. Meet with key sectors and educate their representatives about the interdependency portions of the questionnaire. A better understanding should minimize the significant variances in the scores.
- Begin conducting vulnerability assessments to identify security issues and vulnerabilities for the high priority assets identified during this study.
- Provide or develop an appropriate vehicle or system for infrastructure owner/operators to exchange and share security-related information. Such a system should enable simple, secure, rapid and reliable transmission and exchange of information and needs to be scalable, so that the system can begin with a few selected groups and increase rapidly to serve larger groups of owners/operators. The system needs to be able to interface with a wide variety of technologies and user groups, including state and local government agencies and public and private organizations. Finally, the system should be capable of layered access to information, so that fully authenticated groups would be authorized to receive all available information, while unauthenticated groups could only access selected portions of the information.
- Incorporate key recommendations from the Interdependency Workshop. In particular, establish an interdependency forum serving infrastructure owners/operators. The forum would serve as a process to foster ongoing participation and better understanding of interdependencies. Goals of the forum would be increasing education and sharing information among infrastructure sectors, and to develop a methodology for encouraging ongoing participation and continued involvement from key owners/operators. Create and foster cross-sector partnerships focused on infrastructure security and disaster resilience.
- Encourage and support the development of statewide plans (Oregon and Washington) to meld the states' priorities for critical infrastructure protection into the Portland/Vancouver urban area plan.

Contents

Section	Page
1 Introduction.....	1-1
1.1 Purpose	1-1
1.2 Scope.....	1-2
1.3 Background	1-2
1.3.1 National Efforts.....	1-3
1.3.2 State Efforts.....	1-5
1.3.3 Regional Efforts.....	1-7
1.3.4 Canadian National Critical Infrastructure Asset Protection.....	1-8
2 Critical Infrastructure - Definition and Identification	2-1
2.1 Definition.....	2-1
2.1.1 Definition of Critical Infrastructure	2-1
2.2 Identification	2-2
2.2.1 Identification Process	2-2
2.2.2 Critical Infrastructure Sector Thresholds	2-2
2.2.3 Portland/Vancouver Urban Area Thresholds.....	2-2
3 Prioritization	3-1
3.1 Methodology	3-1
3.1.1 Key Attributes of Critical Infrastructure	3-1
3.1.2 Evaluated Prioritization Methods	3-2
3.1.3 Selected Prioritization Approach.....	3-2
3.1.4 Impact Categories.....	3-6
3.1.5 Impact Levels	3-6
3.1.6 Interdependencies	3-8
3.1.7 Importance Weights	3-9
3.1.8 Calculation of Prioritization Scores.....	3-9
3.1.9 Methodology Benefits	3-10
3.2 Collection of Asset Information.....	3-10
3.3 Responses	3-14
3.4 Interdependencies Workshop.....	3-15
3.4.1 Event Scenarios	3-16
3.4.2 Workshop Outcomes.....	3-17
3.4.3 Workshop Results and Affect on Prioritization Scoring Process	3-18
3.4.4 Interdependencies Workshop Summary Report.....	3-18
3.5 Prioritization Scoring Results	3-18
4 Protection Recommendations	4-1
4.1 Introduction.....	4-1
5 Future Actions.....	5-1
5.1 Introduction.....	5-1
5.2 Problems Encountered.....	5-1
5.2.1 Inventory and Participation	5-1
5.2.2 Scoring Consistency	5-1
5.3 Follow-on Recommendations	5-2
5.3.1 Continue Obtaining Completed Questionnaires.....	5-2
5.3.2 Normalize Questionnaire Scoring	5-2
5.3.3 Establish Consistent Interdependency Scores	5-2

5.3.4	Begin Vulnerability Assessment Process.....	5-2
5.3.5	Information Exchange.....	5-2
5.3.6	Statewide Plans.....	5-3
APPENDIX A - Participating Organizations		1
APPENDIX B - Grant Programs.....		1
APPENDIX C - Scoring Results		1
APPENDIX D - Protection Recommendation Source Documents.....		1
APPENDIX E - Interdependency Workshop Report.....		1

Exhibits

Exhibit 1-1	1-1
Five-County Urban Area – Clackamas, Columbia, Multnomah and Washington County in Oregon, and Clark County in Washington.....	1-1
Exhibit 1-2	1-3
NIPP Protection Framework.....	1-3
Exhibit 1-3	1-4
NIPP Risk Management Framework.....	1-4
Exhibit 1-4	1-9
Canadian NCIAP Scoring Methodology.....	1-9
Exhibit 3-1	3-3
Generalized Representation of Value Modeling.....	3-3
Exhibit 3-2	3-7
Impact Categories.....	3-7
Exhibit 3-3	3-8
Impact Category Example.....	3-8
Exhibit 3-4	3-11
Questionnaire.....	3-11
Exhibit 3-5	3-12
Prioritization Questionnaire Instructions	3-12
Exhibit 3-6	3-14
Number of Facilities by Sector.....	3-14
Exhibit 3-7	3-17
Sector Interdependency Diagram Example – Dam Break Scenario	3-17
Exhibit A-1	A-1
List of Participating Organizations.....	A-1

Acronyms and Abbreviations

24X7	Twenty-four hours a day, seven days a week
AASHTO	American Association of State Highway Transportation Officials
AHP	Analytic Hierarchy Process
ARC	Airport Reference Code
ATM	Automated Teller Machine
BPA	Bonneville Power Administration
BSL2	Bio-safety Level 2
BZPP	Buffer Zone Protection Program
CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability
CBR	Chemical, Biological, or Radiological
CBRNE	Chemical, Biological, Radiological, Nuclear or Explosive
CCTV	Closed-circuit television
CDC	Centers for Disease Control and Prevention
CI/KR	Critical Infrastructure/Key Resources
CIPP	Critical Infrastructure Protection Plan
COG	Continuity of Government
COOP	Continuity of Operations
DHS	Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
EAS	Emergency Alert System
EOC	Emergency Operations Center
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
HSOC	Homeland Security Operations Center (now the NOC – National Operations Center)
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation, and Air Conditioning

ISP	Internet Service Provider
IT	Information Technology
kV	Kilovolt
LNG	Liquefied Natural Gas
MIT	Massachusetts Institute of Technology
MW	Megawatt
NCIAP	National Critical Infrastructure Asset Protection
NERC	North American Electric Reliability Corporation
NICC	National Interagency Coordination Center
NIPP	National Infrastructure Protection Plan
NJSP	New Jersey State Police
NOC	National Operations Center
NRC	Nuclear Regulatory Commission
OCATS	Oregon Critical Asset Team Survey
OEM	Office of Emergency Management
OHSP	(New Jersey) Office of Homeland Security and Preparedness
ODP	Office for Domestic Preparedness
PIH	Poisonous by Inhalation
PNWER	Pacific Northwest Economic Region
PPE	Personal Protective Equipment
PUC	Public Utilities Commission
SAV	Site Assessment Visit
SCADA	Supervisory Control and Data Acquisition
SMART	Simple Multi-Attribute Rating Technique
UAPOC	Urban Area Points of Contact
UASI	Urban Areas Security Initiative
UAWG	Urban Area Working Group
USDA	U.S. Department of Agriculture
VRAP	Vulnerability Risk Analysis Program

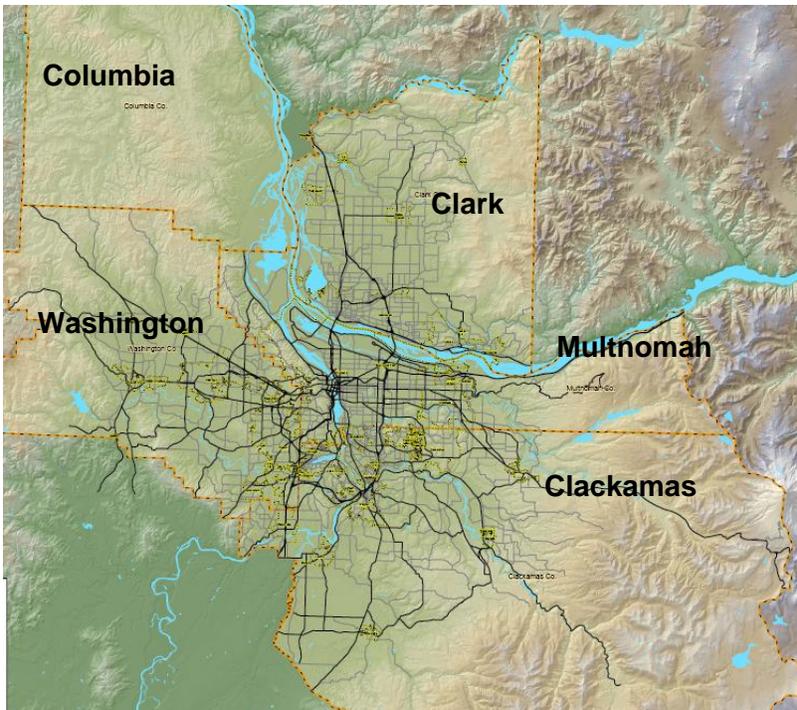
1 Introduction

1.1 Purpose

Since 2003, the Department of Homeland Security (DHS) has provided funds to the Portland/Vancouver Urban Area through its Urban Areas Security Initiative (UASI) grant program to strengthen the region's terrorism incident preparedness, prevention, response, and recovery capabilities. The Portland/Vancouver urban area program is managed by the Urban Area Points of Contact (UAPOC) Group and a larger Urban Area Working Group (UAWG), which includes the UAPOC Group itself and the chairs of numerous regional discipline-focused workgroups. The UAPOC Group dedicated fiscal year 2005 UASI grant funds to developing an urban area critical infrastructure protection plan (CIPP) and selected CH2M HILL to facilitate, process, and prepare the plan.

The UAPOC Group's goal in preparing the CIPP is to provide a blueprint or framework for future security enhancements in the urban area's critical public systems and facilities.

The Portland/Vancouver Urban Area is defined as the city of Portland, Oregon, along with the five surrounding counties: Clackamas, Columbia, Multnomah, and Washington (all in the state of Oregon), and Clark County (in the state of Washington).



The region covered by the project is indicated in Exhibit 1-1.

EXHIBIT 1-1
Five-County Urban Area –
Clackamas, Columbia, Multnomah
and Washington County in Oregon,
and Clark County in Washington

1.2 Scope

The scope of the work initiated by the UAPOC Group was to develop a plan that would:

- Formally define critical infrastructure for the Portland/Vancouver Urban Area
- Identify the urban area’s critical public and private infrastructure
- Identify categories of critical public and private infrastructure
- Identify interdependencies between the urban area’s critical public and private infrastructure
- Group the urban area’s critical public and private infrastructure into identified categories
- Prioritize the urban area’s critical public infrastructure by category
- Identify means and methods of protection for the urban area’s critical public infrastructure using best practices, industry and national standards, and/or the recommendations of recognized protection agencies (e.g., the Federal Bureau of Investigation (FBI) and DHS)
- Provide recommendations for:
 - Protection approaches for categories and priorities of infrastructure and systems
 - Agreements needed to enhance protection
 - Information sharing between infrastructure sectors, levels of government, and disciplines

1.3 Background

Several communities have undertaken efforts to identify and prioritize their critical infrastructure (CI), often in response to the National Infrastructure Protection Plan (NIPP) and related national programs like the Buffer Zone Protection Program (BZPP). In some cases – as in New Jersey, described below – it was done unilaterally prior to promulgation of federal programs. In the absence of an existing federal standard, each community determined its own methodology.

One commonality in the other approaches reviewed for this plan and how they differ from the approach used for this effort is that the criticality of a given infrastructure asset was not established as a threat-independent ranking. The other approaches applied some form of vulnerability analysis – usually against a terrorist attack – to generate a ranked list based upon the risk generated by that threat. The Portland/Vancouver Urban Area method ranks all critical infrastructure assets in terms of the impact the loss of each asset would create regardless of the event – whether manmade or natural – that caused the loss. This approach provides a useful tool for emergency planning in that this ranked list can easily be analyzed against threats from a major earthquake or volcanic eruption to criminal or terrorist activity.

Put more simply, the Portland/Vancouver Urban Area approach does not use asset vulnerability in determining its protection priorities; it relies on regional asset criticality to guide those decisions.

1.3.1 National Efforts

The National Infrastructure Protection Plan

To establish a benchmark for the efforts of developing the Portland/Vancouver Urban Area CIPP, the National Infrastructure Protection Plan (NIPP) was first examined.

The NIPP provides the unifying structure for the integration of existing and future Critical Infrastructure/Key Resources (CI/KR) protection efforts into a single national program. The NIPP framework enables the prioritization of protection initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters.

Achieving the NIPP goal requires a collaborative partnership between and among a diverse set of security partners, including the federal government; state, territorial, local, and tribal governments; the private sector; international entities; and nongovernmental organizations. The NIPP provides the framework that defines the processes and mechanisms that these security partners will use to develop and implement the national program to protect CI/KR across all sectors over the long term. Refer to Exhibit 1-2.

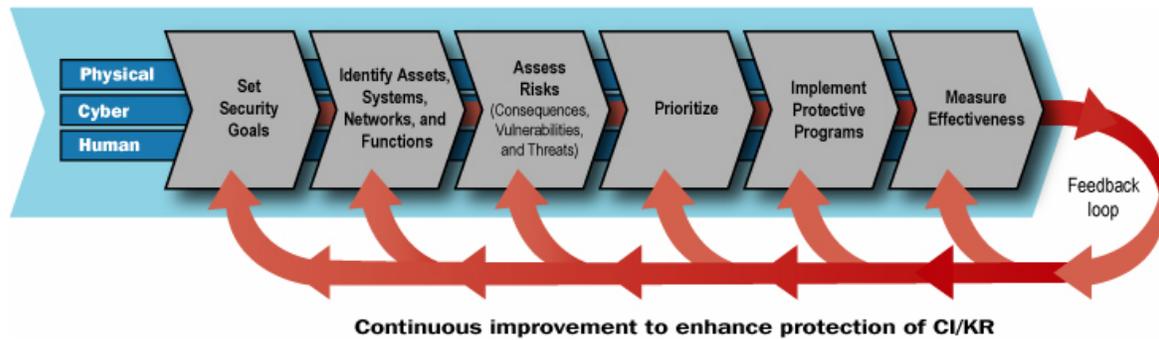
NIPP Goal: Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and strengthening national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

EXHIBIT 1-2
NIPP Protection Framework



The NIPP Risk Management Framework is the cornerstone of the NIPP. The framework includes six steps that entail setting security goals; identifying assets, systems, networks, and functions; assessing risk; prioritizing; implementing protective programs; and measuring effectiveness. Refer to Exhibit 1-3.

EXHIBIT 1-3
NIPP Risk Management Framework



Risk is defined as the potential for loss, damage, or disruption to the Nation's CI/KR resulting from destruction, incapacitation, or exploitation during some future manmade or naturally occurring event.

The NIPP Risk Management Framework:

- Establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk
- Provides for continuous improvement and feedback
- Provides the framework to prioritize CI/KR protection for assets, systems, networks, and functions
- Is flexible and adaptable to the risk landscape of each sector

Development of the NIPP was built on a series of progressively focused national policy documents designed to use a risk management framework to foster a more secure environment for the nation's citizens and critical infrastructure:

1. National Strategy for Homeland Security & National Security Act of 2002: Mobilizes and organizes the United States to secure the U.S. homeland from terrorist attacks.
2. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets: Strategy to secure infrastructures and assets vital to American public health and safety, national security, governance, economy, and public confidence.
3. Homeland Security Presidential Directive (HSPD) 7: Critical Infrastructure Identification, Prioritization, and Protection to establish national policy for federal departments and agencies to identify and prioritize CI and protect it from terrorist attacks.

4. National Strategy to Secure Cyberspace: Plan to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control, or with which they interact.

Through the NIPP framework, DHS works with states and other government and private sector security partners to gain an understanding of how CI/KR protection is being conducted across the country, the priorities and requirements that drive these efforts, and the ways in which such efforts are funded.

Risk Analysis and Management for Critical Asset Protection

DHS is working to develop a standardized risk assessment methodology, Risk Analysis and Management for Critical Asset Protection (RAMCAP) that will be used to compare risk to CI across communities as well as across infrastructure sectors. However, the RAMCAP methodology is still undergoing development and the exact release date remains uncertain. Originally scheduled for a 2005 release, it was determined that the initial version did not adequately provide a means to ensure that unique factors were considered in some sectors. Failing to address those factors made cross-sector comparisons less valid. The efforts presently underway are intended to tailor the RAMCAP process, creating separate versions for each sector that will perform a thorough analysis of that sector and then allow a valid cross-sector comparison of the risk results. Release of these RAMCAP versions is expected sometime in 2007.

1.3.2 State Efforts

Previous State of Oregon Assessments

An effort, called the Oregon Critical Asset Team Survey (OCATS), was initiated shortly after September 11, 2001, by the Oregon State Police to identify and assess critical infrastructure. The Oregon State Police received lists of critical infrastructure from each county. The assets were subsequently included in a ranking process by the U.S. Department of Justice. It is unknown how the original list of critical infrastructure was developed within each county, as there was no standard definition of critical infrastructure used in the process. Each of the assets was evaluated by local law enforcement personnel using the CARVER methodology.

Developed by the U.S. Department of Defense to assess and set priorities for military targets, CARVER is an acronym for Criticality, Accessibility, Recoverability, Vulnerability, Effect and Recognizability.

- **Criticality** refers to how important the target is.
- **Accessibility** refers to how easily a target can be reached.
- **Recoverability** refers to how long it will take to replace or repair the target.
- **Vulnerability** refers to how susceptible the target is to an attack.
- **Effect** refers to the impact the target's destruction will have on the public.
- **Recognizability** refers to how readily a target can be identified and not confused with other structures.

State of New Jersey Initiatives

The State of New Jersey reacted before the U.S. government in implementing a unified approach to identifying CI, quantifying risk, and requiring mitigation. The State established the New Jersey Domestic Security Preparedness Task Force after the New Jersey Domestic Security Preparedness Act was passed and went into effect on October 4, 2001, less than a month after the September 11 attacks. Their first product was the identification of the 100 most critical facilities statewide, followed by a 90-day period for each of those “Top 100” to self-conduct a vulnerability assessment and implement measures to mitigate identified vulnerabilities. The approach used was based on the CARVER method.

(From: <http://www.njhomelandsecurity.gov/dsptf/NJDSPTF-04-05-021706.pdf>)

New Jersey’s critical sites include business/industry infrastructures, communication facilities, dams, government infrastructure, recreation centers, retail shopping areas, public utilities, transportation sites, and chemical manufacturing and storage locations. In July 2002, the Task Force issued an order requiring measures to improve the level of protection from terrorism at the most critical of these sites.

Continuing subsequent efforts to evaluate potential targets, the Task Force refined its evaluation criteria by placing the sites in five tiers, with Tier 1 being the most critical. The New Jersey tiering system is as follows:

- **Tier 1** critical infrastructure sites are those identified by the Task Force and its agencies that have met certain Department of Homeland Security criteria.
- **Tier 2** critical infrastructure sites are those sites that the Task Force (working with member agencies) determined met certain state criteria for criticality such as capacity, population served, etc. Sites assigned to Tiers 1 and 2 represent the facilities currently receiving priority attention from the state.
- **Tiers 3 through 5** capture sites that do not meet the criticality levels of Tiers 1 and 2, but present areas of concern based on specific threat scenarios. They have been identified by the Task Force’s member state agencies or county agencies.

(From: http://www.nj.gov/oag/DSPTF_2003_AnnRpt_052804.pdf)

New Jersey also implemented a comprehensive field visitation program that has the capability to deliver security and preparedness assistance to designated critical infrastructure facilities with the purpose of better security and preparation for acts of terrorism as well as all natural and manmade hazards. The field visit teams are composed of staff from the Office of Homeland Security and Preparedness (OHSP), the New Jersey State Police (NJSP), the New Jersey Office of Emergency Management (OEM), various state departments, and representatives from county prosecutors’ offices, and local police and fire departments.

The teams assist both the private sector and the public sector in preventing and preparing for a potential terrorist attack, identifying and reducing the possible consequences of such an attack, and enhancing the integrated protection, preparedness, and readiness capabilities of the facility, local law enforcement, and emergency response organizations. During a Site Assessment Visit (SAV) the team conducts both a comprehensive, facility-specific security

vulnerability assessment using a computer-based tool known as Site Profiler and a thorough review of the facility and government response organizations' contingency action plans. Contingency action plans are specific preparedness plans and emergency response readiness measures.

The visitation schedule is developed by the OHSP based upon priorities driven by current threat and risk analysis of facilities in the State Critical Asset Tracking System. Private sector participation is maintained through awareness of the obvious benefits of ensuring emergency responders have a current understanding of a facility's vulnerabilities and emergency response needs, as well as thorough awareness that allocation of additional target hardening and risk mitigation resources will be prioritized through this site visitation process.

1.3.3 Regional Efforts

King County, Washington (Region 6 Critical Infrastructure Protection Plan)

King County uses a three-tier method to categorize critical infrastructure. Critical infrastructure is grouped by tiers depending upon their sector category. The County assigns top priority and funding to critical infrastructure within the top tier. The tiering system emphasizes a cascading effect, so that the highest priority is assigned to those sectors depended upon by other sectors. The tiers are:

- **Tier 1:** Energy, Water/Wastewater, Information Technology (IT), Telecommunications, Transportation, Healthcare Systems (Emergency Medical Services, Advanced Life Support, Hospitals, Public Health, Laboratories)
- **Tier 2:** Government Facilities, Banking/Finance, Food/Agriculture, Defense Industrial Base, Postal, Shipping
- **Tier 3:** Icons and Monuments, Chemical Industry, Emergency Services, Commercial Facilities

State of Washington Efforts

Washington State directed each infrastructure sector to identify its top 10 critical assets, resulting in 170 critical infrastructure assets over 17 sectors. The state's critical infrastructure asset database included:

- A standard naming convention so that commonality was reached in naming assets from varying regions.
- Critical nodes for cascading effects and the consequences that a disrupted sector has on other systems.

The Washington State study used the following evaluation criteria: human health, economics, national security, and environmental impacts. The approach is very qualitative

as each asset is assigned a consequence of 1 to 5 and a comprehensive point scoring system is not used. No weighting system or other approach is used to capture the relative importance of each of the criteria.

1.3.4 Canadian National Critical Infrastructure Asset Protection

The Canadian National Critical Infrastructure Asset Protection (NCIAP) program uses the following evaluation criteria: human health, economics, national security, public confidence, and interdependency impacts. It also uses a point system where impacts are gauged as follows: Severe=15, High=5, Medium=3, Low=1. No weighting system or other approach is used to capture the relative importance of each of the criteria. The NCIAP methodology is shown in Exhibit 1-4 on the following page.

EXHIBIT 1-4
Canadian NCIAP Scoring Methodology

Impact Factor	Severe	High	Medium	Low
Score	15	5	3	1
Concentration of People and Assets Impact (potential for catastrophic effects)	Greater than 10,000 people	Between 1,000 and 10,000 people	Between 100 and 1000 people	Less than 100 people
Economic Impact Direct cost of restoration including critical information and information technology (service relies on or asset contains critical information and IT)	Direct damage and restoration > \$1 billion	Direct damage and restoration \$100 million to \$1 billion	Direct damage and restoration \$10 to \$100 million	Direct damage and restoration under \$10 million
Critical Infrastructure Sector Impact (service or asset relates to a critical infrastructure sector)	Sector may shut down or international impact	National Provincial	regional or	Local
Interdependency Impact	Debilitating impact on other sectors	Significant impact or disruption to other sectors	Moderate impact on important missions of other sectors	Minor impact on important missions of other sectors
Service Impact (potential for immediate significant impacts)	High cross-sector cost, recovery time longer than one year (years)	High cost, long recovery time (months - year)	Medium cost, significant recovery time (days - weeks)	Low cost, brief recovery time (hours - days)
Public Confidence Impact	High national risk and ability to control in doubt	Public perceives high national risk and low ability to control risk	Public perceives moderate risk and moderate ability to control risk	Public perceives low risk and high ability to control risk

Total Score

Notes:

An inventory of assets and/or services is required for completeness and full documentation.

If an asset is not critical as it has a negligible consequence, a score of "0" should be used.

This assessment can be refined using quantitative scoring (such as 0 to 15).

Estimates can be further refined by having experts examine other variables such as potential impact on people, the environment, confidence in government, etc. either through models or through Business Impact Assessment studies.

2 Critical Infrastructure – Definition and Identification

2.1 Definition

2.1.1 Definition of Critical Infrastructure

The USA Patriot Act of 2001, Homeland Security Presidential Directive 7 (HSPD-7), and the draft 2006 National Infrastructure Protection Plan (NIPP), define critical infrastructure as:

- **Critical Infrastructure – National Definition:**
“Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

The starting point for the Portland/Vancouver Urban Area definition for critical infrastructure was developed by the UAPOC Group and used in the plan kickoff meeting in April 2006; it stated:

- **Regional Critical Infrastructure – Starting Definition – April, 2006:**
“Publicly and privately controlled systems and assets essential to the healthy functioning of the entire urban area community, most particularly those that are essential to the security, safety, health and/or economy of the urban area and its residents. Incapacitation or destruction of any of these systems or assets would have a serious impact on public safety, health or security, the functioning of government, and/or regional economic security.”

This definition was discussed and edited during several workshops with sector representatives. After several workshops, the resulting regional definition for critical infrastructure was:

- **Portland/Vancouver Urban Area Critical Infrastructure Definition – September, 2006:**
Publicly and privately controlled systems and assets, including the built and natural environments and human resources, essential to the sustained functioning of the Portland/Vancouver metropolitan area including the counties of Clackamas, Columbia, Multnomah, and Washington in Oregon and Clark County in Washington. Such systems and assets specifically include those necessary to ensure continuity of security, safety, health, and sanitation services, support the area's economy, and/or maintain public confidence. Incapacitation or destruction of any of these systems or assets would have a debilitating impact on the area either directly, through interdependencies, and/or through cascading effects.

2.2 Identification

2.2.1 Identification Process

In order to identify the regional infrastructure that is considered critical, it was necessary to develop sector threshold definitions, which could be used to filter the critical from non-critical infrastructure. The starting point for developing the Portland/Vancouver urban area thresholds was the NIPP sector thresholds.

2.2.2 Critical Infrastructure Sector Thresholds

The NIPP establishes thresholds for each of the seventeen critical infrastructure sectors. These thresholds establish the measurement by which an asset is considered critical or non-critical. For example, electrical power substations are defined as critical within the NIPP on the basis of their voltage and population served. From the NIPP:

Critical electric substations (are defined as having voltages of) 500 kV or larger, and substations 345 Kv or larger that are part of a critical system supporting population in excess of one million people.

2.2.3 Portland/Vancouver Urban Area Thresholds

A series of workshops were held with sector representatives to discuss, identify, and vote on appropriate sector thresholds. Beginning with the NIPP thresholds, a series of sector-specific thresholds were developed that uniquely identify the requirements for critical infrastructure within the Portland/Vancouver Urban Area. Typically, each sector discussed their appropriate threshold(s) within a group of eight to ten sector representatives who represented the various elements of their particular sector.

The threshold definitions that were developed for each of the seventeen critical infrastructure sectors are shown in the following pages. The national thresholds are shown for reference in the left-hand column, with the developed Portland/Vancouver Urban Area thresholds shown in the right-hand column.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
1	Healthcare	<ul style="list-style-type: none"> • Primary medical care facilities with unique services (e.g. shock trauma units) serving populations of greater than 250,000. • Primary blood supply facilities servicing national and regional areas. • National Stockpile and unique pharmaceutical (e.g., vaccine facilities for flu, smallpox) facilities. 	<ul style="list-style-type: none"> • Strategically located public healthcare emergency response system resources including medical emergency operations centers, epidemiology, surveillance systems, mobile trauma units, emergency transport services, flight units, laboratories, sanitation, HAZMAT, infection control, isolation and quarantine facilities, morgue facilities, and other essential public health emergency medical services required for sustainment of the delivery of emergency healthcare for the residents of the Portland/Vancouver Urban Area. • Private healthcare facilities and healthcare delivery networks including acute care, critical care, infectious disease, burn, trauma, psychiatric, rehabilitation, long-term care, academic, veterans, and military hospitals that have at least a 50-bed capacity or that individually provide at least 10 percent of the Portland/Vancouver Urban Area's emergency or specialty healthcare services. • Healthcare laboratories and research facilities that are designated as a BSL2 level or higher or possess the capability to manage Select Agents and/or High Consequence Pathogens as defined and determined by the Centers for Disease Control (CDC) and U.S. Department of Agriculture (USDA). • Public and private pharmaceutical and medical supply stockpile resources, storage areas, and delivery systems such as the Strategic National Stockpile (federal stockpiles of pharmaceuticals and critical medical supplies), Chempacks (federal stockpiles of nerve agent antidote and ventilators), personal protective equipment (PPE) stockpiles, and Cities Readiness Initiative (mass medication distribution program) assets, which support the delivery of emergency medical treatment for first responders and the residents of the Portland/Vancouver Urban Area. • Major blood supply facilities serving the Portland/Vancouver Urban Area, to include collection, testing, laboratory, processing storage, maintenance, distribution, treatment, and monitoring infrastructure.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
2	Emergency Services – 911 Centers	<ul style="list-style-type: none"> National Emergency Operations Centers (e.g., HSOC, NICC, NRC, etc.); Operation centers responsible for receiving and disbursing National Strategic Stockpile supplies at the state level, and in support of urban center distributions with populations greater than one million. 	<ul style="list-style-type: none"> County, city and special district Emergency Operations Centers; state agencies' emergency services communications centers. The emergency medical communication system centers (including towers and/or dispatch centers) that service the counties plus healthcare system-specific communication centers, and the (7) public safety answering points (PSAP). Special resources housing critical equipment, vehicles, or other assets necessary for public welfare (such as Hazmat response, bomb squad equipment, CBRN mitigation equipment) that cannot easily be replicated.
3	Government Facilities	<ul style="list-style-type: none"> Federal or State-level COOP/COG Facilities. 	<ul style="list-style-type: none"> Co-located county, city, state centers of government performing critical functions of service to the region, including unique operations of national security impact, i.e., hazardous materials, response, emergency management, and U.S. Department of Defense (DOD) support. Facilities performing criminal justice functions, such as court administration, legal trials, and incarceration (>500 beds). May include facilities of mixed use and of regional iconic value. Overall loss creates > \$500 million in economic impact and has a labor force capacity to potentially unemploy 1,000 people.
4	Commercial Buildings	<ul style="list-style-type: none"> Commercial Centers: Loss creates economic impact of greater than \$10 billion or has a capacity greater than 35,000 individuals. Office Buildings <ul style="list-style-type: none"> a • Height greater than 500 feet and/or of significant importance. b • Economic Impact of loss greater than \$10 billion. c • Capacity greater than 8,000 individuals. 	<ul style="list-style-type: none"> Commercial Centers: Loss creates economic impact of greater than \$5 billion or has a capacity greater than 20,000 individuals.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
5	Public Institutions	<ul style="list-style-type: none"> Public Institutions (Educational Facilities): Economic impact of loss greater than \$10 billion or capacity greater than 25,000 individuals. 	<ul style="list-style-type: none"> College or university research facilities of >5000 population that participate as a research center of material security interests and possess Select Agents and/or High Consequence Pathogens as defined and determined by the CDC and USDA, respectively. Facilities serving critical educational requirements of the region including medical and other critical sciences. Economic impact of loss would be >\$500 million and displace >5000 people from performing critical missions of regional significance.
6	Sports & Entertainment	<ul style="list-style-type: none"> Stadiums/Arenas: Economic impact of loss greater than \$10 billion or capacity greater than 25,000 individuals. Amusement/Theme Parks: Economic impact of loss greater than \$10 billion or capacity greater than 35,000 individuals. Hospitality Industry: Economic impact of loss more than \$10 billion or capacity more than 8,000 individuals. 	<ul style="list-style-type: none"> Large public gathering facilities that include parks, stadiums, and entertainment centers and have a capacity of >20,000 individuals. Locations for major regional events such as festivals, exhibits, and sports. Parks of >30 acres that supply water resources, navigable waterways, and/or hiking trails of major cultural and recreational value to the region. Public gathering facility that represents an icon of the region and its loss would impact public confidence and morale.
7	Monuments & Icons	<ul style="list-style-type: none"> Monuments/Icons of National Significance. 	<ul style="list-style-type: none"> Facilities and parks that have regional and national recognition symbolic of cultural values and regional geography. Loss of monument and icon would severely impact values held by 50,000 individuals of the region and cost >\$100 million to replace.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
8	Information Technology <ul style="list-style-type: none"> – Hardware – Software – Internet Service Providers – Network Access Points 	<ul style="list-style-type: none"> • IT Systems: Systems with access or control points distributed on both coasts and throughout the country. • Networks: Networks with nodes distributed on both coasts and throughout the country. • Digital Control Systems: Control Systems with access or control points distributed on both coasts and throughout the country. • Major primary data storage and processing facilities. 	<ul style="list-style-type: none"> • Public safety radio communication facilities, including towers serving first responder voice communications as part of a radio network in population centers of more than 50,000. • Microwave hubs providing voice and data transmissions for a Public Utilities Commission (PUC) certified communications provider with more than 10,000 subscribers • Internet Service Provider (ISP) Network Operations Centers serving more than 10,000 subscribers. • Govt. Network Operation Centers (NOCs) serving more than 20 percent of a local government's data or voice customers. • Data Centers that house more than 20 percent of the region's public health & safety, medical, or banking records. • Supervisory Control and Data Acquisition (SCADA) NOCs for a water, transportation or electrical utility that serves more than 20 percent of the region's population. • A local, state, or federal Emergency Response and Emergency IT Operations Center.
9	Telecom <ul style="list-style-type: none"> – Wired – Wireless 	<ul style="list-style-type: none"> • Major telephony hotels. • Control centers controlling national or regional telephone traffic. 	<ul style="list-style-type: none"> • All tandem Central Offices. • Mobile Switching Centers serving over 100,000 calls per week. • All Telco Hotels with more than four Interexchange Carrier points of presence. • Fiber routes (end-of-run) or microwave equipment serving a hospital, corrections facility, EOC or SCADA NOC with no redundancy.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
10	Broadcast Media	<ul style="list-style-type: none"> • None. 	<ul style="list-style-type: none"> • EAS (Emergency Alert System) infrastructure. <ul style="list-style-type: none"> – National Weather Service – Relay network equipment – Transceiver equipment • Stations (radio, TV) with areas of coverage that encompass the vast majority of the people within the Portland/Vancouver Urban Area, 24x7, with appropriate staff and resources to operate 24x7, licensed as a full time station. <ul style="list-style-type: none"> – Transmitters – first priority – Studio – second priority
11	Financial Services: <ul style="list-style-type: none"> – Banking – Savings – Insurance 	<ul style="list-style-type: none"> • Wholesale Securities/Funds Transfer Services in excess of \$50 billion per year. • Financial entities that provide wholesale funds or government securities transfer and settlement services. • Primary dealers in the government securities market. • Primary/backup for the backbone computer infrastructure for stock market exchanges. • Major banking and financial centers. 	<ul style="list-style-type: none"> • Retail banking transactions in excess of \$1 billion per year as a major funding source for regional households. • Commercial banking transactions in excess of \$5 billion per year as a major funding source for regional businesses. • Employs 150 or more collocated in branches/retail outlets (grocery, department stores, and financial centers). • Cluster of ATM/branches within 100 yards of major arterial roads representing \$10 million total cash reserves.
12	Dams	<ul style="list-style-type: none"> • High Hazard Dams, or Dams that produce over .5 megawatts (MW) of hydropower or provide irrigation to agriculture greater than 10,000 acres or provide for navigation on significant waterways or provide flood control or locks that provide significant waterway navigational ability or levees that provide significant flood control that the loss of which would cause significant economic impact or loss of life. 	<ul style="list-style-type: none"> • Dams that produce over 500 MW of hydropower or provide irrigation to agriculture greater than 5,000 acres or provide for navigation on significant waterways or provide flood control or locks that provide significant waterway navigational ability or flood works systems (i.e., levees, pump stations, control structures, etc.) that provide significant flood control that the loss of which would cause loss of life of over 50 people.
13	Water	<ul style="list-style-type: none"> • Water treatment facilities, ground water systems (wells), water transmission systems (aqueducts, viaducts, pipelines, open channels) that serve populations or water reservoir system(s) including ground or elevated that serve populations of greater than one million persons. 	<ul style="list-style-type: none"> • Drinking water systems that serve populations of greater than 35,000 persons and/or include a water treatment system, and/or include large raw water impoundment.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
14	Wastewater	<ul style="list-style-type: none"> Wastewater treatment facilities, wastewater collection systems and pumping systems (force mains) or wastewater storage system(s) that serve populations greater than one million persons. 	<ul style="list-style-type: none"> Wastewater systems that serve populations of greater than 100,000 persons and/or include a wastewater treatment facility.
15	Energy – Electricity	<ul style="list-style-type: none"> Major power generation facilities that exceed 2000 MW and if successfully attacked would disrupt the regional electric grid. Hydroelectric facilities and dams that produce power in excess of 2000 MW or could result in catastrophic loss of life if breached. Substations that are the sole source of power to critical commercial or government facilities. Regional transmission coordination centers: Control centers for Regional Transmission Organizations, Independent Transmission Operators, and Regional Coordinators. Transmission substations necessary for the reliable operation of the transmission grids. Electric substations 500 kV or larger, and substations 345 kV or larger that are part of a critical system supporting population in excess of one million people. 	<ul style="list-style-type: none"> Major power generation facilities that exceed 200 MW. Hydroelectric facilities and dams that produce power in excess of 500 MW or could result in catastrophic loss of life if breached. Substations that are the single-point failure of power to critical commercial or government facilities. Regional transmission coordination centers: Control centers for Regional Transmission Organizations, Independent Transmission Operators, and Regional Coordinators. Transmission substations necessary for the reliable operation of the transmission grids. Electric substations 115 kV or larger that are part of a critical system supporting population in excess of 50,000 people.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
16	Energy – Oil and Gas	<ul style="list-style-type: none"> • Refineries with refining capacity in excess of 225,000 barrels per day. • Product pipelines with a capacity in excess of 200,000 barrels per day. • Natural gas pipelines with a capacity equal to or greater than 1 billion cubic feet per day. • Natural Gas and Liquid Natural Gas Storage (LNG) facilities. • Major petroleum handling facilities such as pipelines, ports, refineries, and terminals. 	<p>Petroleum:</p> <ul style="list-style-type: none"> • Facilities with greater than 400,000 barrels of aboveground storage capacity for petroleum products. • Product pipelines with a capacity in excess of 10,000 barrels per day and/or 1000 barrels per hour. <p>Natural Gas facilities:</p> <ul style="list-style-type: none"> • Natural gas pipelines with a capacity equal to or greater than 150 million cubic feet per day. • Major petroleum handling facilities such as pipelines, pump stations, ports, refineries, and terminals with capacity in excess of 1500 barrels per hour. • Natural gas and liquidified natural gas (LNG) storage facilities of 5 million cubic feet or greater. • Control stations that are critical to the supply of natural gas to 50,000 or more customers.
17	Postal and Shipping	<ul style="list-style-type: none"> • Major collection, sorting, or distribution centers for national or regional shipments. 	<ul style="list-style-type: none"> • U.S. mail processing and distribution plants that serve one or more counties within the state. • Shipping hubs serving over 100,000 people.
18	Defense	<ul style="list-style-type: none"> • None. 	<ul style="list-style-type: none"> • Defense infrastructure providing strategic protective services for the region, as follows: <ul style="list-style-type: none"> – Air National Guard facilities having over 500 full-time personnel. – Army National Guard facilities having over 50 full-time personnel. – Coast Guard facilities serving as a communications hub for search and rescue operations, federal maritime law enforcement, and/or federal marine pollution response, and having over 50 individuals assigned, with 3+ vessels stationed. – Ship repair facilities with crane lifting capacity of 120 metric tons.
19	Transportation – Aviation	<ul style="list-style-type: none"> • Major airports (passenger and freight). 	<ul style="list-style-type: none"> • Code C or D airports based on the Federal Aviation Administration's (FAA) Airport Reference Code (ARC).

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
20	Transportation – Rail Freight	<ul style="list-style-type: none"> • Railroad Information Technology and Communications Infrastructure critical nodes. • Rail tunnels and bridges or other critical assets where no practical reroute and rebuild time is over 6 months if all resources are available, rerouting results in 75 percent degradation of service. • Primary entry points used to transport commercial or military shipments, which if destroyed would significantly impact the people, economy, or national security. • Unsecured rail yards, located within populated areas (greater than 50,000), that on any given day contain large quantities (greater than 5 tank cars) of poisonous by inhalation (PIH) materials. • Rail yards that if disabled would cause significant disruption of national economy. 	<ul style="list-style-type: none"> • Railroad information technology and communications infrastructure critical nodes. • Rail tunnels and bridges or other critical assets with no practical reroute and where rebuild time is over 6 months if all resources are available; rerouting results in 75 percent degradation of service. • Primary entry points used to transport commercial or military shipments to critical ports or maritime facilities, which if destroyed would significantly impact the people, economy, or national security. • Infrastructure which, if disabled or destroyed, could result in the deaths of 50+ people. • Unsecured rail yards that on any given day contain large quantities (greater than 5 tank cars) of poisonous by inhalation (PIH) materials. • Rail yards that if disabled would cause significant disruption of national or regional economy, over \$500 million.
21	Transportation – Mass Transit	<ul style="list-style-type: none"> • Subways: Subway systems and supporting ventilation systems. • Bus: Terminals located within urban centers with a population of greater than 500,000 or servicing >5,000 passengers daily. • Passenger Rail: Terminals located within urban centers with a population of greater than 500,000 or servicing greater than 50,000 passengers daily. • Cruise: Ports/Terminals located within urban centers with a population of greater than 500,000 or servicing greater than 10,000 passengers daily. 	<ul style="list-style-type: none"> • Mass transit assets, facilities or infrastructure with a Vulnerability Factor and a Criticality Factor each greater than or equal to 100, as defined in the DHS-ODP Special Needs Jurisdiction Tool. • Passenger Bus: Terminals located within urban centers with intermodal transit (bus and rail) capabilities. • Passenger Rail: Terminals located within urban centers with yearly ridership of greater than 500,000 passengers.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
22	Transportation – Seaports and Ferries	<ul style="list-style-type: none"> • Seaports that have designated Strategic National Defense Seaport. • Seaports that represent the majority of imports and exports of containerized and petroleum cargoes. • Seaports and facilities that service the Strategic Petroleum Reserve. • Locks and dams critical for the operation of major inland commercial waterways. • Harbor entrance waterway choke points that if blocked would deny port access. 	<ul style="list-style-type: none"> • Seaports and terminals that represent the majority of imports and exports of containerized and petroleum cargoes, including petroleum terminals. • Harbor or river entrance waterway choke points that if blocked would deny port or major waterway arterial access.
23	Transportation – Trucks	<ul style="list-style-type: none"> • None. 	<ul style="list-style-type: none"> • None.
24	Transportation – Hwy/Bridges/ Tunnels	<ul style="list-style-type: none"> • None. 	<ul style="list-style-type: none"> • All highways, bridges and tunnels with a Vulnerability Factor and a Criticality Factor each greater than or equal to 50, as defined in the American Association State Highway Transportation Officials (AASHTO) vulnerability assessment guidelines.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
25	Food and Agriculture	<p>Distribution Facilities that ship to five or more states.</p> <ul style="list-style-type: none"> • Food processors with product distribution to more than ten states. • Producers with herd of more than 20,000 bovine, 30,000 swine or 500,000 poultry or distribution to more than ten states or production of 50,000 – 250,000 bushels of crop. 	<ul style="list-style-type: none"> • Distribution and food storage facilities that ship to three or more states or internationally or have food storage valued at over \$5 million. • Processing Plants: Processing of food staples: provides 50 percent (or more) of supply of staple food products used within region. <ul style="list-style-type: none"> – Dairy processing – Meat processing – Grain milling/processing – Fruit/vegetable processing • Production Growing: Raising/Harvesting of food, providing 50 percent (or more) supply of the following: <ul style="list-style-type: none"> – Grain – Fruits/Vegetables – Poultry/Egg production – Livestock
26	Nuclear	<ul style="list-style-type: none"> • Nuclear Reactors and Spent Fuel Facilities. 	<ul style="list-style-type: none"> • Any nuclear reactors within region.
27	Chemical	<ul style="list-style-type: none"> • Sites that could cause death or serious injury in the event of a chemical release and have greater than 300,000 persons within a 25-mile radius of the facility. • Economic impact of more than one billion dollars per day (e.g., an event impacting multiple sectors and cumulatively cause this amount of economic damage). <p>Note: The term “sites” includes manufacturing plants; rail, maritime, or other transport systems; pipeline and other distribution networks; and storage, stockpile, and supply areas.</p>	<ul style="list-style-type: none"> • Chemical facilities that have less than 300,000 but more than 70,000 people living within a 25-mile radius that have offsite consequences. • Facilities with greater than 500,000 gallons of aboveground storage capacity for hazardous substances and petroleum products.

Item	Sector	National Thresholds (from DHS)	Portland/Vancouver Urban Area Thresholds
28	Manufacturing Facilities (Industrial Asset – Manufacturing Facilities)	(Commercial Center Threshold:) <ul style="list-style-type: none"> • Loss creates economic impact of greater than \$10 billion or has a capacity greater than 35,000 individuals. 	<ul style="list-style-type: none"> • Facilities with a loss creating economic impact of greater than \$500 million or employing more than 2,000 individuals. • Facilities that produce a product that is needed for national or regional security. Examples may include (if not already covered under a previous threshold) facilities that manufacture a critical component for the following industries: <ul style="list-style-type: none"> – Electrical – Water supply/waste treatment systems – Transportation of employees to work – Supply of critical items—e.g., liquid nitrogen. – Support services—communications

Decision Goal

The decision goal is the overall purpose of the evaluation. It is that which is to be accomplished by making a decision. It should clarify what is included and excluded from the scope of the evaluation.

Fundamental Values, Objectives, and Criteria

Objectives are the important non-monetary aspects of a decision that are arrived at through careful thinking about issues. In essence, they reflect repeated efforts to answer a simple question: "Why is this issue important?" When the response becomes, "Because it is," a fundamental value or objective has been identified.

Values, objectives, and criteria are often used almost interchangeably in decision analysis. Although this is not strictly correct, it rarely affects the quality of the analysis. Simply stated, values underlie and motivate objectives. An example of a value statement is, "An ecologically diverse environment is essential." Such a value motivates the objective, "reduce threats to the ecosystem." Fundamental objectives are the most basic elements in the model. They are also referred to as evaluation criteria and may be further characterized by the development of sub-criteria, which ultimately produces an objectives hierarchy (also called a value hierarchy).

Performance Measures

Once the objectives are fully developed and the decisionmaker(s) agree that they fully represent the important issues in the problem, performance measures are required to determine how well alternatives perform against the objectives. In Exhibit 3-1, performance measures are represented as scales beneath the objectives. Performance measures may be quantitative or qualitative, depending upon the objective and the availability of data for each measure.

Typically, performance measures are arithmetically transformed to a scale of zero-to-one. For example, if a cost scale ranging from \$1,000 to \$2,000 were to be converted to a zero-to-one scale, then \$1,000 would rate a "one" on the new scale; \$2,000 would rate a "zero;" and \$1,500 would rate a 0.5. This zero-to-one scale described above implies a linear relationship between cost and value. This means that increasing cost from \$1,000 to \$1,500 is as important as increasing cost from \$1,500 to \$2,000. The two incremental changes are of equivalent value. Scales can also be nonlinear when changes along the scale have different degrees of importance.

Alternatives

Alternatives are actions that may be taken to accomplish objectives. A well-considered value model includes a complete set of alternatives. Care must be taken not to exclude or overlook alternatives that might meet the stated objectives.

Alternatives are often the first components identified when evaluating infrastructure solutions. As soon as a need or problem is identified, alternatives come to mind. Typically, alternatives are identified, then the attributes are compared. It is important to re-examine

alternatives generated this way after the objectives hierarchy is well-defined so that the important values can be used to define the alternatives, instead of the other way around.

Weighting Objectives

Based on the value system of the decisionmaker(s), some objectives may be more or less important than other objectives. For example, loss of an ecosystem may be more important to a particular decisionmaker than the cost to protect that ecosystem. The desire to protect a critical salmon spawning ecosystem may result in the determination that protection costs are worth any price, deemed as insignificant compared to the potential loss of salmon spawning. Obviously, different stakeholders faced with the same problem may have different underlying value systems, and, therefore, may have a different sense of what's most important in the given problem.

This leads to the concept of "weighting" objectives. Assigning weights to objectives is a subjective exercise based on the values of the stakeholder(s). This is typically done in a workshop setting where a trained facilitator ensures that participants think clearly about the relative importance of different values. Weighting is done after the performance measures have been developed, so stakeholders can include in their consideration the extent to which the full set of alternatives vary in performance.

Weights may be assigned in a number of ways. One common approach is to allocate 100 points or "dollars" among the objectives in a manner that results in the most value or benefit (one of several methods). Weights are then converted to a zero-to-one scale regardless of the method used to obtain weights.

Rating Alternatives and Aggregating Scores

Rating or scoring alternatives is the process by which the performance measurement scales are applied to the alternatives. This is essentially a weighted averaging process where scores are weighted by the value weights and summed for each alternative.

Put more simply, rating alternatives is a process in which the scores of each alternative are weighted. Higher weighting values give more importance to an alternative. Lower weight values give lower importance to an alternative. The higher the score, the greater the impact.

Interpreting Results

The results of any decision analysis are best regarded and applied as *decision aids*. Results should inform rather than dictate the decision. The analysis provides a way of organizing and comparing complex information. To the extent the decisionmaker(s) believe that the structure of the value model represents the important issues, the weights and performance measures are appropriate, and the scores are accurate, they may be confident in the results.

It is also valuable to evaluate the model for sensitivity to weighting. If the results of the model do not change unless there are substantial changes in weights, then the decisionmaker(s) may be confident in the results.

3.1.4 Impact Categories⁵

Impact categories are the harmful attributes or events/objectives that may occur from a malevolent action. The team prepared an initial list of categories that was reviewed and discussed at a July 20, 2006 workshop with planning participants. After the workshop, a meeting was held on July 25, 2006 with a small group of planning participants to discuss and refine the list of categories. During the meeting, some categories were discarded and others added. The final list of impact categories included:

1. Human Health and Safety Impact – the number of immediate and long-term deaths that could result theoretically from worst-case damage/impairment/hostile takeover of a facility
- 2a. Economic Impact – Lost income during outage
- 2b. Economic Impact – Replacement cost
3. Emergency Systems Impact – The impact of a lost asset on emergency response capabilities, either in direct services or in enabling access to emergency services (including evacuation, access to affected locations, communications, etc.).
4. Environmental Impacts to Species and/or Ecosystems
5. Iconic/Symbolic Impact

3.1.5 Impact Levels⁶

Establishing Performance Scales

A scale of zero to four was used as the performance scale for measuring the magnitude of impact for all impact categories, except a scale of zero to one was used for iconic/symbolic impact. In all cases, a score of zero is used for no impact and four (or one for iconic/symbolic) was used to represent the maximum foreseeable impact. Specific definition of the circumstances that would merit a particular score is shown in Exhibit 3-2.

The estimated magnitude of impacts associated with the World Trade Center attack and other recent disasters was used to develop the ranges used to characterize the human health and safety and economic impact factors. For example, the World Trade Center attacks resulted in more than 2,700 deaths and estimated economic impacts (direct and indirect value added) of more than \$12 billion⁷. Also, the relationship between deaths and economic losses was set so that each impact was valued at a level that is approximately consistent with the results of recent federal government estimates of the economic impacts of a loss of life⁸. The other ranges were developed using professional judgment by the team.

⁵ Impact categories is another term for the objectives within an objectives hierarchy.

⁶ Impact levels is another term for performance measures.

⁷ *Preliminary Report, Economic Impact of the September 11 World Trade Center Attack*. New York City Central Labor Council and the Consortium for Worker Education, Fiscal Policy Institute, 2001.

⁸ *The Economic Impact of Vehicle Crashes*. U.S. Department of Transportation, 2000.

EXHIBIT 3-2
Impact Categories

Scores **Impact Categories**



1. Human Health and Safety Impact—How many immediate and long-term deaths could theoretically result from worst-case damage/impairment/hostile takeover of the facility?

4	Greater than 2,000
3	Between 2,000 and 200
2	Between 200 and 20
1	Less than 20
0	No impact



- 2a. Economic Impact—Lost Income during Outage

4	Greater than \$10 billion
3	Between \$10 billion and \$1 billion
2	Between \$1 billion and \$100 million
1	Less than \$100 million
0	No impact



- 2b. Economic Impact—Replacement Cost

4	Greater than \$10 billion
3	Between \$10 billion and \$1 billion
2	Between \$1 billion and \$100 million
1	Less than \$100 million
0	No impact



3. Emergency Systems Impact—Asset's impact to emergency response, either in direct services or in enabling access to emergency services (including evacuation, access to affected locations, communications, etc.).

4	100% Shutdown. Severs critical evacuation route, shuts down emergency systems.
3	50% Shutdown of systems within a localized area. Results in 2-3 hours of delay.
2	10% Shutdown of systems within a localized area. Results in 1 hour of delay.
1	1% Shutdown of systems within a localized area. Results in some minor delay.
0	No impact



4	Catastrophic impacts to species and/or ecosystems. Irreversible damage.
3	Severe impacts to species and/or ecosystems
2	Moderate impacts to species and/or ecosystems
1	Low impacts to species and/or ecosystems
0	No impact



5. Iconic/Symbolic Impact

1	Regional symbolic importance
0	No symbolic importance

The Impact of Asset Destruction

Participants were asked to estimate the impact that would result from the destruction of the assets for which they were responsible using a worst-case scenario that included the following characteristics:

- Complete destruction of the building, making it unusable until repaired or replaced.
- All staff working onsite are killed as a result of the incident.
- Destruction occurs at the worst-possible peak (busy) time for your industry.
- The direct attack is limited to the facility being evaluated. Simultaneous attacks on other facilities are not assumed nor are large-scale attacks affecting an entire region or sector.

Participants were also asked to consider secondary effects. For example, for a chemical plant, consider the effects of a chemical plume drifting from the plant site to adjacent areas.

Participants entered scores for each impact category for each asset. The scores were reviewed by the planning team, and some follow-up contacts were made to ensure that the approach was clear and to make any adjustments that seemed warranted.

Example

For example, consider a commercial mall facility. Assume that this mall experiences a catastrophic event and is destroyed, and that the resulting loss of income totals \$200 million until it is rebuilt and reopened. (See Exhibit 3-3 below).

Question: Assuming the destruction of a mall generates a lost income of \$200 million – what is the score for Economic Impact category 2a?

Answer: A \$200 million loss results in a score of “2” for the Economic Impact category.

EXHIBIT 3-3

Impact Category Example



4
3
2
1
0

3.1.6 Interdependencies

If destroyed, many assets would affect the performance of other assets or systems elsewhere in the region or beyond. It is important to consider these interdependencies when assessing the impacts associated with asset destruction. Thus, urban area participants were also asked to assess the impact to the following sectors if the asset being evaluated was destroyed or damaged.

- Agriculture and Food
- Banking/Finance

- Chemical
- Public Institutions/Commercial Assets
- Dams
- Defense Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare
- Information Technology
- Monuments/Icons
- Nuclear Facilities
- Postal/Shipping
- Telecom
- Transportation
- Water/Wastewater

Evaluators were asked to assign a zero to four rating for each impact category (except when rating the iconic/symbolic category, which used a rating of one-to zero) for each of these sectors.

The ratings were assumed to be cumulative over all sectors and the asset being evaluated. For example, if the asset being evaluated was given a score of 3 for an attribute, and two other sectors were given interdependence scores of 2 and 1 respectively, the total score for that category would be 6 (i.e., 3+2+1).

3.1.7 Importance Weights

A facilitated process was used during the July 20 and August 15, 16, 29, and 30 workshops to assess importance weights for each impact category. After each workshop, the participants were surveyed and asked to assign a relative weight value to each category. The resulting importance weights for each category, after considering all input, were as follows:

- Human Health and Safety Impact - 28
- Economic Impact, Lost Income during Outage - 19
- Economic Impact, Replacement Cost - 18
- Emergency Systems Impact - 18
- Environmental Impacts to Species and/or Ecosystems - 12
- Iconic/Symbolic - 5

3.1.8 Calculation of Prioritization Scores

The total prioritization score for an asset is the sum of each impact score (for the asset being evaluated and interdependencies) multiplied by its importance weight.

Example

For example, consider the commercial mall facility experiencing total destruction and an economic loss to revenue of \$200 million. The score for the Economic Impact category of the mall closure was determined earlier to have an impact score of “2.”

The importance weighting for Economic Impact - Lost Income is 19, as noted previously.

Question: Assuming the destruction of a mall results in an Economic Impact score of 2, what is the corresponding weighted score for that impact?

Answer: The weighted score is 38. The weighted score is the product of the impact score multiplied by the weighting value or ($2 \times 19 = 38$).

3.1.9 Methodology Benefits

The prioritization of critical infrastructure is a challenging process not easily accomplished. This methodology provides the following benefits:

- A sound theoretical basis
- Simplicity
- Transparent to stakeholders, with repeatable results
- Sensitivity (weighting) analysis incorporated
- Provides a foundation for additional, in-depth, risk assessment methods

In the future, more in-depth analysis can be conducted of the most critical infrastructure, including the application of threat and vulnerability assessments, to develop plans to improve the overall security of the region.

3.2 Collection of Asset Information

To obtain information about the assets identified within the region, a questionnaire was developed and sent to each infrastructure contact. Response to the questionnaire was mixed, with some sectors providing good response and others providing poor or no response. The questionnaire is shown on the following pages within Exhibits 3-4 and 3-5.

EXHIBIT 3-4
Questionnaire

INFRASTRUCTURE ASSET NAME				BACKGROUND INFORMATION														LEGEND					
[Enter name of facility here.]				EVALUATOR'S NAME: [Enter Your name here.]																<input type="text"/>	= CELLS COMPLETED BY USER.		
				REGION SERVED: [Enter Extent of Region Served by the Facility; City, County, Region, State, etc.]																<input type="text"/>	= SCORING RESULTS - DO NOT EDIT.		
				POPULATION SERVED: [Enter Number of People Directly Served by the Asset on an Average Daily Basis.]																			
SCORING ASSUMPTION				INTERDEPENDENCY IMPACT																			
Assume a worst case malevolent action causing complete destruction of the evaluated facility.				ASSET IMPACT		What is impact to other sectors if the asset being evaluated is taken out or damaged? (if no impact, enter '0').																	
Impact Level	IMPACT CATEGORY			Impact to asset on its own (0 - 4)	Agriculture & Food	Banking / Finance	Chemical	Public Institutions / Comm. Assets	Dams	Defense Base	Emerg. Services	Energy	Gov. Facilities	Healthcare	Info. Technology	Monuments / Icons	Nuclear Facilities	Postal / Shipping	Telecom	Transportation	Water / Wastewater	NOTES	
	1. Human Health and Safety Impact - How many immediate and long-term deaths could theoretically result from worst-case damage / impairment / hostile takeover of the facility?			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	[List any assumptions or scoring choices made.]
	4 Greater than 2,000 3 Between 2,000 and 200 2 Between 200 and 20 1 Less than 20 0 No impact				Enter Impact to other Sectors (0 - 4)																		
	2a. Economic Impact - Lost Income during Outage			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	[List any assumptions or scoring choices made.]
	4 Greater than \$10 billion 3 Between \$10 billion and \$1 billion 2 Between \$1 billion and \$100 million 1 Less than \$100 million 0 No impact				Enter Impact to other Sectors (0 - 4)																		
	2b. Economic Impact - Replacement Cost			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	[List any assumptions or scoring choices made.]
	4 Greater than \$10 billion 3 Between \$10 billion and \$1 billion 2 Between \$1 billion and \$100 million 1 Less than \$100 million 0 No impact				Enter Impact to other Sectors (0 - 4)																		
	3. Emergency Systems Impact - Identify asset's impact to emergency response, either in direct services or in enabling access to emergency services (including evacuation, access to affected locations, communications, etc.).			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	[List any assumptions or scoring choices made.]
	4 100% Shutdown - Severs critical evacuation route, shuts down emergency systems, severs communications capability. Results in several hours of delay or more. 3 50% Shutdown of systems within a localized area. Results in 2-3 hours of delay. 2 10% Shutdown of systems within a localized area. Results in 1 hour of delay. 1 1% Shutdown of systems within a localized area. Results in some delay, but less than 1 hour. 0 No impact				Enter Impact to other Sectors (0 - 4)																		
	4. Environmental Impacts			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	[List any assumptions or scoring choices made.]
	4 Catastrophic impacts to species and/or ecosystems. Irreversible damage. 3 Severe impacts to species and/or ecosystems 2 Moderate impacts to species and/or ecosystems 1 Low impacts to species and/or ecosystems 0 No impact			(0 - 1)	Enter Impact to other Sectors (0 - 1)																		
	5. Iconic / Symbolic Impact			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	[List any assumptions or scoring choices made.]
	1 Regional symbolic importance 0 No symbolic importance																						

EXHIBIT 3-5
Prioritization Questionnaire Instructions

<u>Item</u>	<u>Notes</u>
<i>As general note - only enter data in the white cells. Please do not make changes to the green or orange cells.</i>	
0 Copy this file and create a separate file for each asset / facility being evaluated.	Use a descriptive file name for each facility file that you create.
1 Develop a worst-case scenario for your asset(s) or facilit(ies).	<p>Worst-case scenario may vary for each facility type, but it should include the following characteristics:</p> <ol style="list-style-type: none"> 1. - Assume <u>complete</u> destruction of the facility, making it <u>unusable</u> until repaired or replaced. 2. - Assume <u>all staff working on-site are killed</u> as a result of the action. Consider long-term deaths due to release of elements of the facility. For example, a chemical plant explosion could also release chemical plumes, causing long-term deaths in the form of increased cancer rates. Use your best judgement to evaluate the impact. 3. - Assume destruction occurs at <u>worst-possible peak</u> (busy) time for your industry. 4. - Consider <u>secondary effects</u>. For example, if you are a chemical plant, consider the effects of a chemical plume drifting from your plant site to adjacent areas. List all secondary effects in the notes column to document your concerns. 5. - Assume that the direct attack is limited to the facility being evaluated. Simultaneous attacks on other facilities are not assumed in this exercise. Large scale attacks affecting an entire region or sector are not being evaluated in this exercise. For example, a nuclear blast taking out an entire City is not evaluated in this exercise.
2 Complete the background information requested for your asset(s).	<p>Provide the asset name, the region served, and the number of people directly served.</p> <ol style="list-style-type: none"> 1. - Enter text in the white cells, not the green or orange cells.
3 Answer each Impact Category questions.	Enter the answer for each impact category - enter 0, 1, 2, 3 or 4 as appropriate, looking at the impact levels provided for each score (0, 1, 2, 3, 4).
4 Identify the Interdependency impact to other sectors for each Impact Category, for the worst-case scenario.	<p>Enter the answer for each impact category, for each sector affected - enter 0, 1, 2, 3 or 4 as appropriate. Enter 0 for the sector that the asset belongs to.</p> <ol style="list-style-type: none"> 1. - Provide scores for your facility's impact to other sectors if your facility is taken out or destroyed. 2. - Refer to the same range of impact level values (0,1,2,3,4) listed for each impact category. 3. - Provide scoring for as much as you know about your facility's importance to other sectors. If you can't think of any interdependencies or don't know - enter '0'. 4. - The interdependency scores will be reviewed after the Interdependency Workshop, and will be re-evaluated if needed, to correct scoring.
5 Return the questionnaires to CH2M HILL - Forrest Gist by email: forrest.gist@ch2m.com	Please return the questionnaires by Friday, August 11.

Several meetings, email help messages, and follow-up telephone calls were made to facilitate the process of helping the respondents complete their questionnaires.

In the process of assisting the respondents, several “rules” were established to make the process easier. These include:

- **RULE 1.** Respondents were asked to add notes in the “Notes” column so it is understood what assumptions were made when completing the questionnaire.
- **RULE 2.** Human Health Impact: When completing the prioritization questionnaire, respondents’ should assume a worst-case scenario in which all people in the building are dead.
- **RULE 3.** Human Health Impact: Respondents should use 30 days as the duration for establishing the human health impact for direct and long-term deaths.
- **RULE 4.** Economic Impact: Replacement Costs: Replacement costs are capital costs — construction services to rebuild facility, purchase of new equipment and land, etc. They do not include hiring, training of new staff and knowledge lost. Respondents should make a note in Notes section if the facility is a very knowledge-based entity, in which the equipment costs are low, but the human costs (training, re-hiring, etc.) would be high.
- **RULE 5.** Iconic Impact: Consider whether the infrastructure has an iconic meaning or symbolic impact to the region. Examples might be Multnomah Falls, Timberline Lodge, etc., and probably not a pump station. (See Rule 13).
- **RULE 6.** Interdependencies for Health and Public Safety: If the public at large is affected due to an outage of the respondent’s system, rather than entering a number in each sector interdependency box, the respondents should pick one sector, “Healthcare,” for example, and put the resulting score number in that space, rather than entering a score within each sector. An example was discussed for a telecom provider. If it was to lose a key central office location, a majority of the population would be without phone, cell phone, and 911 capabilities. In such a situation, they would have impacts on every other sector. Rather than entering interdependency numbers within each sector box, the numbers were consolidated into a single sector box.
- **RULE 7.** System Outages: For certain sector groups, for example, power and telecom, taking out one facility may not have as large an impact as taking out a hub facility or taking out two or more facilities, which would be catastrophic. In such cases, a “Super-Scenario” questionnaire was developed, in which two or three simultaneous outages occur, and the questionnaire scored appropriately.
- **RULE 8.** Commonality within Sectors: Respondents should make sure that their understanding of scoring and interdependencies are consistent.
- **RULE 9.** Jurisdictional Boundaries: At facilities that are at a jurisdictional boundary (e.g., county lines, state boundaries, state/federal, etc.), the group most impacted by the event should include the scenario in their scoring.

- **RULE 10. Road Intersections:** For transportation, consider intersections as portions of the road segment. The intersections may be the worst-case location for event scenarios.
- **RULE 11. Non-Profit Agencies or Government Agencies:** For groups that do not make a profit (for example, non-profit or government agencies), use the normal operating income (equaling normal outgoing expenses) as the amount of income lost for the period of the time the facility is disabled.
- **RULE 12. Campus Facilities:** Buildings grouped as a campus, such as colleges or a zoo, should be considered a single entire facility. Complete the questionnaire as one facility for these cases.
- **RULE 13. Iconic/Symbolic Value:** To be considered an icon or regional symbol, consider the following: “Does the facility make a similar impression to people in regions outside of the Portland/Vancouver area?” Icons promote tourism. Icons are a place where people go to feel connected to other people (such as Pioneer Square) or to remember the past (such as the Vietnam and Holocaust memorials and Fort Vancouver). Icons create landscapes (such as Crown Point, St John’s Bridge, the “Big Pink” building). Icons are historic buildings and worldwide headquarters such as Nike. Icons can also be services people come to expect.

3.3 Responses

A total of 375 asset infrastructure questionnaires were received and scored out of a total of 777 critical infrastructure assets (and asset questionnaires) identified within the Portland/Vancouver Urban Area, approximately 48 percent. As shown in Exhibit 3-6, the sectors with the greatest number of identified assets are Water/Wastewater with 229, Emergency Services with 152, and Transportation with 121. The sectors with the highest response percentage are Dams, Defense, Monuments and Icons and Postal/Shipping with 100 percent, followed by Energy with 83 percent, Emergency Services with 61 percent, and Government Facilities with 52 percent.

EXHIBIT 3-6
Number of Facilities by Sector

Sector	Number of Scored Facilities	Total Number of Identified Facilities	Response Percentage
Broadcast Media	7	24	29%
Commercial Facilities	0	2	0%
Dams	4	4	100%
Defense	1	1	100%
Emergency Services	93	152	61%
Energy	43	52	83%
Food and Agriculture	1	2	50%
Government Facilities	40	77	52%

EXHIBIT 3-6
Number of Facilities by Sector

Sector	Number of Scored Facilities	Total Number of Identified Facilities	Response Percentage
Healthcare	4	16	25%
Information Technology	0	1	0%
Monuments and Icons	1	1	100%
Postal/Shipping	9	9	100%
Public Institutions	2	7	29%
Telecom	40	79	51%
Transportation	31	121	26%
Water/Wastewater	99	229	43%
TOTAL 375		777	48%

3.4 Interdependencies Workshop

Throughout the process of evaluating the critical infrastructure, it became apparent that sector interdependencies played a key role in establishing the overall importance of the infrastructure to the region. To explore more fully the interdependencies between sectors, an Interdependencies Workshop was proposed by the planning team and approved by the UAPOC Group.

The purpose of the Interdependencies Workshop was to identify interdependencies among the Portland/Vancouver Urban Area's critical infrastructure. Objectives of the workshop included:

- Gaining a better understanding of regional interdependencies
- Validating the CIPP prioritization process
- Developing a more global understanding of what resources are/information is in place that can be shared with others
- Exploring sector capabilities and methods of operations with other sectors

The Interdependencies Workshop was held October 10 and 11, 2006. The workshop included a presentation by Brandon Hardenbrook of PNWER and Vicki VanZandt of BPA introducing the concept of interdependencies and describing actions that their respective organizations were taking for critical infrastructure protection and security.

A series of six situational emergency scenarios affecting several infrastructures were discussed in a table-top exercise setting. The scenarios included the loss of telecommunications, loss of fuel supply, loss of power, loss of hospital facilities, loss of bridges, and loss of water supply. Questions explored included:

- How does this event directly impact your sector?
- How will impacts to other sectors affect you (secondary and tertiary impacts)?
- What will you need from others?
- What assistance/services/resources/personnel can you provide to others?

3.4.1 Event Scenarios

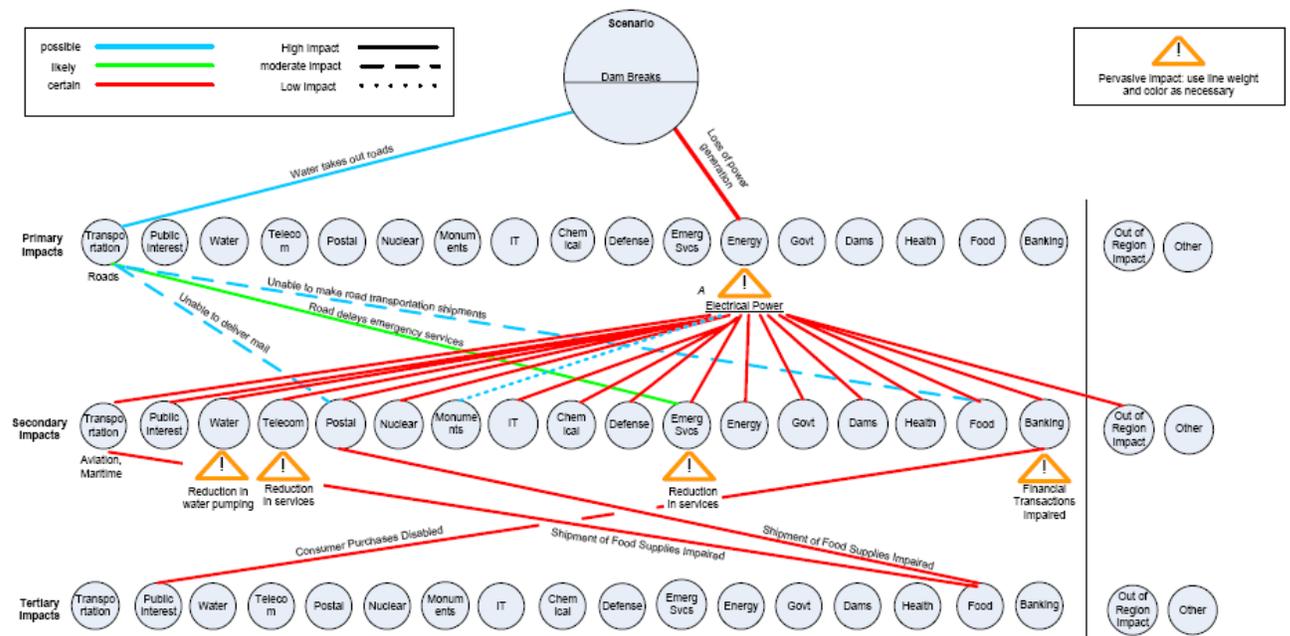
The six scenarios explored within the Workshop were:

- Scenario 1 – Electrical Substation Attack: Strategically targeted electrical substations across the region have been completely destroyed. Assumptions are that the time is mid-January, temperatures will be below freezing for at least two weeks, and power is unavailable to everyone in the area without a generator.
- Scenario 2 – Destruction of Fuel Transmission and Storage: A terrorist act destroys key petroleum and natural gas transmission and storage facilities in Oregon. Assumptions are that it is winter and fuel reserves are distributed by priority of use and will only last up to seven days.
- Scenario 3 – Telecommunications Attack: A terrorist attack at strategically located hubs (Verizon, Qwest, Comcast, etc.) has disabled all telecommunications throughout the region. Assumptions are that cellular, dial-up, and Internet access are not available. Satellite, 450 and 800 MHz, broadcast media, and non-cellular two-way radio systems are still available in the region.
- Scenario 4 – Destruction of Transportation Infrastructure: Simultaneous explosions have destroyed the Interstate and Glenn Jackson bridges and the railroad bridge over the Columbia River. In Portland, explosions destroyed the Steel Bridge and Highway 26 tunnel. Further south, the Boone Bridge was destroyed by another explosion.
- Scenario 5 – Terrorist Attack against Health Services: Several large explosions take place at healthcare facilities within the region. OHSU’s Markham Hill campus, OHSU’s riverfront facility, St. Vincent Hospital, Emanuel Hospital, and the Southwest Washington Medical Center are contaminated with anthrax. Almost three thousand people were killed in the attacks. The terrorists claiming responsibility for the attacks have threatened further attacks on the healthcare system. A number of units of blood products appear to be have been tampered with. Assumptions include that equipment, facilities, and people are contaminated. There has been contamination of inpatient and outpatient care centers. Provision of direct patient care throughout the region is sporadic and very limited.
- Scenario 6 – Destruction of Water Resources: An attack was carried out against the Portland, Oregon metropolitan area’s water supply. Explosions have completely destroyed the Tualatin River, Clackamas River, and Willamette River intake facilities. The terrorists have also targeted and destroyed the Powell Butte transmission facility and Bull Run transmission pipes. Finally, the terrorists bombed key pump houses, area wells, and aquifer storage facilities. Assumptions are that it is late summer, the river water levels are low, and there are wildfires in the area.

Sector Interdependency Diagrams were created to show how an impact on one sector affects other sectors. Refer to Exhibit 3-7 for an example Sector Interdependency Diagram. The large circle at the top of the diagram represents the identified scenario, in this case a dam break. The rows of smaller circles represent the seventeen sectors that could experience primary, secondary or tertiary impacts due to the scenario occurrence (dam break). For example, the solid red line from the dam break scenario circle runs to the energy sector primary impact circle. This represents a certain high severity primary impact to the energy sector (loss of energy). A solid blue line from the dam break scenario circle runs to the transportation sector primary impact circle, indicating a possible high severity primary impact to the transportation sector (washed out roads). This method of representing sector interdependencies is one of the unique developments of the Portland/Vancouver Urban Area CIP.

EXHIBIT 3-7

Sector Interdependency Diagram Example – Dam Break Scenario



3.4.2 Workshop Outcomes

Throughout the workshop, it was apparent that the participants expressed great interest in the process and results of the interdependency exercises. A few of the observations and results from the workshop include:

- **Electrical sector impacts all other sectors.** Electrical power plays a very important role in the operation for all other sectors. Without electrical power, every other sector will see some degradation of service. In most cases, the degradation is critical.

- **Transportation plays a critical role.** Transportation plays a very critical role, perhaps more than originally thought before the workshop. Without transportation, other sectors are impacted due to delays in shipping, deliveries, cash flow, utility resupply, etc.
- **Hospitals are important, but system redundancy exists.** During the Healthcare exercise, it was found that the healthcare system is important, but due to the amount of redundancy in the healthcare network, other hospitals and healthcare resources from other regions can be used to make up a shortfall.
- **Water supply is critical and the region has critical nodes.** Within the region, the water supply system has critical nodes. If these nodes are simultaneously impacted, then water supply to the entire region can be affected. While the nodes may be repaired or replaced, this delay could impact the area for several days.
- **Telecommunications are critical.** Telecommunications have critical nodes within the region. Some of these nodes are used by two or three very large telecommunication provider agencies. If these nodes are disabled, all cell phone service in the region is impacted. Repair of these nodes will take time, due to the amount of physical cabling required at these locations. This issue was not known by most workshop participants until identified within the exercise.

3.4.3 Workshop Results and Affect on Prioritization Scoring Process

Using the information from the Interdependency Workshop, there were a few results that could be derived and applied to the critical infrastructure ranking. The expected ranking of critical infrastructure based on observations and “gut-feel” opinions made during the Interdependency Workshop is as follows:

- Electrical infrastructure - critical electrical power control stations, main substations.
- Primary transportation routes - main bridges, roads.
- Airport
- Telecommunications facilities
- 911 facilities

The prioritization results based on the scores from the questionnaires do not always correlate with these expected results. For example, primary transportation routes such as roads and bridges do not appear at the top of the prioritized list. This may be due to the lack of road and bridge scores received.

3.4.4 Interdependencies Workshop Summary Report

The full results of the Interdependencies Workshop have been published separately within Appendix E.

3.5 Prioritization Scoring Results

For purposes of confidentiality, the results of the prioritization scoring process are not included in this document. They are identified in a separate document provided to the UAPOC Group, but a few general results can be shared:

- Utilities broadly serving the entire Portland/Vancouver Area tend to be ranked highest.
- Utilities providing electrical, telecommunications, or water infrastructure tend to be ranked highest.
- Transportation infrastructure that plays a major role in shipping and transport of goods, emergency services or general transportation within the Portland/Vancouver Urban Area was highly ranked.

4 Protection Recommendations

4.1 Introduction

A number of reference documents were reviewed to develop a set of sector protection recommendations. The 17 critical infrastructure/key resource sectors are:

1. Agriculture and Food
2. Banking/Finance
3. Chemical
4. Commercial Facilities (e.g., Shopping Centers, etc.)
5. Dams
6. Defense Industrial Base
7. Emergency Services (e.g., Police, Fire, Ambulance)
8. Energy
9. Government Facilities
10. Healthcare
11. Information Technology
12. Monuments/Icons (e.g., Statue of Liberty)
13. Nuclear Facilities
14. Postal/Shipping
15. Telecommunications
16. Transportation Systems (e.g., Roads, Bridges, Airports, Seaports, Trains, Mass Transit)
17. Water/Wastewater

The following tables identify a set of protection recommendations. The source documents for these recommendations are published in a separate appendix to this plan. The following are grouped by sector, and are identified as institutional, fiscal or technical recommendations:

- Institutional Recommendations – Recommendations that identify organizational changes, policy improvements, or changes in procedures that affect security.
- Fiscal Recommendations – Recommendations that identify or develop funding sources for increasing security measures.
- Technical Recommendations – Recommendations that develop physical or electronic security improvements, such as improving locks, fencing, or security barriers, or adding closed-circuit television (CCTV) cameras, card readers, or intrusion detection systems.

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Agriculture and Food			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Develop analytical methods for detecting bioterrorist agents in food products.	✓		
Increase number of lab technicians and laboratories with the ability to diagnose and treat animal disease outbreaks and crop contamination.		✓	
Increase state budgets for inspection, detection, and training protocols.		✓	
Track the movement of animals and commodities in transit.	✓	✓	
Incorporate procedures from completed studies on accidental outbreaks of animal disease into procedures for intentional acts.	✓		
Source Reference: USDA Guidelines			
Assess facility for potential sabotage of bulk ingredients. Ensure connections to bulk systems are locked and secured.			✓
Restrict movement of non-employees to areas where they could contaminate food products or agricultural commodities.	✓		
Close and secure entrances and gates when not in use.			✓
Lock and seal all equipment parked at facilities.			✓
Maintain well lit facilities.			✓
Routinely review, update, and exercise emergency response plan and procedures.	✓		
Establish contact with local law enforcement offices to identify specific contact personnel.	✓		
Train employees and managers to make logical connections between observed indicators and specific company operations that may signal an imminent act.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Transportation of agricultural and food commodities should include procedures for attaching trackable seals on trailers.	✓		✓
Evaluate supply chains for animal feed, animal products, seed, fertilizer, and other materials for security procedures improvements.	✓		✓
Develop a comprehensive program for the prevention and detection of contamination, including farms, food processing plants, and distribution chains such as transportation, food stores, and restaurants.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Banking/Finance			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Develop a program utilizing outcome and output of security measures to evaluate the effectiveness of security enhancements.	✓		
Evaluate the results of security controls that have been implemented. Validate whether security controls are effective.	✓		
CCTV systems in banks should be updated so recorded images have sufficient detail to help law enforcement identify suspects.			✓
Generally, security requirements for the banking/finance sector depend on the type of institution and the regulator requirements, e.g., credit union business continuity or information security will be considerably different from large national or global banking institutions.	✓		
Identify and assess the risk of the institution's dependency on electronic networks and telecommunications services.	✓		✓
Ensure that backup files and systems and security of personnel are accounted for.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Chemical			
Source Reference: American Chemistry Council “Responsible Care Security Code of Management Practices”			
Implement a risk-based security management system for people, property, products, and processes.	✓		
Evaluate, respond to, report, and communicate security threats as appropriate.		✓	
Sustain a consistent and reliable security program over time. Document the key elements of the program.	✓	✓	
Share effective security practices with others throughout the industry while maintaining interaction with law enforcement agencies.	✓		
Conduct periodic assessments of the security program, including assessment of programs and processes of chemical suppliers and vendors.	✓		✓
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Conduct a vulnerability assessment of chemical facilities that maintain large quantities of hazardous chemicals in close proximity to population centers.	✓	✓	
Hold employees accountable for security goals and objectives.	✓		
Evaluate the results of security controls that have been implemented. Validate whether security controls are effective in protecting the organization’s assets.	✓	✓	
Create a system that controls the unwanted distribution or misuse of chemicals as weapons, particularly toxic substances such as pesticides and explosives, or components of explosives, such as some fertilizers.	✓		✓
Install fencing and gates to restrict access to a facility or critical asset.			✓
Limit access to facilities to authorized personnel.			✓
Install access control measures to identify and process all personnel, contractors, vendors, and visitors.		✓	✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Provide alarm systems to control entry into control rooms.			✓
Provide perimeter alarm systems to monitor unauthorized intrusion into the facility.			✓
Install recorded CCTV systems to provide local or remote surveillance of the facility and critical assets.		✓	✓
Establish roving security patrols or fixed station security staffing.	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Public Institutions/Commercial Assets			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Establish a security plan for each homeland security threat level.	✓		
Assess and mitigate specific facility vulnerabilities.	✓	✓	
Integrate considerations for potential threats into the engineering design of the facility and supporting systems.		✓	✓
Conduct an interior assessment of HVAC systems and their components.			✓
Develop and rehearse facility contingency plans based on worst-case physical security breaches.	✓		
Evaluate the results of security controls that have been implemented. Validate whether security controls are effective in protecting the organization's assets.	✓		
Review federal building protection standards and practices, including vulnerability and risk assessment methodologies and technology solutions, such as physical barriers, CCTV, etc.	✓		
Implement stringent screening requirements for employees, contractors, and visitors.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Dams			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Perform a vulnerability assessment for each structure.	✓		
Develop protective action plans.	✓		
Establish a comprehensive and fully funded dam safety program.		✓	
Hold employees accountable for security goals and objectives.	✓		
Develop methods for monitoring access to the dam site by visitors, employees, contractors, etc.	✓		✓
Develop information and warning structures for dams during heightened alert levels.	✓		
Identify the areas downstream from critical dams that could be affected by dam failure and develop appropriate population and infrastructure protection and emergency action plans.	✓	✓	
Evaluate technology solutions to identify and mitigate waterborne threats.		✓	✓
Provide fencing and gates to restrict access to the dam.			✓
Limit access to facilities to authorized personnel.			✓
Implement access control measures to identify and process all personnel, contractors, vendors, and visitors.			✓
Install alarm systems to control entry into control rooms.		✓	✓
Provide perimeter alarm systems to monitor unauthorized intrusion into the facility.		✓	✓
Install recorded CCTV systems to provide local or remote surveillance of the facility and critical assets.		✓	✓
Establish roving security patrols or fixed station security staffing.	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Defense Base			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Review vendors' critical infrastructure protection practices.	✓		
Implement enhanced infrastructure protection measures per federal mandates of private industry.		✓	
Integrate infrastructure of private industry and DoD to meet Department of Defense initiatives.		✓	
Include critical infrastructure protection of private industry plants in contracts with DoD.	✓		
Implement security initiatives into private sector production and distribution process.	✓		
Share security-related information between defense organizations and private sector providers.	✓		✓
Evaluate the results of security controls that have been implemented. Validate whether security controls are effective in protecting the organization's assets.	✓		✓
Ensure security, storage, and transport of military goods and personnel.		✓	

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Emergency Services (Police, Fire, Ambulance)			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Share Information between different emergency services and organizations, particularly in the event of an attack.	✓		
Develop capability to respond to a large-scale terrorist attack.	✓	✓	
Develop communication systems sized adequately for a national emergency.		✓	
Ensure protection of first responders and critical resources during emergency response operations.	✓		
Implement local and regional preparedness exercises providing experience and feedback to local officials.	✓		
Adopt interoperable emergency communications system for first responders.		✓	
Develop redundant emergency response networks to improve communications during emergencies.		✓	
Enhance and strengthen mutual aid agreements between local jurisdictions.		✓	
Develop processes to screen non-federal tenants and visitors entering private sector facilities that house federal or local state government organizations.	✓		
Develop long-term construction standards for facilities requiring blast resistance or other specialized security measures.	✓		
Develop measures to enhance security in the common areas of federal or state government facilities.			✓
Evaluate forms of identification of employees and contractors to adhere to Homeland Security Presidential Directive 12 (HSPD12).	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Emergency Services (Police, Fire, Ambulance)			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Ensure alarms, CCTV, and other security systems report to the facility or central command center for evaluation of alarm condition and dispatch of appropriate response.		✓	✓
Provide vehicle barriers and projectile barriers, where appropriate.	✓		✓
Evaluate lighting levels at facilities to ensure adequacy.			✓
Prioritize critical facilities and assets.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Energy			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Provide redundancy and increase generating capacity to provide greater reliability.		✓	
Develop strategies for locating and distributing replacement parts in an emergency event.	✓		
Develop strategies to reduce vulnerabilities of critical components.	✓		
Prioritize critical facilities and assets.	✓		
Provide fencing and gates to restrict access to the facility or critical asset.			✓
Limit access to facilities to authorized personnel.			✓
Establish access control measures to identify and process all personnel, contractors, vendors, and visitors.			✓
Install alarm systems to control entry into control rooms.			✓
Establish perimeter alarm systems to monitor unauthorized intrusion into the facility.			✓
Install recorded CCTV systems to provide local or remote surveillance of the facility and critical assets.			✓
Implement roving security patrols or fixed station security staffing.			✓
Implement alarms, CCTV, and other security systems reporting to the facility or a central command center for evaluation of alarm condition and dispatch of appropriate response.	✓		
Provide vehicle barriers and projectile barriers, where appropriate.			✓
Evaluate lighting levels at facilities to ensure adequacy.			✓
Evaluate cyber access control for monitoring and auditing capabilities.	✓		
Hold employees accountable for security goals and objectives.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Create security assessment program for power plants, substations, transmission lines, and interruption of fuel supplies.	✓	✓	
Develop evaluation of system restoration and recovery after attack.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Government Facilities			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Develop processes to screen non-federal tenants and visitors entering private sector facilities that house federal or local state government organizations.	✓		
Develop long-term construction standards for facilities requiring blast resistance or other specialized security measures.	✓		
Develop measures to enhance security in the common areas of federal or state government facilities.			✓
Evaluate forms of identification of employees and contractors to adhere to Homeland Security Presidential Directive 12 (HSPD12).	✓		✓
Ensure alarms, CCTV, and other security systems report to the facility or central command center for evaluation of alarm condition and dispatch of appropriate response.		✓	✓
Provide vehicle barriers and projectile barriers, where appropriate.	✓		✓
Evaluate lighting levels at facilities to ensure adequacy.			✓
Prioritize critical facilities and assets.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Healthcare			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Review mission critical operations, establish protection priorities, and ensure adequate security and redundancy for critical laboratory facilities and services.	✓		
Enhance the protection of emergency stockpiles of medical supplies and pharmaceutical manufacturing facilities.		✓	✓
Examine legal and regulatory incentives to increase investment in the physical security of facilities.		✓	
Develop communication strategy and plan to handle large numbers of contaminated or ill people, including isolation of patients and protection of health workers.	✓	✓	
Implement a system for protecting and decentralizing needed medical and drug supplies.	✓		
Limit access to laboratories and other critical facilities to authorized personnel.			✓
Prioritize critical facilities and assets.	✓		
Evaluate lighting levels at facilities to ensure adequacy.	✓		
Develop measures to enhance security in the common areas of medical facilities.	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Information Technology			
Source Reference: National Infrastructure Protection Plan			
Evaluate system interconnections (direct connection of two or more cyber systems owned by separate organizations).	✓		
Prioritize cyber assets, systems, networks, and the functions they provide by evaluating cyber threats, vulnerabilities, and consequences.	✓	✓	
Measure the consequences of cyber asset, system, or network destruction using a consistent system to ensure results can be compared across sectors.	✓		
Protect information with anti-virus software and firewalls. Combine these technologies with good security habits to reduce risk.			✓
Source Reference: NRIC Topic Addendum – Integrated Network and Facility Monitoring Systems for Telecommunications			
Alarm and continuously monitor all means of facility access (e.g. perimeter doors, windows) to detect intrusion or unsecured access (e.g. doors being propped open.)	✓		✓
Establish corporate standards and practices to drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks associated with administering and servicing multiple platforms.	✓		✓
Consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.	✓		✓
Service providers, network operators and equipment suppliers should adopt a comprehensive physical security plan and design that focuses on providing an integrated approach that seamlessly incorporates diverse layers of security (e.g., access control and appropriate life safety systems, CCTV and recording, sensor technology, administrative procedures, personnel policy and procedures and audit trails).	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points to include monitoring and recording for incident analysis. Where appropriate, consider providing near-real-time remote monitoring and archiving.	✓		✓
Source Reference: USDA – Physical Security Standards for Information Technology Res tricted Space			
Control facility parking, post signs, make arrangements for towing of unauthorized vehicles; provide adequate lighting for parking areas.	✓		✓
Control facility by armed security guards and an intrusion detection system with central monitoring capability maintained to current life safety standards.	✓		✓
Require all personnel to have and display ID at all times; control and screen all visitors.	✓		✓
Conduct annual security awareness training.	✓		✓
Restrict utilities access to authorized personnel only. Provide emergency power to all critical systems (alarms, radio communications, computer facilities, etc.)	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Monuments/Icons			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Conduct a threat and vulnerability assessment to identify gaps in visitor protection process as well as asset protection.	✓		
Conduct security focused public outreach and awareness program.	✓		
Collaborate with state and local governments and private foundations to assure the protection of symbols and icons outside federal domain.	✓	✓	
Evaluate innovative technologies to ensure the protection of visitors to monuments and other like attractions.	✓		
Make provisions for extra security during high-profile events taking place in or around national or regional icons.	✓	✓	
Improve site security, screening of visitors, contractors, and other workers and suppliers.	✓		✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Nuclear Facilities			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Develop a standard methodology for conducting vulnerability and risk assessments for nuclear power plants.	✓		
Establish common process and identify resources needed to enhance security at nuclear power plants.	✓	✓	
Develop a standard process for requesting external security augmentation at nuclear power plants during heightened periods of alert and in the event of an imminent threat.	✓		✓
Pursue state and federal legislation to criminalize the carrying of unauthorized weapons or explosives into nuclear facilities.	✓	✓	
Enhance the capabilities of nuclear power plant security forces.		✓	✓
Develop standards and implement additional training in counter-terrorist techniques for private security forces.	✓	✓	
Advocate legislation to make federal prohibitions on sabotage applicable to nuclear facilities and their operations.	✓		
Enhance public outreach and awareness programs and emergency preparedness programs.		✓	
Source Reference: GAO Nuclear Security – Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environmental Sites.			
Set standards for individual protective force officers to participate in training exercises simulating attacks by a group of mock terrorists.	✓		
Ensure dependable radio communications as required by DOE Manual 473.2-2, Protective Force Program Manual.			✓
Transform current protective force into an 'elite force', modeled on US Special Forces.	✓		✓
Develop and deploy new security technologies.		✓	✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Consolidate and eliminate nuclear weapons material between and among sites.	✓		
Create a sound Energy, Science and Environment (ESE) management structure that has sufficient authority to ensure coordination across all ESE offices that have Category I special nuclear material.	✓		
Source Reference: Project on Government Oversight – Nuclear Power Plant Security: Voices from Inside the Fences. (Dated October 2, 2002).			
Significantly upgrade the Design Basis Threat (DBT).	✓		
Create a prioritized target/assets list. Immediately include spent fuel pools on that list as a primary target.	✓		
Apply "Fatigue Rule" to security guards.	✓		
Require a two-man rule in vital areas to reduce the risk of "insider."	✓		✓
Provide no more than two to three weeks notice prior to force-on-force tests.	✓		
Guards to be tested in force-on-force scenarios should not be told of the scenarios in advance.	✓		
Include outside responders as participants in the mock attacks with realistic timelines for arriving at the plant.	✓		
NRC should require utilities to hire security directors with a background in physical security.	✓		
NRC should give their security forces pay and benefits (health care coverage, retirement) commensurate with those accorded to onsite fire departments and local police.	✓	✓	

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Postal/Shipping			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Increase reserve stockpiles of equipment and materials needed for emergency-incident response, particularly for CBR (Chemical, Biological, or Radiological) contaminants.	✓		✓
Conduct enhanced risk analysis of key facilities. Risk analysis should take into account terrorist capabilities and motivations, and facility vulnerabilities.	✓	✓	
Improve customer identification and correlation mechanisms at designated mail intake points and improve passive, nonintrusive parcel inspections for the detection of hazardous materials.	✓	✓	
Evaluate and address conflicts in federal, state, and local laws and regulations that impair the abilities of multi-jurisdictional entities to respond effectively in emergency situations.	✓		
Raise the level of physical security and protection regarding the safety and well being of employees, contractors, suppliers, and others that live near or have access to sites and facilities.		✓	✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Telecom			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Implement a security assessment program for telecommunications centers, transmission towers, and relay towers.	✓		
Evaluate capability to provide alternate telecommunication routing through the existing telecommunication architecture.	✓		
Identify critical intersections among various infrastructures. Develop strategies that better address security and reliability.	✓	✓	
Conduct vulnerability assessments within facilities where different types of equipment and multiple carriers are concentrated.	✓		✓
Limit access to facilities to authorized personnel.			✓
Install access control measures to identify and process all personnel, contractors, vendors, and visitors.			✓
Provide alarm systems to control entry into control rooms.			✓
Provide perimeter alarm systems to monitor unauthorized intrusion into the facility.			✓
Establish recorded CCTV systems to provide local or remote surveillance of the facility and critical assets.			✓
Provide roving security patrols or fixed station security staffing.			✓
Source Reference: NRIC Topic Addendum – Integrated Network and Facility Monitoring Systems for Telecommunications			
Alarm and continuously monitor all means of facility access (e.g. perimeter doors, windows) to detect intrusion or unsecured access (e.g. doors being propped open.)			✓
Establish corporate standards and practices to drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks associated with administering and servicing multiple platforms.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.	✓		✓
Service providers, network operators and equipment suppliers should adopt a comprehensive physical security plan and design that focuses on providing an integrated approach that seamlessly incorporates diverse layers of security (e.g., access control and appropriate life safety systems, CCTV and recording, sensor technology, administrative procedures, personnel policy and procedures and audit trails).	✓		✓
Conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points to include monitoring and recording for incident analysis. Where appropriate, consider providing near-real-time remote monitoring and archiving.	✓		✓
Establish access control procedures that: 1) Confirm identity of individuals, 2) Confirm authorization to access facility, and 3) Create record of access (e.g., written log, access control system log).	✓		✓
Include security as an integral part of the facility construction process to ensure that security risks are proactively identified and appropriate solutions are included in the design of the facility (e.g., facility location selection, security system design, configuration of lobby, location of mailroom, compartmentalization of loading docks, design of parking setbacks).	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Transportation			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Develop improved decision making policies for rail transportation of hazardous materials.	✓		
Develop technologies and procedures to screen rail cars and passenger baggage.		✓	
Devise or enable a railroad hazardous materials identification system that supports the needs of first responders.	✓	✓	
Harden transportation infrastructure against terrorism through technology.			✓
Create and maintain a driver/operator security education and awareness program.	✓		
Identify, clarify, and establish authorities and procedures as needed to bring pipelines and facilities back on line as quickly as possible after a disruption of service.	✓		
Improve and upgrade response and recovery plans for pipelines.	✓	✓	✓
Facilitate security assessments to identify vulnerabilities and interdependencies for ports.	✓		
Develop plan for implementing security measures corresponding to various threat levels.	✓		✓
Establish security plans to minimize security risks at ports, vessels, and other critical maritime facilities.	✓	✓	✓
Develop a template for improving physical and operational port security.	✓		
Study and develop appropriate guidelines and technology requirements for the security of cargo and passenger ships.	✓		
Improve security of waterways, such as developing electronic monitoring systems for water traffic.			✓
Conduct comparison modeling of shipping systems to identify and protect critical components.	✓		

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Identify requirements and procedures for periodic waterway patrols.	✓	✓	
Develop appropriate guidelines to protect mass transit.	✓		
Develop design and engineering standards for facilities, and rail and bus vehicles.	✓	✓	
Develop an overall protective architecture for mass transit systems.	✓		
Develop models for integrating priorities and emergency response plans in the context of interdependencies between mass transit and other critical infrastructure.	✓	✓	

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
SECTOR: Water/Wastewater			
Source Reference: The National Strategy For The Protection of Critical Infrastructure and Key Assets			
Identify high-priority vulnerabilities and improve site security. Assessment should include loss of controls, or sabotage of information management systems that control water treatment.	✓		✓
Identify processes and technologies to better secure key points of storage and distribution, such as dams, pumping stations, chemical storage facilities, and treatment plants.		✓	✓
Improve analytic capabilities to improve detection of contaminants in water systems.		✓	✓
Partner with other local water agencies to enhance information exchange and coordinate contingency planning.	✓		
Create cross-sector working groups to develop models for integrating priorities and emergency response plans for interdependencies between the water sector and other critical infrastructure.	✓		
Provide fencing and gates to restrict access to the facility or critical asset.			✓
Limit access to facilities to authorized personnel.			✓
Establish access control measures to identify and process all personnel, contractors, vendors, and visitors.			✓
Install alarm systems to control entry into control rooms.			✓
Implement perimeter alarm systems to monitor unauthorized intrusion into the facility.			✓
Install recorded CCTV systems to provide local or remote surveillance of the facility and critical assets.			✓
Establish roving security patrols or fixed station security staffing.			✓

Security Measure	Institutional Recommendations	Fiscal Recommendations	Technical Recommendations
	(Organizational policies, procedures)	(Developing funding sources for increasing security measures)	(Developing physical and electronic security improvements)
Ensure that alarms, CCTV, and other security systems report to the facility or a central command center for evaluation of alarm condition and dispatch appropriate response.			✓
Provide vehicle barriers and projectile barriers, where appropriate.			✓
Evaluate lighting levels at facilities to ensure adequacy.	✓		✓
Evaluate cyber access control for monitoring and auditing capabilities.	✓		✓
Hold employees accountable for security goals and objectives.	✓		✓
Improve analytic capabilities to detect contaminants in water systems.		✓	

5 Future Actions

5.1 Introduction

The Critical Infrastructure Protection Plan development process yielded several positive results.

First, a definition of critical infrastructure for the region was established. Thresholds for each sector and sub-sector were adopted with the consensus of plan development participants.

Next, a methodology for assessing critical infrastructure was developed and was used to score and prioritize the critical infrastructure assets. A total of 375 critical infrastructure assets of an identified 777 assets within the urban area were scored and prioritized.

Finally, an infrastructure interdependencies workshop was conducted for regionally critical infrastructure owners/operators. The workshop enhanced the understanding of interdependencies and their importance to infrastructure planning.

5.2 Problems Encountered

The CIPP project was very ambitious. It broke new ground in identifying and prioritizing critical assets within a region. As far as can be determined, this effort is the best attempt in development of a comprehensive method to identify, categorize, and prioritize assets thus far.

Gaps in the plan are described below.

5.2.1 Inventory and Participation

Participation in the project was voluntary, resulting in some sectors having gaps. For example, the Banking, Healthcare, Food/Agriculture, and state and federal government facilities sectors were poorly represented. As a result, the information received and the asset inventory for these sectors is incomplete.

Similarly, the inventory received for the CIPP was provided by the participants, meaning that if a significant entity chose not to participate, their assets would not necessarily be included in the plan. Fortunately, most of the major regional entities chose to participate, but some larger private entities did not. As a result, their assets are not included in the plan.

5.2.2 Scoring Consistency

Inconsistent prioritization scores arose due to the complexity of the scoring system and the use of different scorers in the process.

The scoring system was somewhat complex, as a necessary result of incorporating interdependency impacts. This resulted in inconsistent scores; some groups accurately

scored the interdependencies, and others chose to ignore or gloss over the interdependency scores, resulting in inaccurate scoring.

Different scorers were used in the process. All asset owners/representatives were asked to score their assets. This resulted in inconsistent scores for similar assets in some cases.

5.3 Follow-on Recommendations

Suggestions for continuing the progress of this effort are described below.

5.3.1 Continue Obtaining Completed Questionnaires

Continue efforts to obtain completed questionnaires to close gaps within certain sectors. Some sectors did not seem to understand the goals and desired outcomes from the plan, and did not fully participate in the questionnaire process. Directed outreach to key sectors would be beneficial to gain their participation. Notable sectors that did not turn in questionnaires were:

- Transportation
- Healthcare
- Banking and Finance

5.3.2 Normalize Questionnaire Scoring

Review and correct scoring results that appear too high or too low relative to similar assets. Some groups have unusually high (or low) scores. This may be caused by variations in the understanding of the respondents in filling out the questionnaires, particularly in the interdependency section of the questionnaire. Questionable high scores were noted for one telecom central office, one dam, and several levees. Questionable low scores were noted for several aviation and maritime facilities.

5.3.3 Establish Consistent Interdependency Scores

Meet with key sectors to establish consistent interdependency scores. Educate their representatives about the interdependency portion of the questionnaire. A better understanding should minimize significant variances in the scores. Notable sectors that could benefit from having additional support for interdependency scoring were:

- Water/Wastewater
- Telecom

5.3.4 Begin Vulnerability Assessment Process

Begin conducting vulnerability assessments to identify security issues and vulnerabilities for the high-priority assets identified during this study.

5.3.5 Information Exchange

Provide or develop an appropriate vehicle or system for infrastructure owners/operators to exchange and share information. There is a high degree of interest among the participants in receiving and exchanging information. A secure, user friendly and cost-effective method to exchange and share security-related information would be very beneficial.

5.3.6 Statewide Plans

Encourage and support the development of statewide plans (Oregon and Washington) to ensure the states priorities for critical infrastructure protection work in concert with the Portland/Vancouver Urban Area plan.

APPENDIX A - Participating Organizations

EXHIBIT A-1
List of Participating Organizations

Organization	Sector	Phone
Bonneville Power Administration	Energy	503-230-5148
British Petroleum	Energy	360-371-1500
City of Boring Water	Water—Wastewater	503-806-7132
City of Gresham Wastewater	Water—Wastewater	503-618-2539
City of Portland Water Bureau	Water—Wastewater	503 823-7474
City of Portland Wastewater (BES)	Water—Wastewater	503-823-2494
City of Tigard	Government Facilities	503-784-7789
Clackamas County Transportation	Transportation	503-650-3647
Clark County Information Technology	Information Technology	360-816-2251
Clark County Regional Emergency Services Agency (CRESA)	Emergency Services	
Clean Water Services	Water—Wastewater	503-681-3626
Columbia County	Transportation	503-366-3963
Convention Center	Commercial Assets	503-731-7901
Department of Homeland Security	All	503-250-2815
Federal Reserve	Banking & Finance	503-276-2901
Joint Water Commission (JWC)	Water—Wastewater	503-681-6158
Kinder Morgan Energy Partners	Energy	503-220-1257
KPTV (Meredith)	Commercial Assets	
KXL Rose City Radio	Commercial Assets	
Multnomah County Drainage District	Dams	
Multnomah County Facilities	Government Facilities	503-849-3436
Multnomah County Health Department	Healthcare & Public Health	
NW Natural	Energy	
Oregon Department of Agriculture	Agriculture & Food	503-986-4727
Oregon Department of Energy	Energy	503-378-2856
Oregon Department of Transportation	Transportation	

Organization	Sector	Phone
Oregon Public Utility Commission	Energy	503-378-6631
PacifiCorp	Energy	503-618-6338
PNWER	All	
Port of Portland (Aviation & Marine)	Transportation	503-460-4116
Portland Center for the Performing Arts	Commercial Assets	
Portland Department of Transportation	Transportation	503-823-1789
Portland Fire	Emergency Services	503-823-3049
Portland General Electric (PGE)	Energy	503-742-8289
Portland Office of Emergency Management	All	
Portland Parks	Government Facilities	503-823-5478
Portland Police	Emergency Services	
Portland State University	Commercial Assets	503-781-4430
Postal Service, Portland District	Postal & Shipping	503-279-2075
Qwest	Telecom	503-242-8290
Railway (HDR)	Transportation	503-423-3728
Safeway	Agriculture & Food	503-657-6314
TriMet	Transportation	503-962-4982
Tualatin Valley Fire & Rescue	Emergency Services	
Tualatin Valley Fire & Rescue	Emergency Services	503-642-0399
U.S. Air Force Reserve	Defense Industrial Base	
U.S. Army Corps of Engineers	Dams	503-808-4441
U.S. Coast Guard	Defense Industrial Base	
U.S. Department of Transportation	Transportation	503587-4709
United Parcel Service (UPS)	Postal & Shipping	503-978-7242
Verizon	Telecom	503-614-0982
Washington County - Facilities	Government Facilities	503-846-4869
Washington County - Transportation	Transportation	503-846-7653
Washington County - Emergency Management	All	
Washington County - Telecommunications	Telecom	503-846-8097
Washington State Department of Transportation	Transportation	360-905-2260

APPENDIX B - Grant Programs

DHS Grants Program

In 2006, \$399 million was available for a series of related infrastructure protection grants. These grant programs included:

Port Security Grant Program

More than \$168 million was provided for port security grants to create sustainable, risk-based efforts for the protection of critical port infrastructure from terrorism. The Nation's 100 most critical seaports (plus an additional seaport eligible in 2005), representing 95 percent of the foreign waterborne commerce of the United States, were eligible to participate in the port grant program.

Transit Security Grant Program

Transit security grants were funded at more than \$136 million for the owners and operators of the nation's critical transit infrastructure, including rail, intracity bus and ferry systems. Eligibility for funding was limited to those who provide services within a defined Urban Areas Security Initiative (UASI) jurisdiction. A priority for this grant was the protection of underground operations from improvised explosive devices.

Intercity Bus Security Grant Program

Approximately \$9.5 million was provided to eligible owners and operators of fixed route intercity and charter bus services to protect bus systems and the traveling public from terrorism. Program priorities included facility, driver and vehicle security enhancements; emergency communications technology; coordination with local police and emergency responders; training and exercises; and passenger and baggage screening programs in defined UASI service areas.

Intercity Passenger Rail Security Grant Program

Amtrak was awarded more than \$7.2 million to continue security enhancements for intercity passenger rail operations in the Northeast Corridor (service between Washington, D.C. and Boston), Amtrak's hub in Chicago, and the West Coast service area in key, high-risk urban areas.

Trucking Security Program

The American Trucking Association received \$4.8 million for the Highway Watch program to continue to enhance security and overall preparedness of the nation's highways. The grant priorities of the Trucking Security Program included identifying and recruiting participants; ensuring that the Highway Watch Program address homeland security and safety issues in conjunction with the National Preparedness Goal; and maintaining a full-time Highway Watch Call Center.

Buffer Zone Protection Program Grants

The Buffer Zone Protection Program provided grant funding to build security and risk-management capabilities to secure critical infrastructure including chemical facilities, nuclear and electric power plants, dams, stadiums, arenas, and other high-risk areas. In

fiscal year 2006, this program awarded approximately \$48 million in grant funds to state and local authorities.

Chemical Sector Buffer Zone Protection Grant Program

The Chemical Sector Buffer Zone Protection Grant Program was a targeted effort that provided funds to build security and risk-management capabilities at the state and local level for chemical sector critical infrastructure to protect against acts of terror and other hazards. In fiscal year 2006, the Chemical Buffer Zone Protection Program received \$25 million.

For each grant, the DHS Preparedness Directorate relied on an integrated team of subject matter experts drawn from both DHS operating components and sector-specific departments to develop, design, compete, review, and support the infrastructure grants as part of the national preparedness effort

APPENDIX C - Scoring Results

[THESE SHEETS REMOVED FOR CONFIDENTIALITY PURPOSES]

APPENDIX D - Protection Recommendation Source Documents

[PUBLISHED SEPARATELY]

APPENDIX E - Interdependencies Workshop Summary Report

[PUBLISHED SEPARATELY]