Washington State
Homeland Security Region 6

Critical Infrastructure Protection Plan

September 2005

THIS PAGE INTENTIONALLY BLANK

CIP Plan Benefits

Washington State Homeland Security Region 6 (geographic King County) developed this plan to assist owners and operators (both private and public sector) and regional government representatives in protecting the Region's critical infrastructures—an objective necessary to securing the economic and social well being of the Region's citizens. This plan describes a *voluntary* system for sharing information on vital infrastructures to assist with critical infrastructure protection (CIP) decision-making. The processes and methodologies listed in this Plan will bring together partners who have a common goal of ensuring that the Region's way of life is not undermined by failures in infrastructure.

If You Are an Infrastructure Owner or Operator

Region 6 government entities understand that owners and operators of critical assets must provide the first line of defense for their own facilities and systems. Owners and operators routinely carry out risk management activities and invest in protective measures as a necessary business function. This plan is not intended to tell owners and operators how to conduct these regular business activities. Rather, it is intended to put these activities into a common framework and language to allow the entire critical infrastructure protection community to share information and understand interdependencies between sectors. As a result, this framework will encourage a collaborative approach for developing and implementing smart protective measures.

This plan will help owners and operators to:

- Connect with other owners and operators in their sector to share best practices and identify the most critical assets within their sector.
- Provide information on initiatives and tools that may assist with assessing vulnerabilities.
- Understand their dependencies on other infrastructure sectors and then connect them with other sectors to identify and protect cross-sector assets that are considered most vital.
- Identify ways that regional government agencies can assist owners and operators with protecting their critical infrastructures.

The Region 6 Homeland Security Council (R6 HSC)/Emergency Management Advisory Committee (EMAC) and its subgroup, the Regional Homeland Security Subcommittee (RHSS), is not mandating the sharing of specific asset or vulnerability data with it, unless owner/operators are specifically requesting resources from the Region. Under this Plan, the sharing of asset information remains a voluntary option for owners and operators who need additional assistance in addressing vulnerabilities.

If You Are a Regional Government Entity

This plan will help regional government entities to better coordinate with infrastructure owners and operators by establishing communication networks and increasing their understanding of owner/operator needs. It will also allow them to effectively prioritize and allocate resources for regional CIP.

THIS PAGE INTENTIONALLY BLANK

Executive Summary

Washington State Homeland Security Region 6 (geographic King County) has developed this Critical Infrastructure Protection (CIP) plan to protect critical assets that are vital to the current way of life in the Region. This Plan presents approaches to ensure there are adequate priorities, communications, methods, and resources to protect these vital assets from all hazards (natural, accidental, and human-caused).

Owners and operators will find this plan useful in helping to connect with other critical infrastructure owners and operators and regional government entities that can assist them with protecting their assets. The Plan defines the processes for ensuring that decision-makers, owner/operators, and governmental entities have the information necessary to make judgments about protection.

This plan addresses processes and methodologies to protect and mitigate the impacts on critical infrastructures *prior to an incident*. This Plan is not a response plan; thus, it does not address how owners and operators or emergency responders should respond to an incident or bring the critical infrastructure back on line after an incident.

As part of an initial planning effort, this Plan focuses on the six most critical sectors: Energy, Information Technology, Telecommunications, Water and Wastewater, Transportation, and Healthcare Systems. Future efforts may incorporate the eleven other critical infrastructure sectors.

This plan is designed to work in conjunction with other national, state, and local efforts. It often incorporates tools and initiatives that are being used by the U.S. Department of Homeland Security that are applicable to the Region.

Region 6 governmental entities expect that infrastructure owners and operators will continue their critical infrastructure protection efforts already underway and invites them to participate in the Critical Infrastructure Protection Work Group as well as sector specific information sharing networks already in existence. These networks allow owners and operators and regional governmental entities to share best practices, understand sector and cross-sector needs, and inform collective decision-making on how best to utilize resources.

Annually, the CIP Work Group will coordinate a CIP cross-sector interdependency forum to bring together owners and operators of different sectors to discuss and resolve cross-sector interdependency issues as well as develop a consensus on regional CIP priorities.

The Region 6 Homeland Security Council (R6 HSC) through its subgroup, the Regional Homeland Security Subcommittee (RHSS), may assist public and private sector owners and operators in providing funding for infrastructure protection, using Homeland Security grant funding. The RHSS is not mandating that owner/operators share specific asset or vulnerability data with it, unless the owner/operator is specifically requesting funds or resources from the Region.

The CIP Work Group's mission is to identify critical infrastructure in the Region, establish priorities, and provide appropriate resources to protect those assets. The CIP Work Group will coordinate with other Homeland Security Regions to assist owner/operators in effectively securing critical infrastructures that cross jurisdictional boundaries. Additionally, it will act as a facilitator and information coordinator. The CIP Work Group will facilitate information coordination by:

- Notifying owner/operators through the Interdependency Forums, or other information sharing bodies of changes in national, state, or local policy related to CIP.
- Informing owner/operators of grant and funding opportunities and notify them of deadlines, procedures, and submission requirements.
- Communicating progress towards or awards related to CIP grants and funding with owner/operators.

In some circumstances owners and operators may identify vulnerabilities that they are unable to address. In these cases, the Region 6 CIP Work Group may be able to provide assistance, either in the form of funding or equipment, or aid with coordinating systemic improvements or protective measures. If an owner/operator is requesting specific resources from the government via the CIP Work Group, they will need to provide additional asset information so that the CIP Work Group may make allocation decisions within its understanding of regional CIP priorities. The CIP Work Group will take into consideration the criticality of the infrastructure by weighing the negative consequences of disruption or failure of the asset. It will also look at the expected probability of success of the protective measure in eliminating or reducing the vulnerability prior to making funding and resource decisions. The owner/operator of the asset will have to provide the information needed for the CIP Work Group to make its assessment and funding decisions.

In summary, this plan focuses on the protection of regional critical infrastructures. It describes priorities, initiatives, methodologies, and tools that can help owners and operators of these assets work collaboratively with regional governmental entities to protect the Region's way of life, economic and social well being, and ensure their own internal, organizational security and continuity goals.

The Region 6 Homeland Security Council, the Regional Homeland Security Subcommittee and its work groups are supported by the King County Office of Emergency Management (OEM). For more information on these groups or to engage in this CIP program, visit the OEM website at www.metrokc.gov/prepare or contact:

King County Office of Emergency Management
3511 NE Second Street
Renton, WA 98056-4192
206-296-3830

Table of Contents

CIP Plan Benefits i
Executive Summary iii
Table of Contents v

1 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 3
1.3 Background and Current Status 5
1.3.1 National CIP Efforts and Drivers 5
1.3.2 State Efforts 5
1.3.3 Regional Efforts – Region 6 HSSP 6
1.3.4 Relationship of this Plan to Other CIP Efforts 6
1.4 CIP Plan Review and Revision 8

2 RISK MANAGEMENT PROCESSES 9
2.1 Identify Critical Assets 11
2.2 Assess Risk 13
2.2.1 Challenges in Critical Infrastructure Risk Analysis 14
2.3 Prioritize Assets 15
2.4 Implement Protective Programs 15
2.5 Assess Effectiveness 16

3 ROLES AND RESPONSIBILITIES 19
3.1 Region 6 CIP Decision-Making Entities 20
3.1.1 Region 6 Homeland Security Council (R6 HSC) 20
3.1.2 Regional Homeland Security Subcommittee 20
3.1.3 Critical Infrastructure Protection Work Group 20
3.2 Local, State, and Federal Governments 21
3.3 Associations 22
3.4 Owner/Operators 23
3.4.1 Vulnerability Reduction and Asset Protection 23
3.4.2 Threat-Initiated Response 23
3.4.3 Information Sharing and Coordination 28
3.4.4 Leadership 29

4 INFORMATION SHARING AND COORDINATION 31
4.1 Background 31
4.1.1 Sharing Threat Information 32
4.2 Sector-Specific Information Sharing Networks 33
4.2.1 Energy Sector 33
4.2.2 Information Technology & Telecommunications Sectors 33
4.2.3 Water and Wastewater Sector 34
4.2.4 Transportation Sector 35
4.2.5 Healthcare Systems Sector 36

4.2.6 Voluntary Status Reporting 37
4.3 Interdependency Forum 37
4.3.1 Logistics of the Forum 38
4.3.2 Confidentiality of Interdependency Forums 38
4.4 Critical Infrastructure Protection Work Group 39
4.4.1 CIP Work Group Membership 39
4.4.2 CIP Work Group Information Dissemination 39
4.4.3 Cross-Regional Coordination 39
4.4.4 Confidentiality of CIP Work Group Meetings 40
4.5 Requesting Resources From Region 6 40
4.6 Information Security 42

5 DECISION MAKING PROCESS 45
5.1 Cross-sector Analyses & Resource Prioritization 45
5.1.1 Consideration of Hazards 45
5.1.2 Consequence Analysis 46
5.1.3 Protective Measure Review 47
5.1.4 Resource Allocation Priorities 47
5.2 Implications of Funding Options on the Decision-Making Process 48
5.2.1 U.S. Department of Homeland Security Grant Programs 49
5.2.2 Funding the Private Sector 51

Appendix 1: Energy Sector 53
Appendix 2: Information Technology Sector 57
Appendix 3: Telecommunications Sector 59
Appendix 4: Water and Wastewater Sector 61
Appendix 5: Transportation Sector 63
Appendix 6: Healthcare Systems Sector 67
Appendix 7: Public Disclosure Exemptions 71
Appendix 8: Acronyms 73

Attachment A: Non-Disclosure & Confidentiality Agreement 77
Attachment B: Owner/Operator CIP Checklist 81

1 INTRODUCTION

1.1 PURPOSE

This document presents the Washington State Homeland Security Region 6 Plan for protecting critical infrastructure across the Region (geographic King County). Critical infrastructure sectors, which include basic systems and functions such as energy, transportation, and telecommunications, provide the foundation for the Region's economy, governance, and security. The purpose of developing this Plan is to protect those regional assets that are vital to the current way of life and well-being (both economic and social) from all hazards (natural hazards, terrorist attack, or human-caused accidents). This plan presents approaches for ensuring that there are adequate communications, methods, and resources to protect against the failure of these critical assets and services.

Target Audiences

This plan is meant for different audiences in Region 6. The primary audience is the *owner/operators* of critical assets, whether they are private companies or public entities. Such owner/operators represent the first line of defense in critical infrastructure protection (CIP). Specifically, this Plan is intended to help owner/operators to:

- Work with other owner/operators in their own sector to identify the most critical assets within that sector;
- Understand their own supply needs (and the vulnerabilities of those supplies) as well as the impacts they have on their users;
- Work with other critical infrastructure sectors to identify those assets across sectors that are considered to be most vital in the Region;
- Identify opportunities for working with other owner/operators and Regional governmental agencies to ensure that the most critical assets are protected.

This Plan is for:
- ❒ Asset Owners and Operators
- ❒ Region 6 Decision-Makers
- ❒ Users of Critical Infrastructure

This Plan is also intended to serve as a *decision-making tool* to support Regional CIP strategies and funding considerations. It defines the processes for ensuring that the decision-makers have the necessary information to make judgments about protection. It also lays out the roles, responsibilities, and activities that need to be carried out at the Regional level to identify, prioritize, and protect critical infrastructures and assets, and provides the structure in which these activities will occur. In general, these CIP decision-makers are the three governmental entities responsible for homeland security and emergency management related planning and execution in geographic King County: (1) the Region 6 Homeland Security Council (R6 HSC)/Emergency Management Advisory Committee (EMAC), (2) the Regional Homeland Security Subcommittee (RHSS), and (3) the Critical Infrastructure Protection Work Group (CIP Work Group). More details on their specific roles and responsibilities are provided in Chapter 3. However, throughout this Plan, the term "Region 6" will be used to generally represent the interests and responsibilities of these three entities. The

Region 6 Homeland Security Council, the Region 6 Homeland Security Subcommittee and its workgroups are supported by the King County Office of Emergency Management (OEM) - phone: 206-296-3830; Address: 3511 NE Second Street, Renton, WA 98056-4192.

Finally, this Plan can be used by other public, private, and non-profit entities that rely on certain critical assets for their own functioning. This includes government and private sector entities from other Homeland Security Regions whose infrastructures are interdependent with those in Region 6.

Plan Structure

In addition to this introduction, this Plan has five main chapters, as follows:

- **Chapter 2, Risk Management Processes**—presents an overall framework and suggestions for specific processes that owner/operators can use to identify critical assets, assess risk, prioritize infrastructure data, and initiate protective measures.
- **Chapter 3, Roles and Responsibilities**—lays out the current and expected roles and responsibilities for private and public sector owner/operators, as well as governmental stakeholders whose mission it is to protect the region.
- **Chapter 4, Information Sharing and Coordination**—describes the process for sharing information and coordinating CIP efforts within and across sectors and with governmental entities.
- **Chapter 5, Decision Making Process**—presents the process that the Region 6 Critical Infrastructure Protection Work Group will use to determine priorities and allocate CIP resources.

This document also contains appendices and attachments that elaborate on the processes described in the Plan, as well as additional, specific information that may be of interest to certain stakeholders.

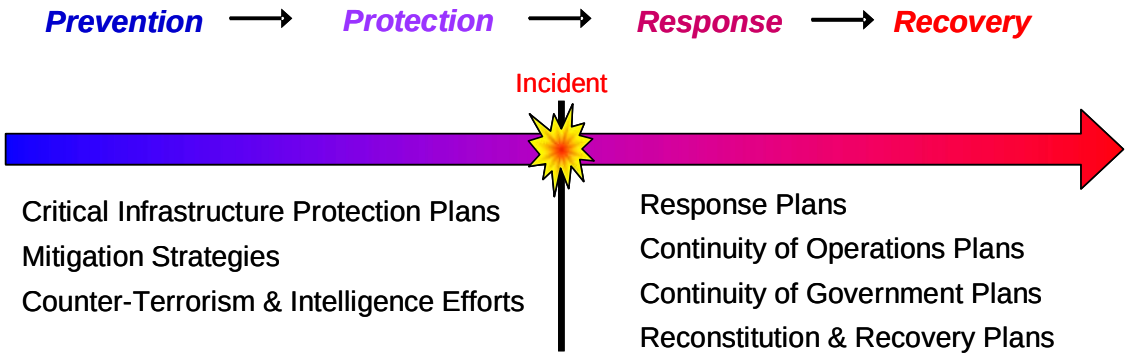
- The first six Appendices provide quick reference guides for the Tier 1 Sectors – Energy, Information Technology, Telecommunications, Water and Wastewater, Transportation, and Healthcare Systems.
- Appendix 7 summarizes the public disclosure exemptions for CI information under Washington State and Federal law.
- Appendix 8 contains the list of acronyms used in this Plan.
- Attachment A contains a non-disclosure agreement that will be used by CIP stakeholders to ensure confidentiality.
- Attachment B provides a checklist for owner/operators to guide and ensure the comprehensiveness of their CIP activities.

A Prevention/Protection Strategic Document

This Plan is not a response plan. Its overall goal is to ensure that critical infrastructure assets are protected, prior to any event that may affect them, in an effort to lessen any effects from a natural or human caused hazard or prevent human caused hazards in the first place. It does not, therefore, address how to respond when such assets are attacked, or how to bring them back on line. Nevertheless, the outcomes of this protection planning process may help to inform first responders and other stakeholders in Region 6 in developing such response and recovery plans. Exhibit 1 illustrates how this CIP Plan relates to other emergency management and homeland security plans.

This Plan is also not intended for use in response to real-time threat information. As a strategic prevention and protection plan, it is designed to achieve the long-term vulnerability reduction of the Region's most critical infrastructures without knowledge of specific threats. Tactical protective activities are the responsibility of a variety of law enforcement and intelligence organizations. Tactical protection is a significant component of CIP and this Plan references its importance and recommends some strategies for implementing protective measures and for sharing threat information. However, those sections are for informative and reference purposes only. This Region 6 Plan proposes an overall threat-neutral approach to CIP.

Exhibit 1: Application of Emergency Management Plans



1.2 Scope

This Plan focuses on protection of regional critical infrastructure. The definition of "infrastructure" or the specific "assets" that comprise the infrastructure may vary from sector to sector. Developed from the framework of the national CIP program, the CIP Work Group has identified 17 separate sectors of infrastructure, which are divided into the following tiers:

TIER 1	Energy[1], Information Technology, Telecommunications, Water and Wastewater, Transportation, Healthcare Systems [Emergency Medical Services (EMS), Advanced Life Support (ALS), Hospitals, Public Health, Laboratories]
TIER 2	Government Facilities, Banking and Finance, Agriculture, Food, Defense Industrial Base, Postal, Shipping
TIER 3	Icons and Monuments, Chemical Industry, Emergency Services, Commercial Facilities

[1] Energy includes electrical, nuclear, gas, oil, and dams.

For this Plan, the RHSS surveyed 51 key stakeholders to prioritize critical infrastructure sectors. Based on the results of that survey, the RHSS decided to focus its efforts in this first iteration on developing a plan for the top six interdependent critical infrastructure sectors: energy, information technology, telecommunications, water and wastewater, transportation, and healthcare systems. As resources become available, the Plan may be expanded to address the other infrastructure sectors based on each sectors tiered prioritization shown above. As this process evolves, it should be understood that Region 6 does not have the responsibility or resources to address each infrastructure. Federal and State authorities have responsibility to protect selected sub-infrastructures such as Postal and Shipping, Government Facilities, Agriculture, and Food. As this plan develops, Region 6 will identify what infrastructures it can and cannot address.

In general, it is understood that assets are considered to be something of importance or value and can include one or more of the following types of elements:

- Physical – The more typical understanding of assets is tangible property, such as buildings, facilities, components, real estate, animals, and products.
- Human – In addition to the physical components, assets can include the employees, visitors, and customers to be protected and the personnel who may present an insider threat (e.g., due to privileged access to control systems, operations, sensitive areas, and information).
- Cyber – Cyber components include the information hardware, software, data, and networks that serve the functioning and operation of the asset.

In addition, assets may include intangibles, such as brand names, images, and knowledge (e.g., about the asset or the business).

Definitions:

Critical Infrastructure: "…those 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." *[Source: USA PATRIOT Act of 2001]*

Key Assets: individual targets "…whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige and confidence." *[Source: "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" (February 2003)]*

In general, Region 6 is focusing on those critical infrastructures and assets that would have an impact on the current way of life in the Region if the asset were disrupted or destroyed. Specific consequences that will be considered are discussed in Chapter 2.1.

1.3 Background and Current Status

This Section provides some background on how CIP is being addressed at both the Federal level and more locally within Washington State and its regions, counties, and cities. This information may be helpful in providing context for this Plan.

1.3.1 National CIP Efforts and Drivers

The national CIP program, which is led by the Department of Homeland Security (DHS), is a sector-based system for protecting critical infrastructure through a risk-management process. Although the Federal government has been carrying out CIP efforts for years, the need for infrastructure protection was formally stated in the Homeland Security Act of 2002.

In December 2003, the President issued Homeland Security Presidential Directive (HSPD)-7 on "Critical Infrastructure Identification, Prioritization, and Protection." This Directive required DHS to develop a national plan to frame the activities of the national CIP effort. HSPD-7 also lists the specific Federal departments and agencies that are responsible for protection activities in 17 critical infrastructure or key resource sectors.

In response to HSPD-7, DHS released an interim version of the National Infrastructure Protection Plan (NIPP) in February 2005. The Interim NIPP provides the framework and sets the direction for implementing a coordinated national CIP effort. It provides a roadmap for identifying critical assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures within and across infrastructure sectors. It also delineates roles and responsibilities among Federal, State, local, tribal, and private sector stakeholders in carrying out these activities. DHS expects to release the Final NIPP in November 2005.

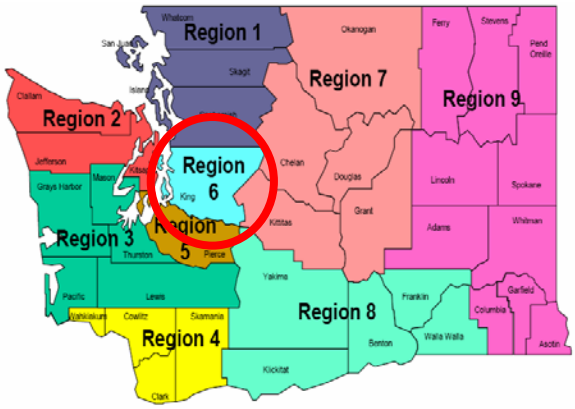
The NIPP applies a risk management framework that promotes application of risk reduction and protection measures where they offer the most benefit.

1.3.2 State Efforts

Washington State is in the process of developing a State CIP program. Under this program, the State intends to establish standardized sector criteria to identify and prioritize infrastructures within the State. The criteria will be based upon a risk management framework that takes into account vulnerability, threat, and consequence. The State will use data collected under this program in concert with threat data to determine overall consequences and risks. Information developed under this program will be maintained in a CI database that the State intends to develop. The database will include geospatial information, an acknowledgement as to whether threat and vulnerability assessments have been executed at the facility (as provided by the owner/ operator), and qualitative assessments to assist with resource allocation decision-making. The State will eventually prioritize asset data using a risk management model. Based upon that prioritization, the State will begin implementing protective actions in 2006.

1.3.3 Regional Efforts – Region 6 HSSP

Within Homeland Security Region 6 of the State (geographic King County), the RHSS developed a Homeland Security Strategic Plan (HSSP) that serves as a primary reference for focusing homeland security efforts in the area. The Region 6 HSSP lists a series of action strategies (objectives) designed "…to protect the citizens, property, environment, culture and economy of Region 6 from acts of terrorism and natural disasters and to minimize the effects of these emergencies." One of the high priority objectives listed in the Region 6 HSSP is the development of a Region 6 CIP plan.



This plan and its subsequent elements are but one part of the Region's overall homeland security strategy as laid out in the Region 6 HSSP. The Region 6 HSSP is the strategic document that guides this CIP Plan. This CIP Plan is the first step toward accomplishing the Region 6 HSSP requirement of assessing regional assets, needs, threats and vulnerabilities from a critical infrastructure perspective.

This CIP Plan has been designed to execute most of the action strategies listed in the HSSP in accordance with the Region's guiding principles:

- A Regional Approach with Broad Participation
- Planning, Coordination, Clear Roles and Responsibilities
- Unifying Standards and Protocols
- Assessment- and Strategy-Based Funding

1.3.4 Relationship of this Plan to Other CIP Efforts

This Plan is designed to assist the Region in protecting regional critical infrastructure by providing priorities, methodologies, and processes that infrastructure stakeholders can use to protect assets within their sectors, as well as address interdependencies between sectors. This Plan will support the efforts of both the national CIP program and the Washington State CIP program. The Region 6 CIP Plan is not intended to supplant other CIP efforts. The processes and methodologies listed in this Plan will bring together partners who have a common goal of maintaining the Region's way of life.

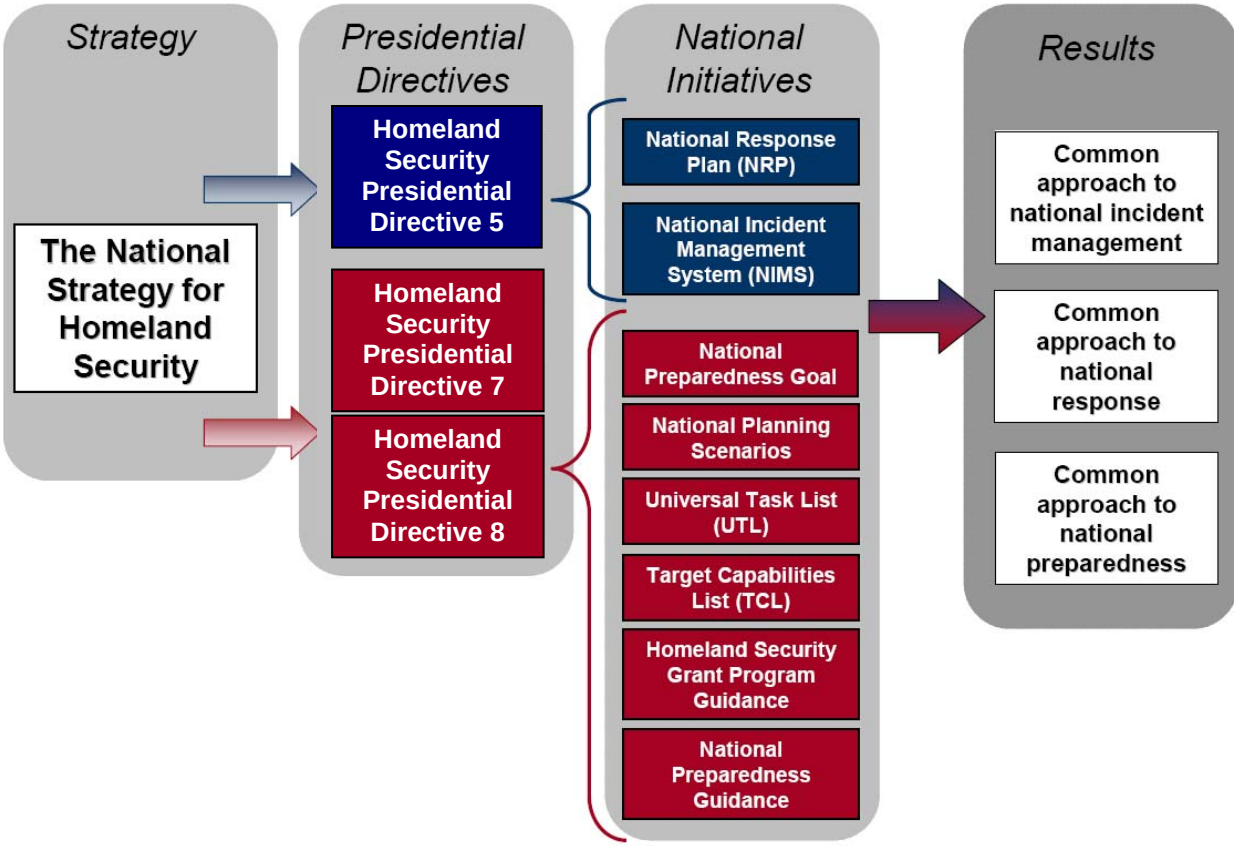
No single plan can address the entire spectrum of threats and vulnerabilities facing each sector at a national, state, regional, or local level. However, the programs that result from this Plan will establish a good foundation for reducing overall vulnerabilities and improving protection capabilities by providing public and private sector decision-makers with common structures to address CIP.

The regional, State, and national CIP efforts described above are part of the nation's overall homeland security effort. To help ensure that the Nation is prepared to prevent, respond to, and recover from threatened and actual domestic terrorist attacks and other emergencies, the President issued HSPD-8 "National Preparedness" in December 2003. As a part of that effort, DHS has established a National Preparedness goal, which includes seven national priorities:

- Expanded Regional Collaboration;
- National Incident Management System (NIMS) and National Response Plan (NRP) Implementation;
- National Infrastructure Protection Plan (NIPP) Implementation;
- Strengthen Information Sharing and Collaboration Capabilities;
- Strengthen Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Detection and Decontamination capabilities;
- Strengthen Interoperable Communications Capabilities; and
- Strengthen Medical Surge and Mass Prophylaxis Capabilities.

Region 6, through this CIP Plan, will contribute to the success of this nationwide effort by supporting the implementation of the NIPP and the National CIP Program. Byproducts of the Region 6 CIP effort will likely support the National Preparedness Goal by indirectly expanding CBRNE detection capabilities, enhancing interoperable communications, and providing sound information for response coordination. Exhibit 2 illustrates the relationship among these national homeland security efforts.

Exhibit 2: National Homeland Security Efforts



1.4 CIP Plan Review and Revision

The Region 6 CIP Plan will be reviewed by the CIP Work Group on an annual basis. The CIP Work Group will consider changes in policy, feedback from stakeholders, and evaluations of the effectiveness of CIP activities Region-wide to ensure the Plan remains applicable, functional, and valuable. Between bi-annual reviews, the Plan will be updated as needed to reflect CIP-related policy changes at the local, State, and Federal levels and also to reflect new guidance from any of those groups.

2 RISK MANAGEMENT PROCESSES

When there are limited resources available for critical infrastructure protection, decisions have to be made about the trade-offs between risks posed by the vulnerabilities of particular assets and the costs of protection. For that reason, the Region 6 CIP program is based on risk management, where the costs of protection are weighed against the reduction in risk.

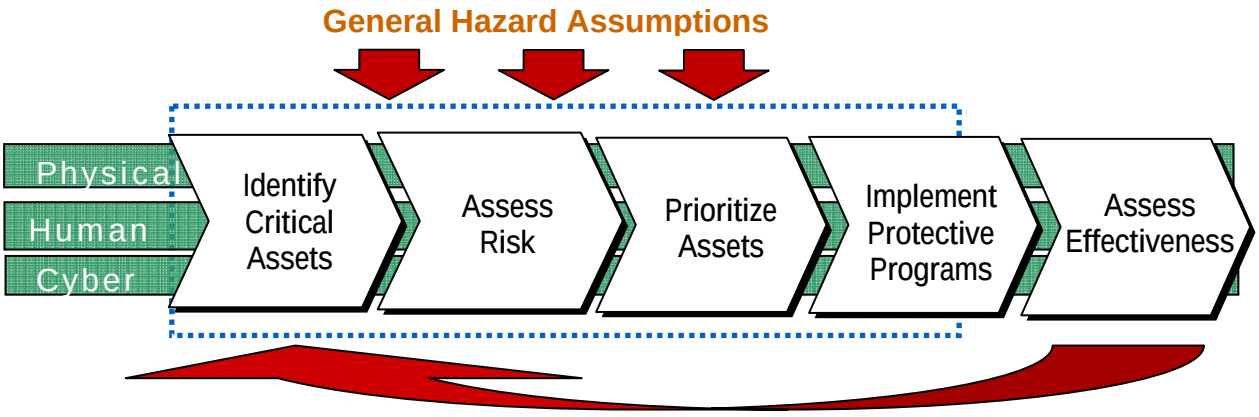
Owner/operators of critical assets, whether in the public or private sector, are responsible for providing the first line of defense for their own facilities. These owner/operators routinely perform risk management activities and invest in protective measures as a necessary business function. Thus, the purpose of this Chapter is not to tell owner/operators how to do those things they already do well, but rather to put these activities into a common framework and language. This will help facilitate information sharing and interdependency analysis across sectors.

Ultimately, the goal is to have each owner/operator maximize reduction in risk by investing in protection where there is the greatest benefit. To get to this end goal, the following general steps are recommended for owner/operators in each sector:

1. Identify critical assets
2. Assess risk
3. Prioritize assets
4. Implement protective programs
5. Assess effectiveness

Each of these activities is discussed in the sections below. Exhibit 3 illustrates the relationship of these activities to the asset's elements and the hazard environment.

Exhibit 3: Risk Management Process Steps



This strategy represents a continuous cycle that is always re-evaluating assets and enhancing protective strategies as needs change. Before delving into each step of the risk management approach, it is important to define the common terms used in this area. The key elements of most risk-based programs are vulnerability, hazard, consequence, probability, and risk, which are defined as follows:

- ***Vulnerability*** **–** the characteristics of an asset's design, location, or operation/use that make it susceptible to damage, destruction, or incapacitation by threats (e.g., terrorist acts, mechanical failures, and natural hazards). Cyber vulnerabilities may emerge as flaws in security procedures, software, or internal system controls, or the design and use of an information or communication system that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited to affect that asset/system or to allow further access to other assets/systems, as well as weaknesses that may lead to failure because of inadvertent human actions, mechanical failures, or natural disasters.

- ***Hazard –*** synonymous with threat, it is the cause of the event that disrupts systems and causes undesirable consequences. In the risk management framework, hazard assumptions should focus on the set of "plausible" threats (natural and human caused) i.e., where there is evidence that the event could happen and could cause damage to the asset in question (as opposed to the universe of all "possible" threats, most of which would be extremely unlikely to occur). The likelihood of each plausible threat actually occurring should be presumed to be equal.

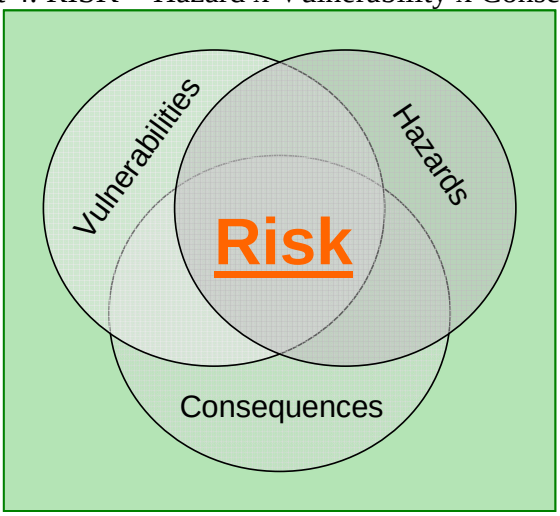
- ***Consequence –*** the negative outcomes associated with degradation or failure of an asset. Specific consequences to be considered are discussed in Section 2.1 below.

- ***Probability –*** The likelihood that a particular set of consequences will occur if the vulnerability is exploited. Probability is determined as a function of vulnerability and threat.

- ***Risk –*** the overall determination of the significance of a hazard associated with a particular event, taking into account the type of event [the threat], the vulnerability of the system or asset to such threats, and consequences (both type and severity) that may result.

Generally speaking, risk is a function of three basic inputs: Hazard, Vulnerability, and Consequence. The relationship between these concepts is illustrated in Exhibit 4.

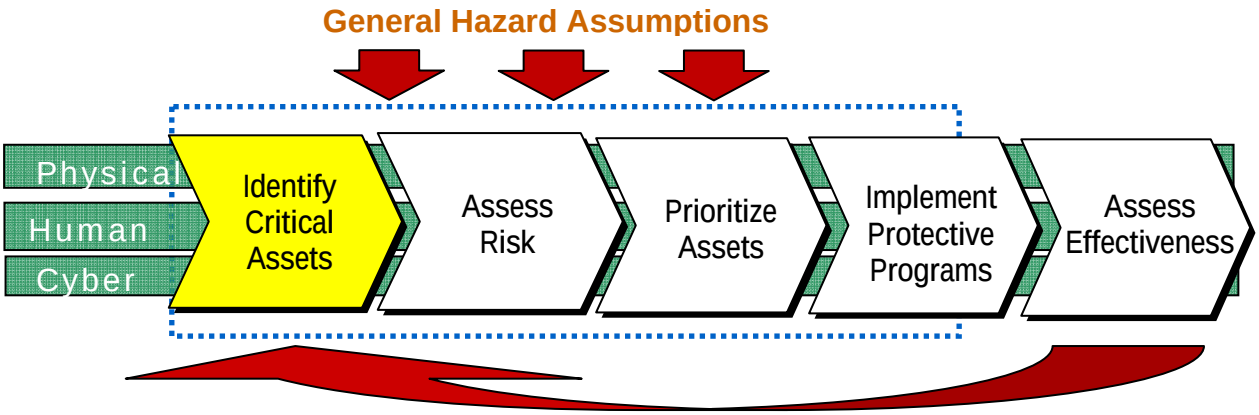
Exhibit 4: RISK = Hazard x Vulnerability x Consequence



For the most part, owner/operators in Region 6 should carry out risk assessment processes using general assumptions about hazards. That is, each owner/operator should examine the vulnerabilities of their assets, and determine the appropriate protection based on what are generally understood to be the plausible events that could affect their assets, including terrorist acts and other hazards, such as major storms, earthquakes, tsunamis, and human-caused accidents.

It is important to understand that for the purposes of the Region 6 CIP program, this model should not be used to determine responses to specific, real-time threat information about particular attacks. Actions taken in response to such explicit information will likely involve law enforcement in determining priorities and implementing protective actions that go beyond the resources of the asset owner/operator. Section 3.2.2 of this Plan describes some general recommendations for Threat-Initiated Response to be considered outside the realm of this CIP program.

2.1 Identify Critical Assets



As infrastructures are built or taken out of service, and technologies controlling these infrastructures change, owner/operators need to keep track of the universe of infrastructure assets that are critical to their everyday functioning. Therefore, the first step in the framework is to identify assets within each company, within the sector, and across sectors, including not only physical assets, but also the human resources and cyber components of various infrastructure systems.

This first step should result in a comprehensive list of critical assets for the business entity. Steps two and three in the process narrow the focus to the most significant of those assets based on the results of risk assessments that consider threat, vulnerability, and consequence. Without an awareness of all potentially critical assets it would be impossible to accurately pinpoint the greatest priorities.

The key decision in creating a list of "critical" assets is deciding what is "critical." To owner/operators of infrastructure, *critical* assets are likely to be those assets that are essential to meeting the mission objectives of the system (e.g., the asset that keeps the telecommunication

system going, the energy grid active, the transportation modes moving, etc.). This is a decision that can only be made by the asset owner/operator who has familiarity with the network and the organization's mission. The owner/operator must attempt to objectively balance what it deems "critical" versus "not critical" (e.g., essential, necessary, replaceable, invulnerable, etc.) as to not be overwhelmed by assets requiring protective attention.

The determination of an asset's "criticality" can also be based on the consequences related to the asset's disruption or destruction (i.e., the negative impacts that occur when a system is destroyed or otherwise fails). As discussed in Chapter 1, the RHSS is focusing on assets that would result in the greatest impact on the way of life in the Region if such assets were disrupted or destroyed. Some of the specific consequences that should be considered by each owner/operator include impacts on:

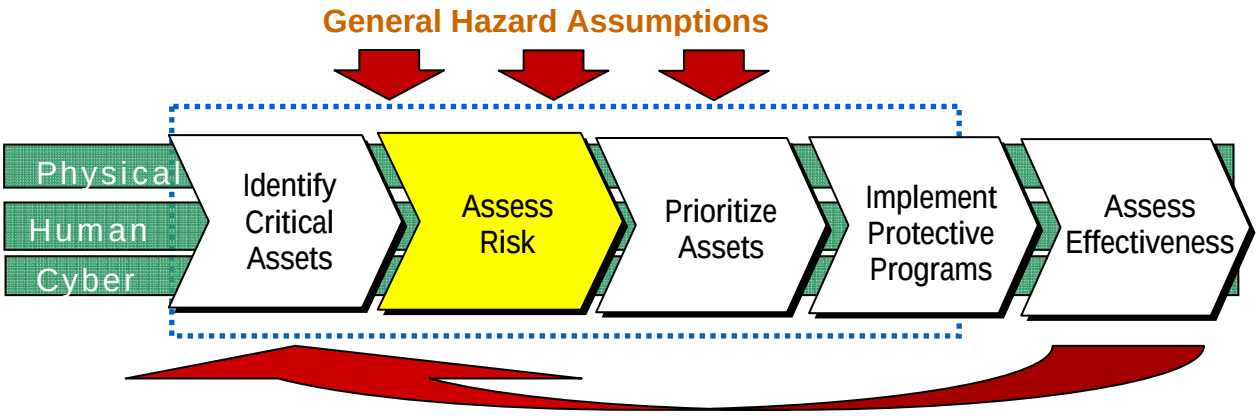
- The surrounding population – e.g., catastrophic health effects or mass casualties, or even loss in morale and public confidence.
- Public and governmental service – e.g., the inability of government agencies to perform essential missions, deliver essential public services, maintain public order, or ensure public health and safety
- The local and regional economy – e.g., due to disruption of the private sector's ability to deliver essential goods and services, or the negative impact on the economy through the cascading disruption of other critical infrastructure and key resources
- The environment – e.g., devastating impacts on local natural resources

In general, the owner/operators in each sector should have a sense of which of their facilities or components are key to operations or will result in such consequences if destroyed. For purposes of the Region 6 CIP plan, it will be important to keep track of such assets and related information, such as:

- Basic asset data (e.g., asset name, location, owner, and function)
- System components that are central to the mission and function
- Dependencies (on what the asset depends in order to function)
- Results of vulnerability analyses
- Continuity, redundancy (including backups), and resiliency built into the asset
- Existing protective actions (e.g., fencing, biometrics, firewalls, procedures, structural and non-structural mitigation, etc.)

As described later in this Plan, the RHSS anticipates that this information will be shared among the owner/operators within a sector to develop an overall understanding of critical assets and their interdependencies sector-wide. When appropriate, this information will be protected by public disclosure laws and agreements.

2.2 Assess Risk



The second major step in the risk-management process involves a set of analyses to assess the vulnerabilities of assets, and use of that data to complete an overall risk analysis. **Vulnerability Assessments** evaluate potential weaknesses of an asset that, if exploited, could result in significant consequences (as discussed above). **Risk Analysis** is a process that combines consequence information, potential hazards, and data from vulnerability assessments to create an overall picture of relative risk. Risk analysis also results in a common quantitative categorization of risk that allows assets with different consequences and vulnerabilities to be compared side by side. This risk information is used to compare assets within and across sectors to allow determination of priority (discussed in Section 2.3).

The more quantitative a risk assessment is, the less biased and more reliable it will likely be. The drawback to detailed quantitative assessments is that they are often expensive and time consuming. However, a comprehensive risk analysis may well be worth it if it results in rational decision-making that leads to tangible, effective security.

Infrastructure risk is typically addressed at one of three levels:

- Risks posed by individual assets or groups of assets
- Risks within a sector due to interdependencies among the assets in that sector
- Risks due to interdependencies across sectors and across regions or the nation

Individual owner/operators are encouraged to focus on risks for single or small sets of assets, primarily those they own. Groups of asset owner/operators within a sector can use that individually generated data to conduct the next level of analysis, which brings in interdependencies among assets and results in a sector-wide risk profile. This sector-wide risk analysis can be conducted in the sector information sharing networks described in Chapter 4. Finally, groups of owner/operators and industry associations (through the Interdependency Forums described in Chapter 4), and Region 6 (through its assessment process described in Chapter 5), can use the sector-specific analyses to review risks across sectors within the Region for a macro-level analysis of the infrastructure system.

2.2.1 Challenges in Critical Infrastructure Risk Analysis

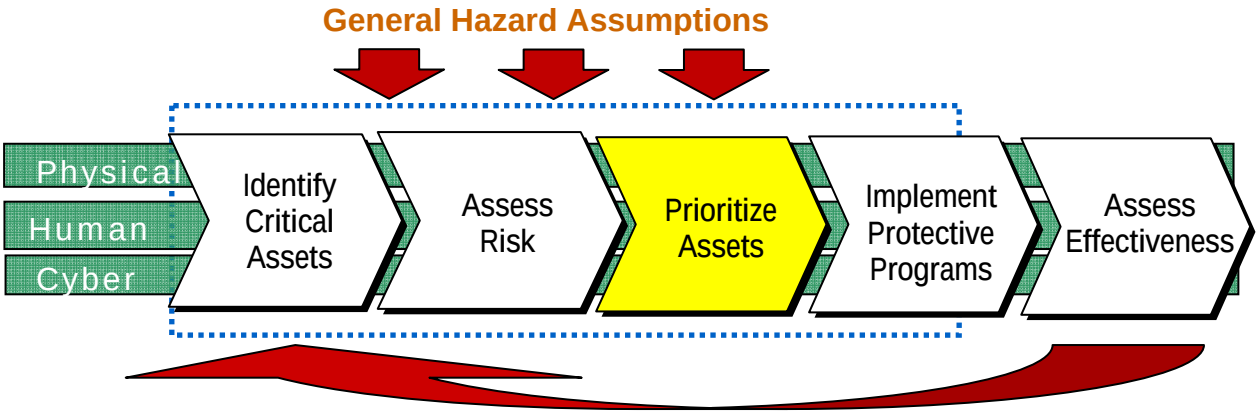
There are several obstacles to overcome in order to determine the relative risks posed by critical assets within and across sectors. The first issue is the *lack of common approach and terminology*. Currently, the private sector, which owns the majority of the country's critical assets, has been using a variety of methods to assess risk. Because these methods can vary widely in approach, it is difficult to objectively compare the relative risks across sectors – for example, comparing the risk of an attack on a nuclear power station with the loss of a bridge carrying key communications lines is difficult to quantify.

A second challenge is *determining the interdependencies among assets and sectors*, where the failure of an asset in one sector may result in cascading impacts throughout other sectors. In general, each sector tends to focus on ensuring the integrity of its own assets. But because critical infrastructures depend on each other, assuring the integrity of the larger system is complex. For example, nearly all sectors rely on the service grids of the energy, information technology, telecommunications, and transportation sectors—failures in these crucial service areas can be devastating to the proper functioning of other sectors. In some sectors, the dependency may be more localized; for example, the proper functioning of firefighters in the Emergency Services sector will be dependent on a reliable local water supply in the Water Sector. Interdependencies can also be the source for a potential exploitation—where one sector is used by a terrorist to attack other sectors. For example, terrorists may destroy a key energy distribution node as a method to attack the capability of a hospital or financial institution.

To help address these challenges, many organizations are attempting to develop a common approach that allows for cross-sector, objective analysis to assist in focusing resources. DHS, for example, has tasked the American Society of Mechanical Engineers (ASME) Innovative Technology Institute LLC, in collaboration with other industrial societies, organizations, and government agencies, to develop the *"Guidance on Risk Analysis and Management for Critical Asset Protection (RAMCAP)."* This document, which is still under review, is expected to become the standard for consistent CIP terminology and approaches to vulnerability and risk assessment, in order to allow the comparison of results from vulnerability and risk assessments on assets in different sectors.

Until this tool or others like it are finalized and tested, Region 6 recommends that each owner/operator continue to use the vulnerability and risk assessment tools to which they are accustomed. If owner/operators have not been engaged in such a process, it is recommended that they communicate with other members of their sector and reference the sector-specific vulnerability assessment tools in the Appendices of this plan, to implement a risk-based assessment program.

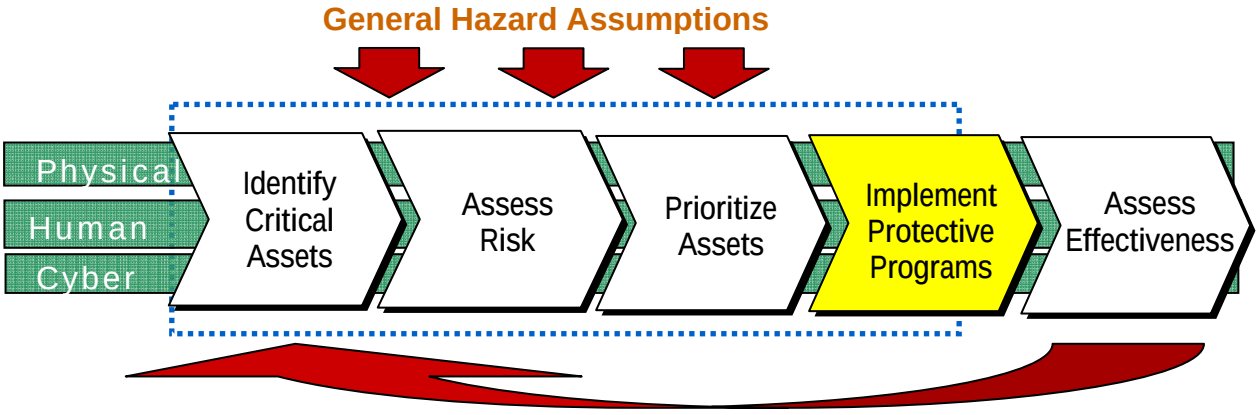
2.3 Prioritize Assets



The purpose of using common risk assessment processes is to ensure that data can be compared within and across sectors to determine which assets pose the greatest risk. This information can then be used to guide the allocation of resources for protective actions, as no business or government has enough resources to address all vulnerabilities. This allocation process should take into account the return on investment of the protective action (i.e., the overall value relative to the overall cost).

Asset owner/operators should conduct an analysis to determine which protective strategies will pose the greatest benefit through reduction in risk. Many methodologies are already being used by asset owner/operators that may be applicable to this process.

2.4 Implement Protective Programs



Using information developed in the steps above, owner/operators can make decisions regarding development and implementation of protective programs to reduce risk for the highest priority assets. A protective program is a coordinated plan of action to prevent, deter, and mitigate infrastructure failures. It is also designed to respond to, and recover from such failures in a manner that limits the consequences and value of the failure (with respect to human caused, malicious attacks). Actions to protect an asset fall into one or more of the following general categories:

- ***Deter***—Actions that cause the potential attacker to perceive that the risk of failure is prohibitive. Examples include improved awareness and security (restricted access, vehicle checkpoints), enhanced police presence, and such cyber-protection features as additional access controls.

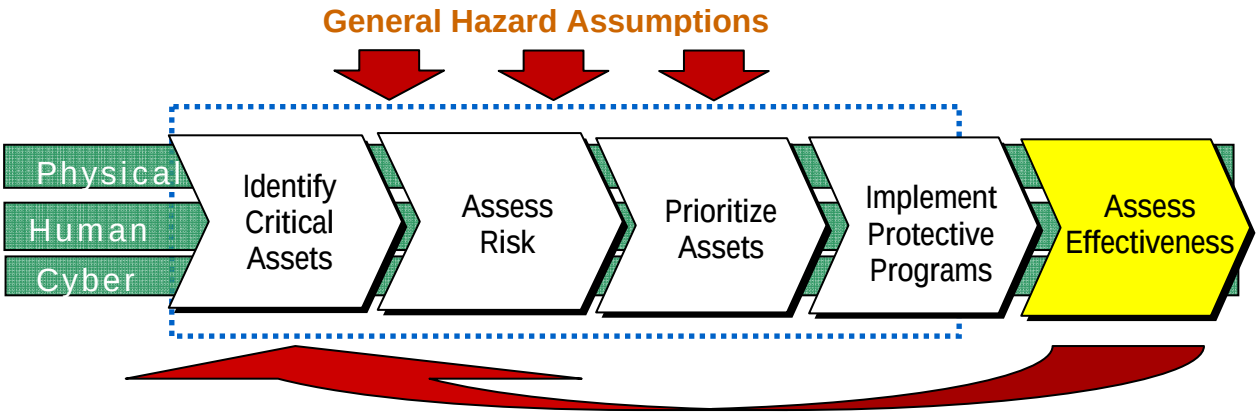
- ***Devalue***—Actions that reduce the attacker's incentive by reducing the target's value. Examples include developing redundancies and back-up systems, or de-emphasizing the importance of a particular event.

- ***Detect***—Activities or mechanisms that identify potential attacks, validate the information, and/or communicate the information as appropriate. For specific assets, examples include intrusion-detection systems, monitoring, operation alarms, surveillance detection and reporting, and employee security awareness programs. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting.

- ***Defend***—Actions that protect assets by preventing or delaying the actual attack or failure caused by another hazard (natural or human caused). These include physical hardening, buffer zones, fencing, and structural integrity.

In addition to implementing protective actions for their own assets, owner/operators may want to collaborate with organizations within and across sectors to develop Regional strategies to reduce vulnerability and prevent disruptions in service.

2.5 Assess Effectiveness



Once owner/operators have implemented protective measures they should develop criteria to measure the effectiveness of those measures. Assessing effectiveness provides a basis for establishing accountability, documenting actual performance, facilitating diagnoses, and promoting effective management. Effectiveness measures supply the data to affirm that specific goals are being met, or to show what corrective actions may be required to stay on target. An assessment of a protective measure may prove that it was unsuccessful in meeting its objectives, or may bring to light solutions to enhance the protective strategy. These effectiveness measures

will vary from sector to sector and even among specific protective actions. Owner/operators should develop measures around the specific objectives of each protective action.

Should owner/operators receive resources from the CIP Work Group to address vulnerabilities and establish protective measures, then the assessment of performance will be required. The CIP Work Group will require the recipient of funds or resources to submit a status report on the effectiveness of the protective measure that was put in place. The CIP Work Group and the recipient owner/operator will work together to develop a mutually acceptable set of measurements in these situations.

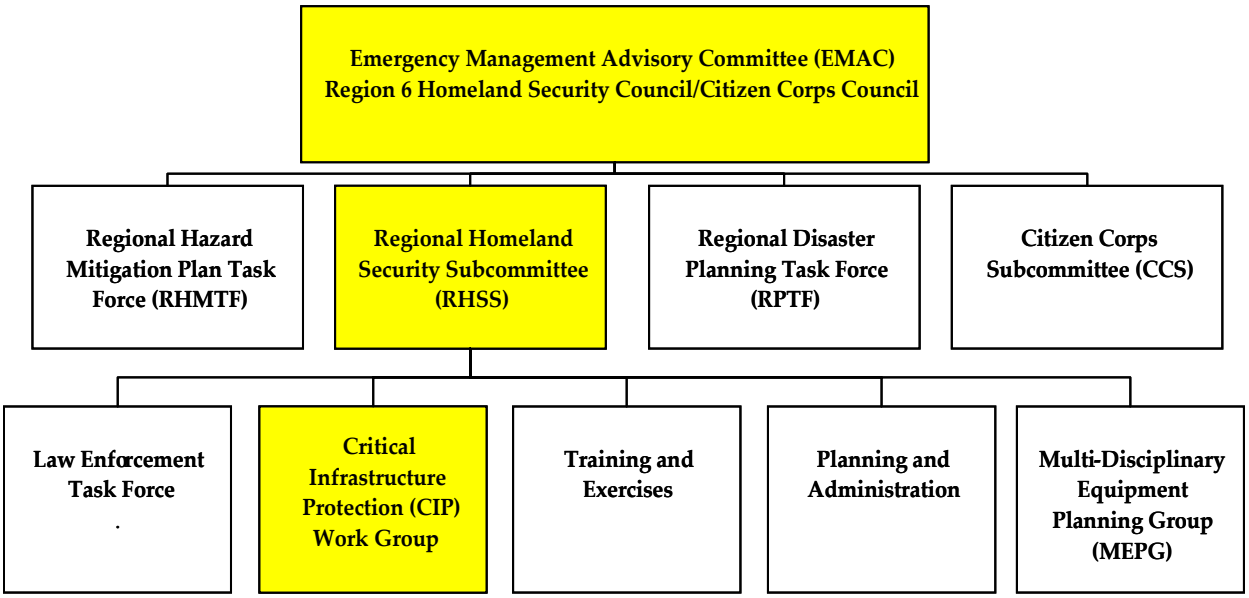
THIS PAGE INTENTIONALLY BLANK

3 ROLES AND RESPONSIBILITIES

This Chapter of the Plan lays out the current and expected roles and responsibilities of stakeholders involved in regional critical infrastructure protection. Specifically, these stakeholders are:

- The Region 6 decision-making bodies:
  - The **Region 6 Homeland Security Council**, which also acts as the **Emergency Management Advisory Committee (EMAC)** has responsibility for funding allocations.
  - The **Regional Homeland Security Subcommittee (RHSS)**, which will review and approve CIP strategies and funding recommendations of;
  - The **Critical Infrastructure Protection Work Group (CIP Work Group)**, which will *develop CIP strategy*, make prioritization and funding decisions based on information provided by stakeholders whose current CIP needs must be supplemented with government support.
- **Local, Federal, and State Governments**, which are ultimately responsible for the securing of infrastructures that meet State or Federal criteria for designation as having State or National significance, respectively.
- **Associations,** which play an essential role in bringing together infrastructure owner/operators to increase and improve communications, identify interdependencies, share best practices, and enhance sector and cross-sector security.
- **Infrastructure owner/operators**, who will be responsible for implementing risk-management programs to secure their infrastructures and assets.

Exhibit 5: Region 6 Homeland Security/Emergency Management Organizational Structure



3.1 Region 6 CIP Decision-Making Entities

In Region 6, Homeland Security is a coordinated effort that requires representation from many disciplines to ensure we protect and secure people and infrastructure. Several government-organized regional committees and work groups are diligently working to provide oversight and recommendations on how to address these unique issues and effectively allocate resources. Exhibit 5 depicts the organizational structure of these bodies, whose responsibilities are described in the next three sections.

The Region 6 Homeland Security Council, the Region 6 Homeland Security Subcommittee and its workgroups are supported by the King County Office of Emergency Management (OEM) - phone: 206-296-3830; Address: 3511 NE Second Street, Renton, WA 98056-4192.

3.1.1 Region 6 Homeland Security Council (R6 HSC)

The Region 6 Homeland Security Council (R6 HSC) also serves as the Emergency Management Advisory Committee (EMAC) and as the Citizen Corps Council. As the R6 HSC, its responsibilities are to oversee emergency management and homeland security-related issues, including regional planning and policies, and homeland security grants. It also approves regional government expenditures and work plans related to homeland security. As it relates to this CIP program, the R6 HSC will continue its operations in accordance with its Charter.

3.1.2 Regional Homeland Security Subcommittee

The Regional Homeland Security Subcommittee (RHSS) is one of the subcommittees of the EMAC. Its primary responsibility is to complete the real ground work through its Work Groups, as it relates to homeland security, by promoting regional coordination to address the management of terrorism prevention, response, and recovery activities. It is responsible for organizing and recommending projects, direction, and funding allocations to the R6 HSC.

The overall efforts of the RHSS are supported by six work groups that further review and address needs based upon the ever-changing requirements of the Region. They include the:

1. Multi-Disciplinary Equipment Planning Group (MEPG)
2. Training and Exercises Work Group
3. Planning and Administration Work Group
4. Critical Infrastructure Protection Work Group
5. Community Emergency Response Team (CERT)/Citizen Corps Planning Group
6. Law Enforcement Work Group

3.1.3 Critical Infrastructure Protection Work Group

The CIP Work Group is one of the dedicated work groups of the RHSS. As such, its primary mission is to facilitate and encourage the protection of regional critical infrastructures and assets. It develops CIP strategy, prioritizes infrastructure, reviews critical infrastructure needs and provides consultation to the RHSS on critical infrastructure-related security issues. It also monitors the processes for communicating with all CIP stakeholders and discipline groups.

The CIP Work Group is responsible for the development and maintenance of this CIP Plan and, as such, has overall responsibility for implementing this Plan. The CIP Work Group will be responsible for prioritizing infrastructure and assets based on information voluntarily provided by infrastructure owner/operators, and then addressing vulnerability concerns, as appropriate, in coordination with the owner/operators. The CIP Work Group will also support owner/operators by assisting them in coordinating with government counterparts in neighboring Homeland Security Regions to address vulnerabilities, protective strategies, and potential funding sources for infrastructures with cross-jurisdictional ties that are brought the CIP Work Group's attention. The CIP Work Group will seek approval for any funding requests and/or allocations from the RHSS.

3.2 Local, State, and Federal Governments

Both the State of Washington and the Federal governments are involved in CIP efforts to identify and create a database of critical infrastructures that meet a set of criteria for having state or national significance, respectively. They are simultaneously working to ensure the security and continuity of those assets. Local jurisdictions within Region 6 are also working to identify their own critical infrastructures. Region 6 has the following expectations of local, State, and Federal governments related to CIP:

- Because of the limited resources available to it, Region 6 will not be able to protect all infrastructures within the Region. Region 6 expects that the local, State, and Federal governments will assume the responsibility for coordinating with owner/operators on the long-term vulnerability reduction of infrastructures within Region 6 that meet their criteria for local, State, or National significance.
- The protection/continued operation of locally, State, or Federally owned/operated infrastructures will be ensured by the appropriate local, State, or Federal owner/operator.
- Notify the Region 6 Homeland Security Council, through King County OEM, of infrastructures identified as having local, State, or National significance, respectively.
- Notify the Region 6 Homeland Security Council, through King County OEM, of activities underway with owner/operators in Region 6 to identify infrastructures, evaluate vulnerabilities, and enhance security.
- Share owner/operator contact information with the Region 6 CIP Work Group through King County OEM.
- Provide the Region 6 CIP Work Group, through King County OEM, with the contact information of Federal, State, and local CIP personnel, respectively.
- Federal and State governments should provide tools to owner/operators for conducting vulnerability and threat self-assessments, and conducting interdependency analyses.
- Develop incentives to promote the voluntary engagement of owner/operators in CIP.
- Federal and State governments should serve as a resource for expert advice on addressing physical, cyber, and human vulnerabilities.
- Provide recommendations for improving regional CIP strategies.

- Federal and State governments should provide funding sources, as available, to Region 6 so it may coordinate the protection of regionally significant infrastructures, including those owned/operated by the private sector.
- Enhance national, state, and local (respectively) information sharing and coordination mechanisms within and across sectors to encourage owner/operator collaboration.
- Collect information on suspicious activities and/or threats witnessed by Region 6 stakeholders.
- As appropriate, Federal and State governments should analyze and authenticate intelligence then share threat information directly with infrastructure owner/operators who may be at risk through appropriate communication vehicles such as the Northwest Warning, Alert, and Response Network (NWWARN).
- Federal and State governments should share threat information and coordinate with local law enforcement to implement tactical protective measures around infrastructures facing plausible and/or specific threats.

3.3 Associations

Critical infrastructure sector associations are an essential component of the Region 6 CIP Program. They serve as the first level of communication between owner/operators of the same sector as described in Chapter 4. Although Chapter 4 designates a few key coordinating associations for each sector, Region 6 recommends that all associations that represent infrastructure owner/operators take up the CIP cause by engaging in the following activities:

- Encourage, inform, and educate members of the necessity of participating in Region 6, State, and national CIP efforts.
- Encourage owners/operators to map the interdependencies that are critical in providing their services; and to examine the interdependencies that could be impacted by a disruption of their services.
- Develop relationships with associations from other sectors upon which interdependencies exist with the sector your members represent.
- Provide mechanisms for members to develop personal and trust based relationships upon which they may coordinate CIP strategies.
- Develop standing committees that address critical infrastructure protection or asset security.
- Provide mechanisms for owner/operators to collectively set standards for security, communicate best practices, and discuss interdependencies with other sectors.
- Keep owner/operators apprised of recent developments in CIP and security issues, standards, and best practices related to their sector.

3.4 Owner/Operators

The ultimate protection of the Region's critical infrastructures and key assets depends on the actions of the owner/operators of those assets. Although some protective failures are inevitable in this era of strategic terrorism, asset owner/operators are expected to practice due diligence by doing everything within their power to protect their assets from potential hazards (natural and human caused), make their assets less attractive as targets (e.g., by creating back-up systems), and take actions to reduce impacts if events do occur.

The following sections describe the roles and responsibilities of critical infrastructure owner/operators in Region 6 as expressed during Focus Group meetings held to facilitate development of this Region 6 CIP plan. The activities of both private and public sector owner/operators will focus on four areas: 1) Vulnerability Reduction and Asset Protection; 2) Threat-Initiated Response; 3) Information Sharing and Coordination; and 4) Leadership. As the Region 6 CIP Program is implemented, these stakeholders will work together to further evolve their specific roles and the mechanisms that will be used for coordination and information sharing.

3.4.1 Vulnerability Reduction and Asset Protection

The Region 6 RHSS and CIP Work Group have a close relationship with many of the infrastructure owner/operators within their jurisdiction. This relationship is built on trust, mutual goals, and coordination. Due to this collaborative private-public sector environment, the RHSS and CIP Work Group are aware that most of its owner/operator partners are already working to protect their critical infrastructure and vulnerable assets with the objective of continuity of operations and service. Region 6 expects infrastructure owner/operators to continue their efforts and utilize a risk management-based vulnerability reduction program and apply risk-management techniques to all planning processes. Chapter 2 of this CIP plan provides a suggested risk management framework for owner/operators to use in identifying, prioritizing, and protecting regional critical infrastructures. An essential part of the risk-management framework described in Chapter 2 and one that cannot be mentioned enough, is the absolute necessity to identify interdependencies within and across sectors. The suggestions in that Chapter are consistent with the expected role and responsibilities of owner/operators involved in this CIP program.

3.4.2 Threat-Initiated Response

Infrastructure owner/operators must be prepared to enhance their security measures and activate preparedness plans when credible threats are known. A threat includes any forewarning that something may exploit a vulnerability regardless of intention or cause. For example, threats may range from tsunami and storm warnings, to knowledge of the malicious intentions of a disgruntled former employee, to terrorist attack warnings. In any instance, owner/operators of critical infrastructures should have security and response plans in place to deploy or enhance security measures based on these threats.

Related to threats of potential terrorist attacks, Region 6 will use the DHS Homeland Security Advisory System (HSAS) as the foundation for preparedness. In the event of an increase in the HSAS level or a specific threat against an infrastructure, neither the Region 6 HSC, RHSS, nor

CIP Work Group will implement protective measures. This is a responsibility that Region 6 places on the owner/operator in coordination with proper law enforcement, and State and Federal authorities. Owner/operators are partially responsible for determining the individual level of threat facing their facilities using information from NWWARN, other members of their sector, internal data, or three types of Federal bulletins:

- ***Homeland Security Threat Advisories*** contain actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets. They may, for example, relay newly developed procedures that, when implemented, would significantly improve security or protection. They may also suggest a change in readiness posture, protective actions, or response. This category includes products formerly named alerts, advisories, and sector notifications. Advisories are targeted to Federal, state, and local governments, private sector organizations, and international partners.
- ***Homeland Security Information Bulletins*** communicate information of interest to the nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to Federal, state, and local governments, private sector organizations, and international partners.
- ***Color-coded Threat Level System*** is used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack. Raising the threat condition has economic, physical, and psychological effects on the nation; so, the Homeland Security Advisory System (HSAS) can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information.

Region 6 expects owner/operators to implement appropriate protective measures as the HSAS changes or as owner/operators determine that their infrastructures are in jeopardy based on other data available to them (e.g., knowledge of the malicious intentions of a disgruntled former employee). Region 6 recommends that owner/operators use the HSAS or develop a similar threat/warning system more specific to their organizations. As such, Region 6 offers the following protective action recommendations based on the owner/operators perceived threat level or the HSAS threat level. The protective measures described below may be implemented under most threat conditions (e.g., storm warnings, insider threats, terrorist warnings, etc.). This set of recommendations is by no means comprehensive. The recommendations are only intended to facilitate the identification of protective actions appropriate for your organization. You may chose to implement some, all, or other appropriate measures based on your organization's unique needs.

Exhibit 6: Recommended Owner/Operator Actions Based on Threat Level[2]

Color	Threat Condition	Recommended Protective Measures
Green	**Low** (Little to no risk of terrorist attack)	▪ Conduct or update vulnerability assessments to determine potential exposure to terrorist, natural, and accidental incidents including cyber attack. Employ mitigation strategies, where practical. ▪ Review physical and operational security to ensure it is commensurate with the needs of the facility. ▪ Review emergency response, business recovery, and crisis management plans and identify updates required by changes in physical conditions, personnel, or potential impact on employees or business operations. Review protective actions, including evacuation and shelter-in-place plans and review scenarios where each strategy would be employed. ▪ Establish early-warning systems to quickly learn of potential threats and provide a means of warning employees to take protective actions in the event of an emergency. Coordinate emergency preparedness activities with local public officials. ▪ Conduct training, education, and drills as required by local, state, and federal regulations and as necessary to familiarize personnel with site emergency procedures. ▪ Conduct an annual exercise to validate plans, generate awareness, and educate member of your response and recovery teams. ▪ Ensure your cyber, data, SCADA, and telecommunications networks are being monitored and properly protected. Update any corporate IT/Telecom policies and train employees on proper cyber security techniques: o Use strong passwords and change them regularly o Look out for E-mail attachments and internet download modules o Install, maintain, and apply anti-virus programs o Install and use a Firewall o Remove unused software and user accounts; Cleanout everything on replaced equipment o Establish physical access controls for all computer equipment o Create backups for important files, folders, and software o Keep current with software updates

[2] Based on guidance from the US-Computer Emergency Readiness Team (CERT), the American Red Cross, and "The Homeland Security Advisory System: Providing a Framework for Business Security," *Remote Magazine*, June/July 2004, Volume 1, Issue 3.

Color	Threat Condition	Recommended Protective Measures
		o Implement network security with access control o Limit access to sensitive and confidential data
Blue	**Guarded** (General risk with no credible threats)	▪ Include all measures from Green Level. ▪ Inspect exterior lighting, fence, door and window locks, surveillance equipment, and intrusion alarm systems and verify they are in good condition. ▪ Inspect and test all fire protection, life-safety and alarm or communication systems used to alert building occupants to take protective actions a well as systems used by emergency response and recovery teams to communicate during an emergency. Verify communication links to official government information are open and monitored. ▪ Verify that members of emergency response, business recovery and crisis management teams have access to the latest copies of plans; are familiar with their roles and responsibilities therein, and verify all critical personnel can be contracted 24/7.
Yellow	**Elevated** (Elevated risk of terrorist attack, but a specific region of the USA or target has not been identified.)	▪ Include all measures from Green and Blue Levels. ▪ Secure buildings and storage areas not in regular use. Increase frequency of inspections and patrols within the facility. Close and lock doors and barriers except those needed for immediate entry and egress. ▪ Scrutinize all contractors, visitors, and packages entering the building. Use company- or government-issued photo ID's to verify identify. ▪ Consider restricting access of motor vehicles to those driven by identifiable employees and scheduled deliveries only. ▪ Randomly inspect vehicles and packages entering the site or building, if the facility is considered a terrorist target. ▪ Remove or prevent access to waste containers or areas that could be used to hide an explosive device or terrorist weapon. ▪ Increase exterior surveillance to identify suspicious activities or packages. Report the presence of unknown persons, unidentified or suspicious vehicles, abandoned parcels or packages, and other suspicious activities. ▪ Maintain adequate complement of security personnel to maintain high level of surveillance and staff assigned to emergency functions. ▪ Request that public law enforcement authorities increase the frequency of patrols for unguarded facilities if they are deemed to be potential terrorist targets. ▪ Constantly monitor radio, television, or other official

Color	Threat Condition	Recommended Protective Measures
		communication channels (e.g., NW WARN) to ensure prompt receipt of warning or threat information.
Orange	**High** (Credible intelligence indicates that there is a high risk of a terrorist attack but a specific target has not been identified.)	▪ Include all measures from Green, Blue, and Yellow Levels. ▪ Provide enhanced security to prevent penetration of site perimeter. ▪ Consult local authorities about restricting the use of public roads, walkways, or entrances/exits to public transportation system that might make the facility more vulnerable to terrorist attack. ▪ Contact vendors/suppliers to confirm their emergency response plans are sufficient and prepared. ▪ Erect barriers to control the direction of travel and proximity of motor vehicles; restrict parking in proximity to building or other sensitive areas. ▪ Screen access to all public areas; prohibit access of unauthorized persons. ▪ Randomly inspect vehicles and packages entering the site or building, if inspections are not already conducted. ▪ Provide staffing necessary to cover all unsecured points of entry. ▪ Place all members of emergency response, business recovery, and crisis management teams on alert to respond immediately, if called. ▪ Verify that emergency operations centers and business recovery sites are properly equipped and ready for occupancy, designated staff are prepared to occupy the site to carry out emergency plans, and non-essential staff are directed to work from alternate sites or from him, if and as directed. ▪ Emergency plans should be up-to-date; staff should be briefed regularly. ▪ Emergency procedure drills should be conducted as needed to ensure prompt decision making, notification, and execution of evacuation and shelter-in-place protective actions.
Red	**Severe** (Terrorist attack has occurred, or credible and corroborated intelligence indicates that one is imminent.)	▪ Include all measures from Green, Blue, Yellow, and Orange Levels. ▪ Monitor radio and television to receive official instruction or orders from public authorities; prepare to release non-essential employees and close facilities as directed by governmental authorities. ▪ Activate and execute emergency response and business continuity plans specific to the location and nature of any incident. ▪ Take all appropriate actions to safeguard personnel safety and

Color	Threat Condition	Recommended Protective Measures
		health. ▪ Consider restricting access to the site or important buildings to essential and authorized staff only. ▪ Inspect all vehicles entering the site to detect possible weapons. ▪ Remove from proximity to the building all vehicles whose owners have not been identified. ▪ At important facilities, increase the frequency and scope of security patrols to the maximum level sustainable. ▪ Frequently communicate with members of emergency response, business continuity, and crisis management teams to relay official information, assess staffing and readiness levels, and execute predetermined plans immediately, if warranted. ▪ Activate crisis management plans to evaluate and address any impact; communicate with staff and key stakeholders as needed. ▪ Make available employee assistance programs to address human impacts.

3.4.3 Information Sharing and Coordination

The core of the Region 6 CIP program is founded on the sharing of information among regional stakeholders and their collaboration in addressing regional vulnerabilities. Both private and public sector infrastructure owner/operators in the Region will be invited to participate in information sharing networks within and across sectors coordinated by the CIP Work Group. Although the CIP Work Group will assist in coordinating the logistics of some meetings, asset owner/operators will typically be responsible for control and content. Region 6 infrastructure owner/operators should accomplish the following goals as they relate to information sharing and coordination:

- Collectively set standards for infrastructure security within each sector.
- Share best practice information with other owner/operators.
- Prepare for information sharing and collaboration by developing a common approach to risk management-based vulnerability reduction and asset protection.
- Participate in information exchanges within and among sectors, and with the Region 6 CIP Work Group by sharing protection gaps, resource needs, and (as appropriate) vulnerabilities and asset information.
- Communicate with suppliers, counterparts, and government entities in other Homeland Security Regions if your infrastructures in Region 6 are dependent upon them for proper operation.
- Share appropriate contact information within and across sectors to facilitate independent coordination and guarantee emergency communications.

- Work with the Region 6 CIP Work Group to develop incentive programs to encourage voluntary implementation of protective measures.
- Report any incidents or suspicious activity to local, State, or Federal law enforcement and other infrastructure owner/operators as appropriate. See Section 4.1.1 on Sharing Threat Information for more details.
- Actively participate in existing sector-wide and national information sharing networks [e.g., trade associations; Information Sharing and Analysis Centers (ISACs); Sector Coordinating Councils; Northwest Warning, Alert, and Response Network (NWWARN)].

In some circumstances, asset owner/operators may identify vulnerabilities that they are unable to address. For example, the owner may lack the necessary funds to implement protective measures, or the vulnerability may need to be addressed by someone outside the owner/operator's authority. In these cases, the protection of the asset still remains paramount. If an owner or operator of an asset that is deemed to be high-priority within the Region is unable to take the appropriate protective measures, they should provide the CIP Work Group with information on the asset, its vulnerabilities, and recommendations for protection. The CIP Work Group can use this information to request State and Federal funding, and coordinate systemic improvements on behalf of individual owner/operators. In this type of situation, the CIP Work Group invites owner/operators to openly coordinate with it in the interests of regional and/or national security. The way in which the CIP Work Group will use this voluntarily submitted information is described more fully in Chapter 5.

3.4.4 Leadership

The security of Region 6 and individual infrastructure stakeholders will benefit from the involvement of all sector stakeholders in this CIP effort. The RHSS and CIP Work Group, however, are limited in their resources to recruit stakeholders. Therefore, for this Region 6 plan to be successful, owner/operators will need to step in and help to engage other stakeholders in this effort. The following section outlines some suggested actions that owner/operators can take to become leaders in the CIP effort:

- Become an active member of sector specific information sharing networks.
- Serve as your sector's representative to the Critical Infrastructure Protection Work Group.
- Encourage CIP strategies and best practices within your sector.
- Participate in response and recovery exercises coordinated by government agencies.
- Encourage other owner/operators and associations which you are a member of to participate in the Region 6 CIP effort and in information sharing and coordination mechanisms.
- Implement protective strategies to reduce vulnerability and secure regional services.

THIS PAGE INTENTIONALLY BLANK

4 INFORMATION SHARING AND COORDINATION

The success of a CIP program depends on the efficiency and openness of the mechanisms that exist to share information among asset owner/operators (within and across sectors) and between these stakeholders and the government. Participation in sector specific information sharing networks and annual interdependency meetings is critical to developing region wide communications and trust between infrastructures and government entities. Region 6 recognizes that most owner/operators already engage in CIP for business purposes and it is planning to provide the mechanisms described in this Chapter to enhance current communication and coordination efforts.

4.1 Background

Region 6 has a strong and cooperative relationship with the infrastructure owner/operators in its jurisdiction. This relationship is built on a long history of collaboration, coordination, and trust, which has been mutually beneficial to the private and public sectors. In preparing this plan, the CIP Work Group conducted interviews, surveys, focus groups, and held seminars to solicit the input of sector stakeholders. Those discussions resulted in a unanimous appeal from asset owners for Region 6 to develop information sharing mechanisms that can bring stakeholders from within and across sectors together to develop similar trust relationships and private information sharing agreements among themselves. The owner/operators made it clear that CIP will not get accomplished through government oversight or additional regulation, but rather when owner/operators are given the resources they need to identify, prioritize, and protect assets with the support of their intra- and cross-sector counterparts.

Currently, Region 6 has information sharing organizations as defined below. The CIP Work Group and RHSS would like to see those organizations used to develop trust relationships and CIP information sharing across Region 6. The primary bodies that will be used and their relationships for intra- and cross-sector communications described in this Section are:

- ***Sector-Specific Information Sharing Networks*** – owner/operator-led organizations that currently facilitate CIP coordination within a particular sector. This Chapter provides examples for each of the top six sectors being addressed in this iteration.
- ***Interdependency Forum*** – an annual conference designed to foster trust and cooperative relationships among owner/operators of different sectors, and to determine regional priorities. This Chapter further describes the invitees, logistics, and confidentiality of these meetings.
- ***Critical Infrastructure Protection Work Group (CIP Work Group)*** – this private-public sector working group of the RHSS (described in Chapter 3) represents the operational level of government CIP decision-making. The membership, types of information dissemination, and confidentiality of the Work Group are discussed in this Chapter.

This Chapter also lays out the process and information requirements for submitting resource requests to the CIP Work Group. In support of these processes, the confidentiality and information security safeguards for these groups are described.

4.1.1 Sharing Threat Information

Citizens, owner/operators, and government officials throughout Region 6 must remain vigilant at all times. Even though this Plan is not designed for use with specific threat information, it remains imperative that threat information be properly communicated to ensure the security of life and services. Therefore, any public or private sector entity that becomes aware of a credible threat, particularly terrorist related, facing the King County area, or any other region, is obligated to report that information. Even suspicious and unusual activity should be immediately reported regardless of whether it poses an imminent threat. First contact your local law enforcement agency. Then, using the contact information at right, contact the Puget Sound Joint Terrorism Task Force (JTTF) and the appropriate Federal entity depending on whether the threat appears to be cyber or physical in nature.

Threat Reporting

- Local Law Enforcement
- Puget Sound Joint Terrorism Task Force (JTTF)/FBI Seattle, (206) 622-0460
- Physical Threats: National Infrastructure Coordinating Center (NICC), (202) 282-9201, nicc@dhs.gov
- Cyber/IT Threats: US-Computer Emergency Readiness Team (CERT), (888) 282-0870, soc@us-cert.gov, or https://forms.us-cert.gov/report
- Northwest Warning, Alert, and Response Network (NWWARN), www.nwwarn.gov

Although the flow of information upward to the appropriate response and protection authorities is essential, it is also important that information should flow down from those authorities to owner/operators. Owner/operators are the first line of defense against potential threats and typically have tactical resources and plans prepared to respond to threats, whether specific or not. As such, owner/operators stand ready and eager to receive threat information that has been analyzed and verified by law enforcement, State, or Federal authorities. Furthermore, they are willing to join the proper networks to receive that information and submit to background checks or other authentication processes that may be necessary. Region 6 encourages relevant government entities to share appropriate threat information with owner/operators through existing threat and warning networks such as the Northwest Warning, Alert, and Response Network (NWWARN).

To be truly effective, the two-way vertical flow of information must be complemented with the horizontal flow of information among owner/operators. It is important that owner/operators and Region 6 share available information with their counterparts within and among sectors through their associations, personal contacts, and through NWWARN, a regional component of the Department of Homeland Security's Homeland Security Information Network –Critical Infrastructure (HSIN-CI). NWWARN is a collaborative effort between government and private sector partners within Washington State with a goal to maximize real-time sharing of situational information without delay and provide immediate distribution of intelligence to those in the field who need to act on it. NWWARN uses readily available communication methods to rapidly disseminate actionable information to its members. All critical infrastructure owner/operators throughout Region 6 are encouraged to join NWWARN and actively participate in information sharing, and warning and alert notifications.

4.2 Sector-Specific Information Sharing Networks

No organization knows and understands the regional assets, vulnerabilities, and threats facing a sector better than the local owner/operators of infrastructure assets in that sector. Region 6 will utilize existing sector-specific information sharing networks to bring owner/operators from within a specific sector together to enhance CIP-related information sharing, learning, collaboration, and coordination. In essence Region 6, through these networks, hopes to create an economy of scale for institutional learning and sector protection.

Information sharing networks representing the Tier 1 sectors (Energy, Information Technology, Telecommunications, Water and Wastewater, Transportation, and Healthcare Systems) will be used to coordinate CIP activities. As additional resources become available, the program may be expanded to include an information sharing network for each remaining sector based on that sector's overall prioritization (See Section 1.2).

Each of the six sectors being addressed in this iteration of the CIP planning process have established information sharing and communication networks that have been operational for many years. These pre-existing networks will serve as experienced, functional communication mechanisms for the purpose of CIP. Region 6 intends to engage these forums in enhancing or developing their roles as regional, sector-specific CIP networks. This Section describes these operational networks for each of the Tier 1 sectors.

4.2.1 Energy Sector

Region 6 will coordinate CIP activities through the Western Electric Coordinating Council (WECC) for the electricity sub-sector of the energy sector. The WECC is one of ten regional committees under the North American Electric Reliability Council (NERC). Its membership is comprised of representatives from electric utility providers connected to the bulk electric system for the Western Grid. The WECC recently established a Physical Security Working Group (PSWG) dedicated to the advancement of physical security at critical transmission, generation, and control facilities within its jurisdiction. The Working Group will hold quarterly conference calls and meet twice a year with its membership.

Within the natural gas sub-sector of the Energy Sector, Region 6 will coordinate with the Northwest Gas Association (NWGA). The NWGA is a trade organization of the Pacific Northwest natural gas industry. The NWGA's members include five natural gas utilities serving communities throughout Idaho, Oregon and Washington, and three transmission pipelines that move natural gas from supply basins into and through the region. One of NWGA's primary missions is to facilitate member company interactions in order to develop common understandings among and between industry participants in the region. Region 6 will work to make CIP and security one of those topics among NWGA members. To become involved in this Energy sector association or for more information, contact the NWGA at (503) 228-4754.

4.2.2 Information Technology & Telecommunications Sectors

The information technology and telecommunications sectors are intimately related. In many cases, information sharing entities address both information technology and telecommunications

concerns. Furthermore, many providers provide service to both of these sectors. Therefore, the Region recommends a variety of information sharing and coordination entities that can serve both sectors equally.

A new organization in the region, spearheaded by the Pacific Northwest Economic Region (PNWER) will play a vital role in cyber-security coordination. The Puget Sound Alliance for Cyber Security (PSACS) was developed to provide a forum for trusted information exchange between various cyber-security focused organizations in the Puget Sound Region. It also seeks to provide a "consensus view" of cyber-security issues faced by the country and region including the development of possible resolutions. PSACS members include government IT/telecom service providers, regulators, other information sharing organizations (e.g., Agora, ISSA, CTIN, InfraGard, Pacciso, etc.), functional area experts, and private industry. PSACS is working to enhance cyber incident response, business continuity education and awareness, and best practice and information sharing. The U.S. CERT has created a secure portal for information sharing related to cyber security issues for the Puget Sound Regional Partnership for Infrastructure Security, a sister committee of PSACS. To become involved in PSACS or for more information, contact PNWER at (206) 443-7723.

Although designed for critical infrastructure protection across all sectors, InfraGard has a particularly active component dedicated to IT and telecom infrastructure. While providing a trusted forum for private sector professionals and local, state and Federal law enforcement agencies to exchange ideas and best practices related to security, InfraGard also provides its membership with information about infrastructure security and current risks and threats. In order to maintain a level of trust within the membership, all applicants undergo a background check performed by the FBI. Applications are then screened according to a defined criterion and then passed to the local chapter for final acceptance. In the case of Region 6, there is an active Seattle Chapter. To become involved in this information sharing network visit the InfraGard website at http://www.infragard.net/index.htm.

At a higher level in the information technology and telecommunications sectors, a national resource is the Information Technology Information Sharing and Analysis Center (IT-ISAC) coordinated by the Department of Homeland Security. This organization primarily coordinates threat and warning information, however, it has subsequent roles in coordinating critical infrastructure protection and sharing of best practices. To become involved in this Information Technology Sector information sharing network or for more information, access the IT-ISAC website at https://www.it-isac.org/.

4.2.3 Water and Wastewater Sector

The CIP Work Group will engage with the Water and Wastewater sector through a variety of associations and information sharing networks. For both Water and Wastewater, the CIP Work Group will coordinate with the Washington Association of Sewer and Water Districts (WASWD). Section IV of WASWD membership primarily consists of Region 6 water and wastewater districts. The organization is dedicated to assisting members in meeting their responsibility to provide clean safe drinking water and environmentally responsible wastewater collection and treatment; and to serve as an advocate for districts on issues of regulation and

policy. To become involved in this Water and Wastewater Sector information sharing and planning network or for more information contact WASWD at (206) 246-1299.

On the Water supply side, the CIP Work Group will also coordinate with the Pacific Northwest Section (PNWS) of the American Water Works Association (AWWA). PNWS-AWWA is dedicated to providing leadership to the drinking water profession in the Pacific Northwest in areas of drinking water quality, water resource policy, customer service, and water-related planning issues. The CIP Work Group will also seek out the involvement of some of the applicable PNWS-AWWA committees, including the Washington Water Utility Council (WWUC). To become involved in this Water and Wastewater Sector information sharing and planning network or for more information, contact PNWS-AWWA at (503) 760-6460.

Related to Wastewater, the Region 6 CIP Work Group will coordinate CIP issues with the Metropolitan Water Pollution Abatement Advisory Committee, or MWPAAC, advises the King County Council and Executive on matters related to reducing water pollution. It consists of representatives from cities and local sewer utilities that operate sewer systems in King County. Most of these cities and sewer utilities deliver their sewage to King County for treatment and disposal. To become involved in this Water and Wastewater Sector information sharing and planning network or for more information, contact the King County Department of Natural Resources and Parks, Wastewater Treatment Division at (206) 684-1156.

4.2.4 Transportation Sector

Related to highways, roads, and rail transportation, the Region 6 CIP Work Group will coordinate with the Washington Chapter of the American Public Works Association (APWA) and its Emergency Management Committee. This organization consists of private and public sector transportation stakeholders including municipalities, departments of transportation, engineers, consultants, suppliers, and service providers. To become involved in this Transportation Sector information sharing and planning network or for more information, contact the Washington Chapter of APWA at (206) 625-1300.

Related to transit, particularly bus, ferry, rapid transit, and municipal transit departments, the Region 6 CIP Work Group will coordinate with two organizations – the Washington State Transit Association (WSTA) and the American Public Transit Association (APTA). The WSTA represents 25 transit systems in the State and its members include State and local agencies and organizations, vendors, and consultants. The WSTA specifically works to promote legislation/advocacy, professional development through communication/cooperation, information sharing, and awareness. The WSTA is currently considering the activation of a Security Committee, which the CIP Work Group will work to support. At a more national information sharing level, the APTA consists of representatives from bus, rapid transit and commuter rail systems, and the organizations responsible for planning, designing, constructing, financing and operating transit systems. APTA's Risk Management Committee addresses issues of concern to transit professionals involved in security, safety, and risk management. To become involved in one of these Transportation Sector information sharing and planning networks or for more information contact WSTA at (360) 786-9734 or APTA at (202) 496-4800.

Another organization offering communication and networking support to multiple modes of the transportation sector is the Regional Freight Mobility Roundtable. The Regional Freight Mobility Roundtable is a nationally recognized public-private forum to define and recommend actions serving freight mobility needs in and through central Puget Sound. Private sector participants include rail, marine, air cargo and trucking carriers, and shippers such as Boeing and Weyerhaeuser. Public sector participants include local governments, the ports of Seattle, Tacoma and Everett, state agencies, and federal agencies within the U.S. Department of Transportation (including rail, highway, maritime) and the Department of Defense. As a shared "communication hub," the Roundtable is consulted by the FAST Corridor and provides input into regional and state transportation plans. The CIP Work Group will reach out to the Roundtable in an effort to get its members active in CIP. To become involved in this Transportation Sector information sharing and planning network or for more information contact the Puget Sound Regional Council at 206-464-7090.

The Region 6 CIP Work Group will coordinate aviation/airport CIP issues through two organizations as well - the Washington Airport Management Association (WAMA) and the Northwest Chapter of the American Association of Airport Executives (AAAE). WAMA's mission includes building relationships between members, industry professionals, and State and Federal government representatives to promote effective airport management. Although it has not specifically addressed CIP in the past, its goals of 1) linking airports in Washington State to achieve their common interests, and 2) identifying and addressing problems and opportunities will speak to CIP. The organization includes management staff from Washington's airports, engineers, municipalities, transportation departments, private suppliers, and airlines. At a greater regional level, the Northwest Chapter of the AAAE offers ideas to maximize revenues and minimize costs, provides valuable networking opportunities, keeps members informed on industry issues, and offers expert advice. The CIP Work Group will seek out the assistance of the Chapter's Transportation Security Services Committee to assist in CIP efforts within Region 6. To become involved in one of these Transportation Sector information sharing and planning networks or for more information contact WAMA at (360) 403-3474 or the Northwest Chapter of the AAAE at (970) 640-0551.

4.2.5 Healthcare Systems Sector

Region 6 has a standing Emergency Preparedness Committee for the healthcare community organized by *Public Health: Seattle & King County*. The Emergency Preparedness Committee consists of representatives from all 22 hospitals in King County, Public Health: Seattle & King County, the Washington State Hospital Association, poison control centers, and blood banks.

Although not specifically designed for CIP communications, the Emergency Preparedness Committee's current mission easily accomplishes the goals of facility and staff security. The Committee's current work groups address issues related to strategy, planning, training and exercises. The CIP Work Group will work closely with the Committee to incorporate CIP as an objective into one of its existent work groups or into a new and separate work group.

To become involved in this Healthcare Systems information sharing and planning network or for more information contact Public Health: Seattle & King County at (206) 296-4600.

4.2.6 Voluntary Status Reporting

Although the CIP Work Group cannot mandate that these sector-specific information networks share information with it, it still remains accountable to the Region's 1.8 million residents, the U.S. Department of Homeland Security, and the nation as a whole to monitor and ensure the protection of critical assets within the Region. Therefore, Region 6 requests that each Sector-Specific Network provide voluntary annual status reports on general sector-wide asset identification, protection, coordination, and information sharing activities underway, as well as a description of any difficulties and gaps, and requests for assistance from Region 6, Washington State, or the Federal government. This information need not be specific, but should provide Region 6 with enough information to demonstrate that the sector is taking all necessary actions to secure its infrastructures. Region 6 will use the information provided in these reports (kept strictly confidential as described in Section 4.6) to develop and evaluate strategies, as needed, to better address critical infrastructure threats, vulnerabilities, and protective measures.

4.3 Interdependency Forum

Once each year, the CIP Work Group will coordinate a CIP cross-sector Interdependency Forum. The primary purpose of the Forum will be to establish relationships similar to those developed in the Sector-Specific Information Sharing Networks, but among owner/operators from different sectors. Invitees shall include all owner/operators in the top six sectors and representatives of the Region 6 homeland security organization shown in Exhibit 5.

Some examples of Forum design and agenda items that the CIP Work Group may consider include:

- Facilitated group discussion
- CIP-related presentations
- Guest speakers
- Tabletop exercises
- Cross-sector break-out groups
- Interdependency workshops
- Networking sessions

The purpose of the Interdependency Forum is to open lines of communication and spark CIP-related actions and strategies among infrastructure owner/operators, separate from any public agency-led effort. The Interdependency Forum is also intended to produce a consensus on a set of regional CIP priorities that can be used in grant funding and resource decisions. Those priorities may range in specificity from a list of prioritized assets and corresponding protective remedies to general strategies for information sharing. Any results, decisions, or data derived by/in the Interdependency Forum must officially be approved for CIP Work Group consideration by a vote of the Forum majority. Furthermore, when related to specific assets and vulnerabilities, the original owner/provider of that asset information must grant specific written permission for consideration to the CIP Work Group. Though the members of the CIP Work Group will be in attendance at each Interdependency Forum, and may play various roles including facilitators, presenters, and observers, they will act under the auspices of Non-Disclosure Agreements. CIP Work Group members will not be able to bring information from Forums into their internal considerations without express permission from Forum participants.

4.3.1 Logistics of the Forum

The Sector-Specific Information Sharing Networks are owner/operator-led. Nevertheless, because of the diversity of stakeholders and sheer number of participants, the CIP Work Group will be responsible for setting the agenda, design, and length of each Interdependency Forum based on its knowledge of current CIP activities and needs in the Region. Interdependency Forums may range in length from a half-day to a two day session. Forums shall be held once a year or more frequently based on feedback from participants. The CIP Work Group, in consolidating efforts, may decide to partner with an established organization and task them to lead the coordination of the Interdependency Forums. One organization that plays a similar role in the region and has experience and established relationships is the Pacific Northwest Economic Region (PNWER).

4.3.2 Confidentiality of Interdependency Forums

Interdependency Forums will be designed to be confidential gatherings where owners/operators may openly share specific information related to critical infrastructure assets, vulnerabilities, protective strategies, dependencies, risks, and threats with one another. Under Revised Code of Washington (RCW) 42.30 – the Open Public Meetings Act (OPMA) – Interdependency Forums will be considered *Executive Sessions* and will be closed to the public and media due to their consideration of matters affecting national security, which are exempt from the OPMA under RCW 42.30.110. State and local councils and committees are exempt from Federal open meeting laws under the Federal Advisory Committee Act of 1972, §4(2)(c).

As required by RCW 42.30.110(2) a King County Office of Emergency Management (OEM) representative will be officially responsible for the coordination of these *Executive Sessions*, and recognized by the State of Washington as the presiding officer of the Interdependency Forum. That representative shall publicly announce the purpose for excluding the public from the meeting place, and the time when the *Executive Session* will be concluded. The *Executive Session* may be extended to a stated later time by announcement of the OEM representative.

Prior to the convening of each Interdependency Forum, all participants will sign mutual Non-Disclosure Agreements (NDAs). An NDA is a contract in which the parties promise to protect the confidentiality of information that is disclosed during a specific type of business transaction (see Attachment A).

Participants will have then entered confidential relationships and are legally bound to not disseminate information. Participants who divulge information shared in Interdependency Forums without the written permission of the owner/provider of the information will be pursued through legal means and a court will be requested to stop the violator from making any further disclosures and the affected owner/provider may pursue legal recourse.

Under RCW 42.17.310 (See Section 4.6 – Information Security), items protected from public disclosure will include:

- Notes taken by Region 6 representatives at Interdependency Forums;

- Information given to the CIP Work Group via Forum consensus, or direct submission to the CIP Work Group by participants for the purpose of funding and resource considerations.

4.4 Critical Infrastructure Protection Work Group

In the Regional information sharing and coordination structure (depicted in Exhibit 7), the CIP Work Group will serve to ensure that information sharing programs are effectively executed. As described in Chapter 5 of this Plan, the CIP Work Group is responsible for analyzing data provided to it by any of the information sharing bodies or individual owner/operators, setting priorities, and pursuing grant and resource opportunities based on that information. It will continue to perform these services based on the guidelines set forth in this Plan and any tasks it receives from the RHSS.

4.4.1 CIP Work Group Membership

The CIP Work Group membership will be determined as set forth in its bylaws. The CIP Work Group will include at least one elected representative from each sector who will serve a term of one year. No term limits apply to these positions.

It is the ultimate goal of the RHSS to have one representative from each of the 17 regionally-recognized critical infrastructure sectors sit on the CIP Work Group. The RHSS will also appoint members who reasonably represent the public and private sectors.

4.4.2 CIP Work Group Information Dissemination

The CIP Work Group will typically act as a facilitator and information coordinator. The mechanisms in this CIP information sharing network will feed the CIP Work Group with information from owner/operators so that the CIP Work Group may facilitate resource allocation and regional strategy development. In a few select cases, the CIP Work Group will act as an information provider. The CIP Work Group will:

- Notify owner/operators through the sector specific information sharing networks, or Interdependency Forums of changes in Federal, State, or local policy related to CIP.
- Inform owner/operators of grant and funding opportunities and notify them of deadlines, procedures, and submission requirements.
- Share progress toward or awards related to CIP grants and funding with owner/operators.
- Share appropriate threat information with specific infrastructure owner/operators when granted permission to do so by Federal, State, and law enforcement authorities.

4.4.3 Cross-Regional Coordination

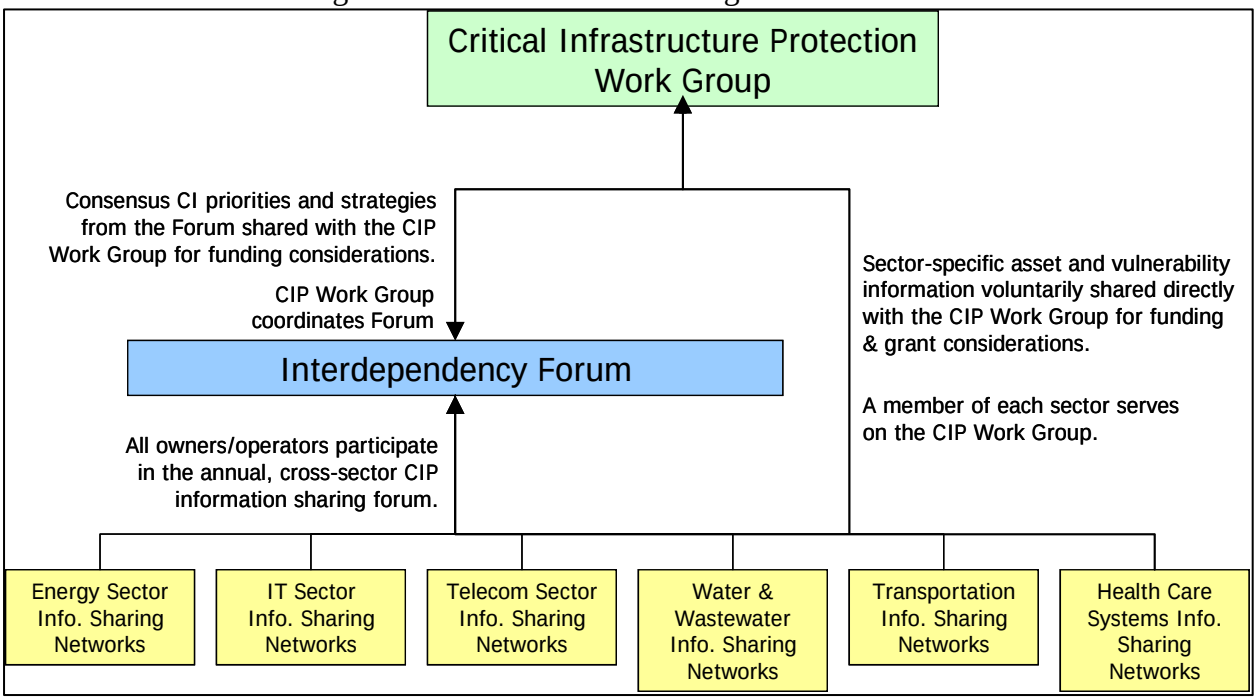
The Region 6 CIP Work Group will reach out to its counterparts in neighboring regions including Chelan, Kittitas, Kitsap, Pierce, and Snohomish counties, which represent portions of Washington State Homeland Security Regions 1, 2, 5, and 7. As owner/operators identify dependencies on assets in other Regions, and as extra-regional stakeholders bring their important dependencies on Region 6 to the attention of the CIP Work Group, joint discussions will be

arranged to fully consider the implications of these interdependencies in each Region. The CIP Work Group will assist owner/operators and other Regions in their efforts to coordinate with each other to secure infrastructures that cross jurisdictional boundaries.

4.4.4 Confidentiality of CIP Work Group Meetings

CIP Work Group meetings will typically be open to the public. However, when the Work Group plans to discuss information specific to national or regional security, and particularly when it is reviewing infrastructure asset information submitted to it by owner/operators, as described in Section 4.5 below, that portion of the meeting will be designated an *Executive Session* and all public observers will be asked to leave. That portion of the meeting and all information shared or discussed within it will then be protected in the same fashion as described in Section 4.3.2 and Section 4.6 of this Plan. Even in closed session meetings, members of the CIP Work Group will be required to sign mutual Non-Disclosure Agreements as described in Sections 4.3.2 and 4.6.

Exhibit 7: Region 6 CIP Information Sharing and Coordination Structure



4.5 Requesting Resources From Region 6

As discussed in Section 3.2.2, there may be times when regional owner/operators identify vulnerabilities that they are unable to address with current resources or authorities. In such cases, the owner or operator should provide the CIP Work Group with information on the asset, its vulnerabilities, and recommendations for protection so that the CIP Work Group may conduct a consequence-based risk assessment of its own, as described in Chapter 5, to determine regional funding priorities. This information should only be provided to an authorized representative of Region 6 along with an express written statement granting Region 6 access to the information provided. This information will be protected from disclosure, as explained in Section 4.6. Unlike the coordination mechanisms described earlier in this Chapter, which will be evolving, the CIP

Work Group is fully operational on this topic and is prepared to handle and make decisions related to resource allocation. The information that the CIP Work Group should have for its resource allocation considerations are:

Asset Information

- Asset name and address or general description of location (e.g., meat processing facility ABC, XYZ Inc., etc.).
- Owner/operator name and address (e.g., ABC Company, contact person, address, telephone number, etc.).
- Sector (e.g., transportation, energy, etc.).
- Asset class or sub-sector (e.g., transportation-marine, etc.).
- Tracking/identification number (if applicable).
- Seasonality/frequency of use.
- Function within the infrastructure (e.g., XYZ Inc. makes batteries for missiles).
- System components that are central to the mission and function (names of major systems).
- Dependencies (e.g., what does the asset depend on to function?).
- Continuity and redundancy to include back-ups built into the asset.
- Existing protective measures (e.g., fencing, biometrics, firewalls, etc.).

Vulnerability Information

- Specific vulnerability assessment related to the asset in question.
- Estimate of the asset's attractiveness or likelihood to be targeted by terrorists (typically closely related to the consequence), or an estimate of the asset's probability of being disrupted or destroyed by other means (e.g., natural disaster).

Consequence Information

- Results of a Consequence Analysis to include the effects of disruption or destruction on:
  - Other infrastructure assets—interdependencies (e.g., what depends on it: people, physical assets, information technology, telecommunications, other sectors, etc.?).
  - The regional economy.
  - Public health and welfare.
  - The public psyche.
  - National or regional security.
  - Estimate of the likelihood/probability that an attack on the asset would result in the predicted consequences.

Protective Measure Recommendations

- Specific protective actions for which the owner/operator seeks resources from the government.
- Specific protective measure for each vulnerability in question, to include acquisition data (cost, timing, etc.).
- Discussion of how each protective alternative will address the problem and the likelihood of the action's effectiveness in eliminating the vulnerability.
- Analysis of the benefits for each protective alternative (e.g., cost/benefit, pairwise, parallel, etc.).

Owner/operators seeking resource assistance from Region 6 should consult Chapter 5 of this plan to see what Region 6 will take into consideration when prioritizing its funding choices. This information can help owner/operators tailor their resource requests to support the decision-making needs of the CIP Work Group. It is important to note that due to the voluntary nature of and resources available to this program, Region 6 may not actually consider the most critical infrastructures in the Region when allocating funds. If the owner/operator determines that they are capable of providing the proper security and ensuring the continued operation of their infrastructures then they may not bring those infrastructures to the attention of Region 6. Therefore, data provided to Region 6 and funding requests associated with that data may involve infrastructures of lesser importance compared to others already being secured by their owner/operator or other government entities[3]. Nonetheless, the infrastructures that warrant resource allocations will be of high regional importance as described in Chapter 5.

4.6 Information Security

Region 6 is committed to protecting the sensitive information that asset owner/operators entrust to it for developing CIP strategies and making funding decisions. Region 6 takes very seriously the consequences to relationships, competitive advantages, business operations, and regional and national security that may result from poor data security and management. Confidential and business sensitive information provided in either electronic or hard copy format to the CIP Work Group or any Region 6 representative will be stored at the headquarters of King County OEM, as the administrator for Region 6, in secure and locked storage accessible only to members of the CIP Work Group and appropriate King County OEM staff with a valid "need-to-know." Such information will not be shared with other government entities, including law enforcement, the State EMD, or DHS, without the express written permission of the owner/provider of that information. Furthermore, asset and vulnerability data will only be used for specific business purposes related to supporting CIP efforts and related issues of regional security. Information will not be removed from King County OEM, disseminated, transferred, or reproduced in whole or part, in any way, without the express written permission of the owner/provider of that information. When new or replacement data is provided to Region 6, obsolete data will be properly destroyed in a manner that will prevent reconstruction of the information in whole or in part.

[3] See Chapter 3, "Roles and Responsibilities," for descriptions of protective measure expectations on each stakeholder.

Information shared during, produced in, or as a result of Interdependency Forums and meetings of the CIP Work Group will be protected from public disclosure under the exemptions for records disclosure as presented in the Revised Code of Washington (RCW) 42.17.310. These exemptions will prohibit and prevent infrastructure information – which may include, but is not limited to, proprietary and business confidential information related to threats, specific assets, vulnerability assessments, cascading effects, and interdependency – voluntarily provided to the CIP Work Group to be disseminated to the public or private parties. For a list of Federal and State exemptions to public disclosure related critical infrastructure protection, which will be used to protect critical infrastructure information as referenced in this plan, see Appendix 7: Public Disclosure Exemptions.

This plan does not address information protections under the Federal Critical Infrastructure Information Act, a designation known as Protected Critical Infrastructure Information (PCII), because the legitimacy of those protections were under review during the development of this plan. Also, as of the time of drafting this plan, the Department of Homeland Security was re-evaluating and revising the PCII Program. This plan will be revised to reflect guidance on this topic from DHS as it is released.

THIS PAGE INTENTIONALLY BLANK

5 DECISION MAKING PROCESS

This Chapter provides guidance on how the CIP Work Group will make decisions on allocating resources for protecting critical assets. In addition, it describes the primary sources of funding for CIP activities and how those funds can be used.

Under the Region 6 organizational structure, the CIP Work Group has the authority to allocate DHS grant dollars on behalf of the RHSS, pending its approval. Furthermore, these allocations must be consistent with the objectives presented in the Region 6 Homeland Security Strategic Plan. This CIP Plan and the programs and processes described within it are in alignment with the Region's action strategies. Therefore, decisions made using the programs and processes described here will satisfy the requirements of the Region 6 HSSP.

5.1 Cross-sector Analyses & Resource Prioritization

This Section presents the protocol that will be used by the CIP Work Group to make prioritization decisions related to CIP. As described in Sections 3.2.2 and 4.5, the CIP Work Group may receive resource requests from owner/operators who are unable to address the vulnerabilities of regionally critical assets without additional support. Because the Region has limited resources and grant dollars, the CIP Work Group will need to identify which security gaps pose the greatest risk and then identify the appropriate strategy and resources for protection.

To prioritize among critical assets and sectors, the CIP Work Group will use a consequence-based crosswalk using information on vulnerability and consequence supplied by the owner/operator. Once priorities have been determined, the CIP Work Group will request that the owner/operator provide information on protective measure choices and an analysis (as discussed in Section 4.5). The CIP Work Group will use this information to identify which protective measures to fund and how that funding will be obtained. It is important to note that due to the voluntary nature of and resources available to this program, Region 6 may not actually consider the most critical infrastructures in the Region when allocating funds. If the owner/operator determines that they are capable of providing the proper security and ensuring the continued operation of their infrastructures then they may not bring those infrastructures to the attention of Region 6. Therefore, data provided to Region 6 and funding requests associated with that data may involve infrastructures of lesser importance compared to others already being secured by their owner/operator or other government entities[4]. Nonetheless, the infrastructures that warrant resource allocations will be of high regional importance.

5.1.1 Consideration of Hazards

In conducting its analysis of critical infrastructure risks across the Region, the CIP Work Group will take into consideration the types of threats facing the Region if available from law enforcement agencies. These generally known hazards and/or threats should be at the foundation of each owner/operator's risk analysis. In considering the threats facing assets of this nation, the CIP Work Group will also consider the 14 national preparedness scenarios relevant to the region

[4] See Chapter 3, "Roles and Responsibilities," for descriptions of protective measure expectations on each stakeholder.

that are being used as the basis for the National Preparedness Goal under HSPD-8. It is recommended that infrastructure owner/operators also use these threat scenarios in internal protection planning efforts once they become available.

5.1.2 Consequence Analysis

The CIP Work Group will need to look across sectors and assets to weigh the consequences of an attack or failure. Typically, a full risk assessment would involve balancing consequence with probability. At this level of decision-making, however, there are two types of probability that will be considered fixed:

Consequence – The negative outcomes associated with degradation or failure of an asset.

- The likelihood of an attack occurring will increase proportionately with an increase in consequence.
- The odds that a particular attack will be successful and result in the potential consequence will be considered 100%. The CIP Work Group will assume that an exploitation of the vulnerability will result in the anticipated consequence.

The following consequence factors will be used for regional-level screening – these factors will be scored in comparison to each other and ranked accordingly by the CIP Work Group.

- Human health and safety impact -- measured as the range of equivalent statistical lives lost
- Economic impact -- measured in dollar ranges
- Environmental impact -- measured in dollar ranges (equal to economic impact at the same categorical level) and displacement
- Sociopolitical impacts (icons and political leadership) -- measured using nonnumerical descriptive categories
- National security impacts (military and response capability) -- measured using nonnumerical descriptive categories

The definition of each consequence-related measure includes “collateral damage” (i.e., damage that occurs outside of the boundaries of the asset, which includes effects related to interdependencies).

Region 6 will rank consequences on a categorical scale of I-V, where category I represents the most significant potential consequences to the region. Because this analysis takes both probability and consequence into consideration it is also synonymous with determining risk. The CIP Work Group will determine the “criticality” of an asset based on the predicted consequences from its disruption/destruction and it will assign a categorical ranking accordingly.

Assets may have special considerations that the CIP Work Group will have to weigh subjectively. For example, the Work Group may determine that a facility where fatalities may include many children takes protective priority over all other assets, regardless of how high their economic impacts, environmental impacts, etc. may be. These special considerations cannot be

accounted for quantitatively, but must be addressed qualitatively by responsible, representative members of the community through the CIP Work Group.

5.1.3 Protective Measure Review

Once the CIP Work Group has chosen the top regional assets based on potential consequences it will review the protective measure selections submitted by the asset owner/operators (if more than one option was offered). As mentioned in Section 4.5, the asset owner/operator must supply the CIP Work Group with select information on protective measure options to facilitate its decisions.

The Region shall take greater consideration of protective options that are eligible for Federal grant dollars as described in the next Section 5.2. Common critical infrastructure protective strategies that the Region may consider, and those which are eligible for DHS grant funding, include:

- Physical security, including extension of security perimeter beyond the limits of facility to create a buffer zone
- Roving security inspections
- Access control
- Background checks for employees, temporary workers, contractors, subcontractors, security force, and potential first responders
- Loss prevention, material control, and inventory management
- Delivery service verification (e.g., request delivery worker identity card)
- Control-room security
- Policies and procedures
- Information/cyber security
- Intelligence, particularly for specific assets (e.g., East Coast vs. West Coast)
- Training on security plans
- Drills involving employees, contractors, public, and media
- Crisis management and emergency response, including incident command system
- Communication of hazards by asset owners to public sector protection forces

5.1.4 Resource Allocation Priorities

To determine its ultimate resource priorities, the CIP Work Group will balance an asset's categorical level of consequence determined in Section 5.1.2 with the estimated level of effectiveness of the protective measure suggested by the owner/operator (required in Section 4.5).

If the owner/operator's benefits analysis (e.g., cost/benefit, pairwise, parallel, etc.) is thorough, then it should include an estimate of how successful the protective measure will be at eliminating the vulnerability (e.g., 95% successful/95% reduction in vulnerability). Using the chart provided in Exhibit 8, the CIP Work Group will crosswalk these two variables to determine an overall level of high (H), moderate (M), or low (L) priority.

Exhibit 8 – Consequence/Protective Measure Effectiveness Crosswalk

Estimated Effectiveness of Protective Measure						
> 95%	L	M	H	H	H	H
90 – 95%	L	M	M	H	H	H
80 – 90%	L	L	M	M	H	H
70 – 80%	L	L	L	M	M	H
60 – 70%	L	L	L	L	M	H
50 – 60%	L	L	L	L	L	M
	VI	**V**	**IV**	**III**	**II**	**I**
	Consequence Category					

For further prioritization considerations, the consequence/benefit level increases from the lower left corner to the upper right. For example, an asset determined High priority categorized by 95% Effectiveness and Consequence Level I is of greater priority than another High priority asset categorized by 92% Effectiveness and Consequence Level II. If funding and resource limitations prevent the Region from addressing multiple and equally significant priorities then further prioritization is required. If specific asset priorities cannot be found through this process, then the CIP Work Group may determine ultimate priority in one of two ways:

1. By a subjective consensus decision of the CIP Work Group members.
2. By pursuing a more detailed and quantitative risk-analysis comparison of the competing assets.

Although the latter option is preferable, risk analysis is typically expensive and time consuming. The CIP Work Group may therefore be asked to use the consensus decision approach, unless time permits and the asset owner/operators in question agree to fund the risk analysis comparison. In either situation, the CIP Work Group will base its funding and protective support decisions on the outcomes of this assessment approach. Those at higher priority levels will receive funding and resource considerations.

Resource allotments from Region 6 to infrastructure owners and operators for the establishment of protective measures will be executed under the auspices of the contractual and legal requirements of King County, the State of Washington, and the U.S. Government.

5.2 Implications of Funding Options on the Decision-Making Process

This Section describes the primary sources of funding for CIP activities and the implications that funding requirements have on the CIP Work Group's resource allocation decisions. The CIP Work Group will consider the information discussed in this Section before making final decisions on resource allocation.

The primary source of CIP-related grants and funding is the Office for Domestic Preparedness (ODP) within the DHS Office of State and Local Government Coordination and Preparedness (OSLGCP). Other sources of homeland security grant funding include:

- Federal preparedness programs, other than from DHS/ODP, including those offered by the Department of Health and Human Services through the Centers for Disease Control and Prevention, Health Resources and Services Administration, and the U.S. Food and Drug Administration; the U.S. Department of Agriculture; the U.S. Department of Justice; the U.S. Department of Transportation; the Federal Emergency Management Agency; DHS Science and Technology; DHS Information Analysis and Infrastructure Protection; and other relevant organizations.
- Washington State homeland security and preparedness programs and resources.
- Local and tribal homeland security and preparedness programs and resources.
- Private sector homeland security preparedness programs and resources.[5]

Although other homeland security grant programs exist, the DHS/ODP is the most consistent and largest provider of funds for CIP. Therefore, this Section will focus on grant prospects from DHS/ODP, which has been the traditional focus of Region 6 in the past. The CIP Work Group should nonetheless explore these alternative sources of funding when Region 6 is considering and seeking out financial support for protective measures for infrastructure systems.

5.2.1 U.S. Department of Homeland Security Grant Programs

The only entity eligible to apply for a DHS/ODP grant is the State of Washington's designated State Administrative Agency (SAA), which is currently the Washington Military Department, Emergency Management Division (EMD). Furthermore, grant funding opportunities are not continuous, and in some cases the application window is only open for one month every few years. Homeland Security Region 6 cannot directly request grant funding from DHS. Therefore, all funding request activities within the Region will need to be closely coordinated with the State EMD. Region 6 will need to clearly communicate its priorities and provide necessary supporting documentation to the EMD during the application window. The CIP Work Group must remain aware of funding needs in other State Homeland Security Regions, because the EMD will ultimately be responsible for allocating funds from DHS to all local units of government.[6] The funding requests of the Region will compete with funding requests from other regions in the State.

[5] From the U.S. Department of Homeland Security Fiscal Year 2005 Homeland Security Grant Program Guidelines and Application Kit.

[6] As defined in the Conference Report accompanying the Department of Homeland Security Appropriations Act of 2005, the term "local unit of government" means "any county, city, village, town, district, borough, port authority, transit authority, intercity rail provider, commuter rail system, freight rail provider, water district, regional planning commission, council of government, Indian tribe with jurisdiction over Indian country, authorized tribal organization, Alaska Native village, independent authority, special district, or other political subdivision of any state."

The Homeland Security Grant Program (HSGP) is the core of the ODP grant system. It consolidates six grant programs into a single application process. The HSGP includes the following grant mechanisms:

- State Homeland Security Program (SHSP)
- Urban Areas Security Initiative (UASI)
- Law Enforcement Terrorism Prevention Program (LETPP)
- Citizen Corps Program (CCP)
- Emergency Management Performance Grants (EMPG)
- Metropolitan Medical Response System (MMRS)

This Section will only focus on those programs that are applicable for regional and local critical infrastructure protection funding, which include the SHSP, UASI and LETPP. Under these programs the State of Washington is required to disperse not less than 80% of the total grant amount to local units of government.[7] Furthermore, transferring funds between grant programs in the HSGP family is strictly prohibited by DHS; therefore, the CIP Work Group must be sure to submit requests for the appropriate grant program and in the correct amount.

The following sections provide a brief description of each of the major DHS/ODP grant programs. For more information on specific funding-eligible programs visit the DHS/ODP website at http://www.ojp.usdoj.gov/odp/grants_programs.htm.

5.2.1.1 State Homeland Security Program (SHSP)

SHSP provides financial assistance directly to each of the states and territories to prevent, respond to, and recover from acts of terrorism. SHSP supports the implementation of the State Homeland Security Strategy to address the identified planning, equipment, training, and exercise needs.

The CIP Work Group should work to identify CIP solutions that are eligible for Federal funding under SHSP. As of the 2005 ODP Guidance the four areas eligible for funding under SHSP include Planning, Training, Equipment and Exercises.

5.2.1.2 Urban Areas Security Initiative (UASI)

UASI provides financial assistance to address the unique planning, equipment, training, and exercise needs of high-risk, high-threat, high-density urban areas, and to assist them in building an enhanced and sustainable capacity to prevent, respond to, and recover from threats or acts of terrorism. Allowable costs for the urban areas mirror those under SHSP, and funding is expended based on Urban Area Homeland Security Strategies. This funding is provided to

[7] Exceptions: 1) The State may retain funds under UASI, but those funds must be used in direct support of the urban area. 2) The local unit of government may request that the State retain its funds under the SHSP for State expenditures in support of the local unit of government. A Memorandum of Understanding specifying expenditures, roles and responsibilities must be signed between the two parties.

identified urban areas through their SAA. Funds under UASI are also available to protect nonprofit organizations located within designated urban areas.

The eligible expenditures under UASI are the same as those discussed under the SHSP—except for the addition of operational reimbursements—and must satisfy the strategies described in the Urban Area Homeland Security Strategy.

5.2.1.3 Law Enforcement Terrorism Prevention Program (LETPP)

LETPP seeks to provide law enforcement communities with enhanced capabilities for detecting, deterring, disrupting, and preventing acts of terrorism. The LETPP is administered by the SAA in close coordination with the state's Lead Law Enforcement Agency (LLEA) directly to law enforcement communities. Many of the programs that the LETPP funds are similar in mission to those the CIP Work Group is seeking to accomplish through the Region 6 CIP program. It is likely that the CIP Work Group will find CIP related solutions under this grant program. If the CIP Work Group identifies potential funding opportunities that suit regional CIP priorities under the LETPP, then it will have to work in close coordination with the LLEA, SAA, and local law enforcement agencies of Region 6. The CIP Work Group will have to market its ideas and strategies to gain buy in, support, and consensus, and then coordinate grant application and request documents. Regardless of whether Region 6 decides to pursue funding through the LETPP in coordination with law enforcement, it should nonetheless communicate its priorities with appropriate law enforcement officials to eliminate duplicate efforts and ensure the efficient use of limited resources.

Like the SHSP and the UASI, the LETPP provides funding in five general categories related to the themes mentioned above – Planning, Operations, Equipment, Training, and Exercises.

5.2.2 Funding the Private Sector

The extent of current guidance from DHS/ODP states that government "grantees are encouraged to collaborate with the private sector to leverage private sector initiatives, resources, and capabilities. Since critical infrastructure is often privately-owned and operated, enhancing public/private partnerships will help identify and advocate opportunities for coordination."[8] The actual distribution of DHS funds to private organizations from government grantees has not been expressly addressed by DHS.

As past precedent, however, DHS has allocated funds to the private sector in some situations. Under the 2004 DHS Appropriations Bill (Senate Report 108-086), private Emergency Medical Service providers became eligible for grants by becoming included in the definition of the emergency response community so long as they are part of a state's emergency preparedness and response plans. Furthermore, DHS has provided direct funding to private companies in situations related to port security, air transportation, and research and development (e.g., the Small Business Innovative Research Grant).

[8] From the U.S. Department of Homeland Security *Fiscal Year 2005 Homeland Security Grant Program Guidelines and Application Kit*.

In the absence of specific DHS guidance on this subject, Region 6, in coordination with the SAA, intends to facilitate the development of individual compacts between itself and private sector entities to address severe CIP needs using DHS or other grant dollars.

Region 6 has successfully distributed equipment and resources to the private sector under a variety of grant programs in the past and will use the same approach for the allocation of Homeland Security and CIP grants based on its priorities as determined in Section 5.1.4. Beyond DHS, grant dollars are available from other sources including multiple Federal Departments (e.g., Department of Health and Human Services, Department of Energy, etc.), and State grant programs. Depending on the sector and the CIP need, Region 6 will allocate funds to private sector entities using the appropriate grant vehicle.