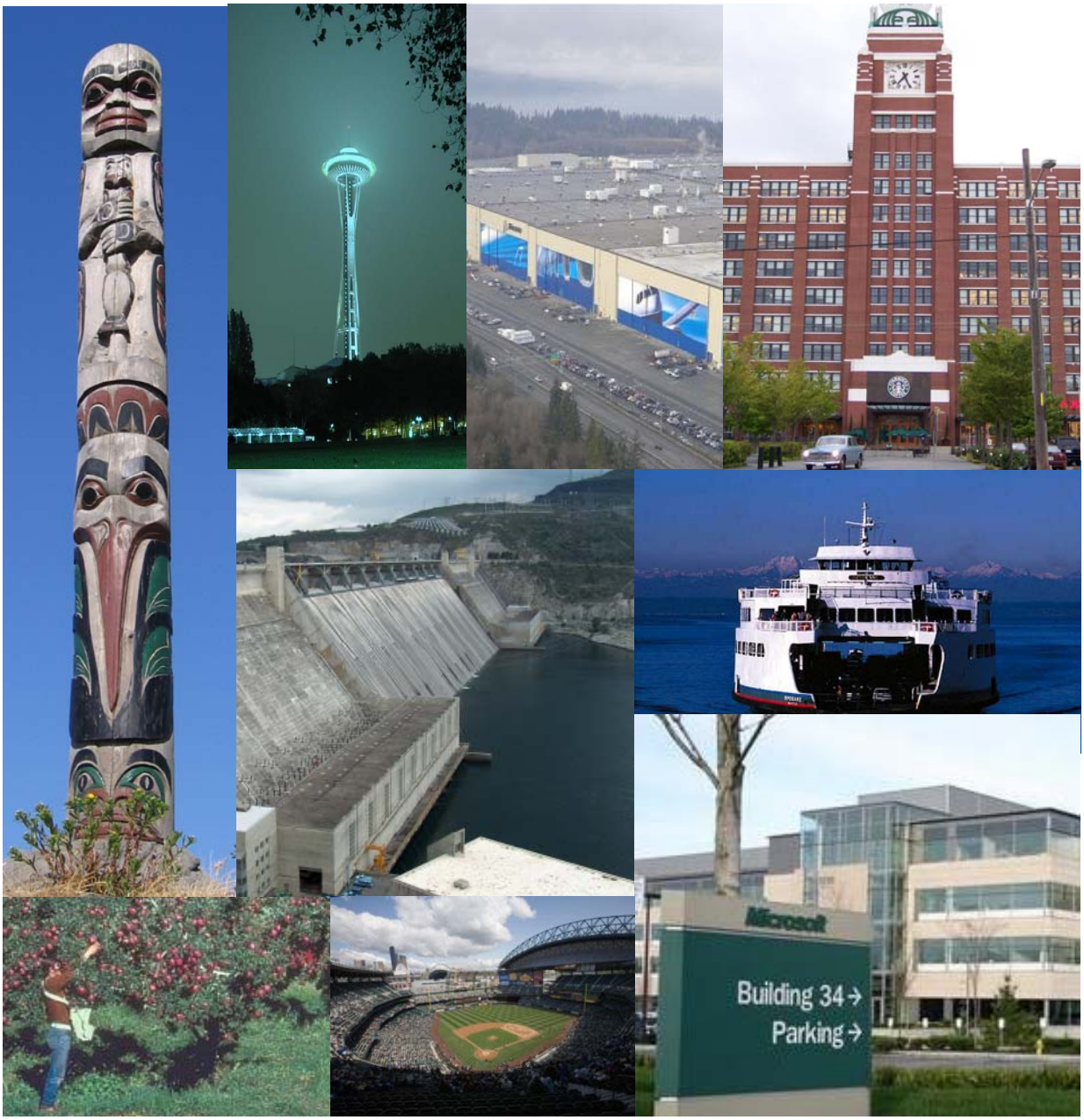
Washington Infrastructure Protection Plan



February 2008

FOREWORD

The Washington State Military Department sincerely appreciates the cooperation and support from those public and privates sector agencies, departments, and local jurisdictions that contributed to the development of the *Washington State Infrastructure Protection Plan* (WIPP). Coordination of the WIPP represents a committed and concerted effort by the public and private sectors to support the national critical infrastructure protection efforts addressed in Homeland Security Presidential Directive 7. It establishes the framework for collection of accurate facilities data used to identify, map, assess vulnerability, and protect critical infrastructure and key resources through State Sector Coordinating Councils and Sector Specific Plans.

We developed the WIPP through the synergistic efforts of the Washington Homeland Security Regional Leads and Coordinators, Washington State Emergency Management Association, Northwest Tribal Emergency Management Council, Washington State Attorney General's Office, Washington State Office of Financial Management, Washington Emergency Management Council, Washington Committee on Homeland Security, Washington Domestic Security Executive Group, Pacific Northwest Economic Region, Pacific Northwest Alert and Warning Network, and the public and private sector leads of the 17 sectors represented on the Committee for Homeland Security Infrastructure Protection Sub-Committee who participated in a two year effort to develop and refine this plan.

The *Washington Infrastructure Protection Plan* is one of the many efforts to be better prepared for emergencies, disasters, and terrorist attacks. It moves the state one step closer to being able to minimize the impacts of those and other events on the people, property, economy, and environment of Washington State.

Timothy J. Lowenberg
Major General
The Adjutant General
Washington State Military Department

James M. Mullen
Director
Emergency Management Division
Washington State Military Department

February 2008

VISION STATEMENT

Resilient infrastructure supports delivery of essential services throughout the state

MISSION STATEMENT

Work with our public and private sector partners to identify and protect critical infrastructure and key resources against all hazards

END STATE

Infrastructure that is resilient to all hazards

Preface

”No critical infrastructure is self-sufficient. The complexity inherent in the interdependent nature of infrastructure systems complicates planning and preparedness for system failures. Recent wide-scale disruption of infrastructure on the Gulf Coast and Pacific Northwest due to weather, in the Northeast due to electric power network failures, and infrastructure failures in the Midwest dramatically illustrates the problems associated with mitigating cascading effects and responding to cascading infrastructure failures once they have occurred. The major challenge associated with preparedness for cascading failures is that they transcend system, corporate, and political boundaries and necessitate coordination [two way sharing of information] among multiple, disparate experts and authorities.”[1]

Protecting infrastructure from attacks and disruptions is an essential first step, and the *Washington Infrastructure Protection Plan (WIPP)* is a guide to work towards this goal. The WIPP is modeled largely on the National Infrastructure Protection Plan and customized to meet the needs of Washington State stakeholders.

At the same time, there is recognition that protection is not enough to keep all-hazards disasters and incidents from occurring. There must be a focus on developing resilient communities and building resilience into critical infrastructures and essential service providers and organizations on which they depend. This means looking beyond protection and security to how to deal with incidents and disasters that go beyond single-point failures and impact interdependent infrastructure systems.

Understanding interdependencies is a major challenge, which Washington State public and private sector stakeholders and other organizations have been working in partnership these last few years to address in working groups, workshops and exercises. This will necessitate a sustained, regional, cross-jurisdiction, cross-sector integrated approach to address these linkages, identify readiness gaps, and develop and implement risk-based solutions. In this regard, the WIPP, like its federal counterpart, should be considered a “living document” that will, in later versions, incorporate new lessons learned and best practices that address both protecting our infrastructures against significant, all-hazards threats and incidents, and on how to expeditiously recover and restore critical service if the unthinkable happens.

[1] Dr. George H. Baker, Institute for Infrastructure and Information Assurance, James Madison University, May 16, 2007.

Table of Contents

List of Appendices

Sector Specific Annexes
Published Separately by IPSC Sector Coordinating Councils

Suggestions / Corrections Submission Form

Fill in your name, title, agency, mailing address, telephone number, fax number and e-mail address. There are two review sections (1) Basic Plan and (2) Appendices. Fill in the blanks regarding the location of information in the plan being reviewed. Attach marked-up copies to this sheet with suggested changes for each of the sections. Make other suggestions or comments in the space provided below. Add extra sheets as necessary. Thank you for your contribution and taking the time to make the next WIPP even better.

Mail to:

Manager
Planning, Analysis, and Logistics Section
Emergency Management Division
Washington Military Department
Building 20 MS: TA-20
Camp Murray, WA 98430-5122
Or e-mail to: j.ufford@emd.wa.gov

Name: _____ Title: _____ Agency: _____

Address: _____

City: _____ State: _____ Zip: _____ -- _____

Telephone: (_____) _____ Fax: (_____) _____

Email address: _____

Basic Plan: _____ Appendices: _____ Other: _____

Chapter: _____ Section: _____ Paragraph: _____ Figure: _____

Suggestion or Comments:

Record of Revisions

Change #	Date Entered	Contents of Change	Initials
Change 1	12 March 08	Addition of Sector 18, Critical Manufacturing to Page iv, Table of Contents Page 2, Basic Plan Page 1-A-7, Tab A, Appendix 1, Washington State Sectors Defined Page 1-B-2, Tab B, Appendix 1, State and Federal Sector Lead Agencies Page 1-D-5, Tab D, Appendix 1, Sector Coordinating Councils (SCC) and Sector Specific Plans (SSP) Page 2-5, Appendix 2, Washington State Infrastructure Taxonomy	jp

Distribution

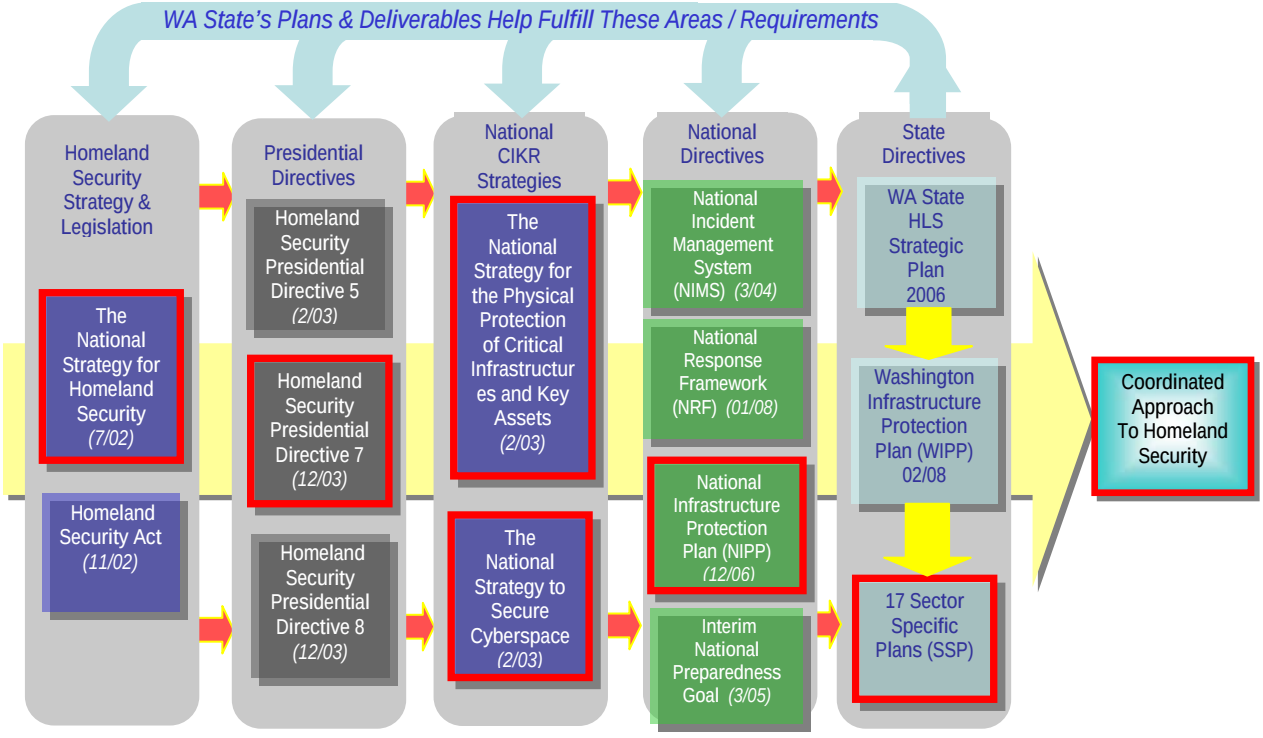
Distribution of this Plan is through the internet as a PDF document to all who may desire a copy at http://emd.wa.gov/plans/plans_index.shtml under Related Links, Plans.

Introduction

Critical Infrastructure and Key Resources (CIKR) owned and operated by the public and private sectors support the delivery of critical/essential services. This is essential to the State's security, public health and safety, economic vitality and way of life. CIKR includes the assets, systems, networks and functions that provide vital services to the State, Pacific Northwest, and the Nation. Emergencies, natural hazards and terrorist attacks on CIKR could significantly disrupt those activities, produce cascading effects and result in large-scale human suffering, property destruction, economic loss, and damage public confidence and morale.

A safe and secure Washington is everyone's responsibility. Protecting CIKR and/or minimizing the impacts of emergencies and disasters, including terrorist attacks on CIKR is essential for making the State safer, more secure and resilient to the threat of any natural or manmade hazard. Protection includes actions to detect, prevent, deter or mitigate the affects of such events. Protection can include a wide range of activities such as improving business protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce safety programs or implementing cyber security measures, among others. The Washington Infrastructure Protection Plan (WIPP) and its supporting Sector Specific Plans (SSPs) draw upon statutory mandates, Presidential Directives, and Federal and State strategies to provide a medium for integrating protection strategies for the present and future.

Homeland Security Strategic Framework



Purpose:

Infrastructure protection is a continuous process with multiple intersecting elements, dependencies and interdependencies that cross and crisscross jurisdictional and natural boundaries. The WIPP and supporting SSPs bring together the voluntary efforts of all levels of government, private sector and non-governmental organizations. Together they provide the mechanism for identifying critical assets, systems, networks and functions; understanding threats; assessing vulnerabilities and consequences; prioritizing protection initiatives; and enhancing information sharing efforts and applying protective measures within and across sectors.

The WIPP will evolve in accordance with changes to the National Infrastructure Protection Plan (NIPP), threat environment and evolving strategies and technology.

Scope:

The WIPP employs an all-hazards approach to identify and protect CIKR with statewide, regional or national implications that if lost or disrupted, regardless of the cause, would have a significant and detrimental impact. Protection of CIKR is primarily the responsibility of its owner/operators with government support as necessary.

The Plan also addresses the identification and protection of CIKR located in other states or Canadian Provinces that have a direct impact on the people, economy, environment and property of Washington.

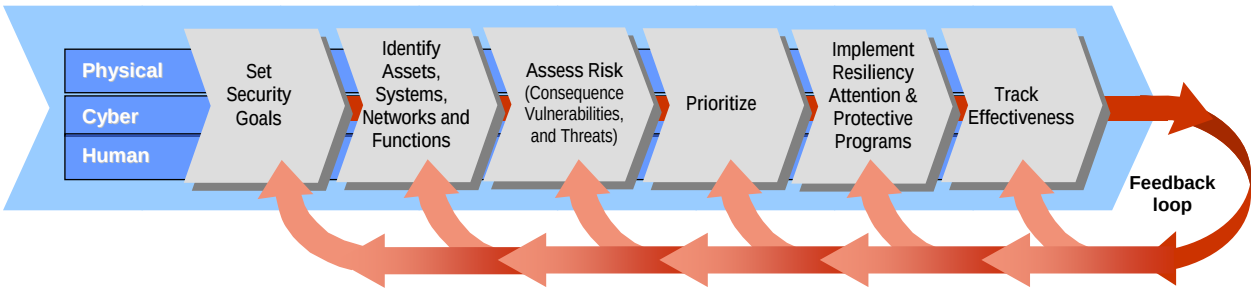
The WIPP, and more specifically the state level SSPs, addresses ongoing and future activities within each of the 18 CIKR sectors, the processes and mechanisms used to prioritize CIKR protection and the interconnectedness of networks and systems upon which the state depends.

Additionally, the WIPP recognizes the importance of these interdependencies and the need for achieving resilience for CIKR and the regions in which they are located, and lays the foundation for building the cross-sector mechanisms, approaches, and solutions to move towards this goal.

Applicability:

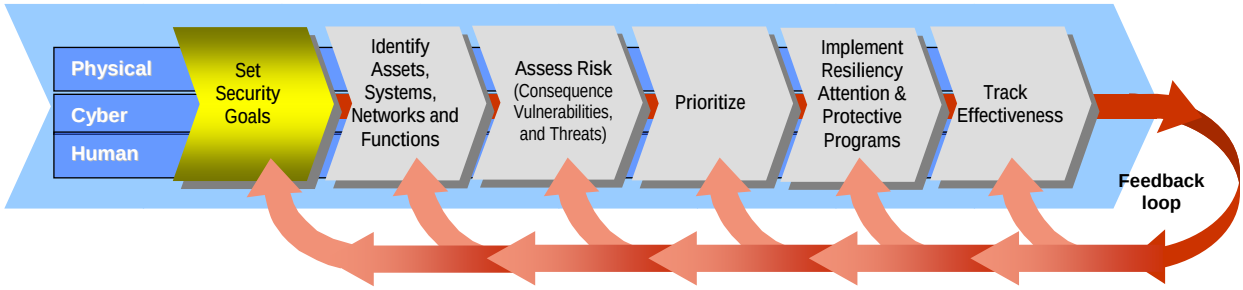
This plan applies to all CIKR within the State and in some instances to CIKR outside the State that has a direct impact on the people, economy, environment and property of Washington. It also applies to all owners, operators, investors, employees and volunteers who frequent, support, purchase, occupy or in any way deal with infrastructure at any level within the State.

1. Risk Management Framework



The Washington Infrastructure Protection Plan (WIPP) parallels the NIPP framework with some variations which are identified herein. Risk is generally defined as the combination of the frequency of occurrence, vulnerability, and the consequence of a specified hazardous event. In the context of the WIPP and NIPP, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) as a result of terrorist attack, natural disaster or other incident, along with the likelihood of such an event occurring and causing the loss. The risk management framework establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk that drives CIKR protection activities. The framework applies to the general threat environment, as well as to specific threats or incidents. Alternative models are not widely accepted or in use for terrorism related threats. Therefore, the WIPP and NIPP currently provide a conventional and augmented framework for the terrorist incident related threat analysis. A more detailed discussion of managing risk is located in Chapter 3 of the NIPP, The Protection Program Strategy: Managing Risk.

Set Security Goals



The Washington Statewide Homeland Security Strategy identifies the statewide CIKR goals and objectives. The state Committee on Homeland Security's (CHS) Strategy Development Working Group defines the goals in the Statewide Homeland Security Strategic Plan with input from State Agencies, public and private sectors and stakeholders. The CIKR goals and objectives are periodically updated and are located in the current *Washington Statewide Homeland Security Strategic Plan*. Additionally, public and private sector partners may refine these goals and

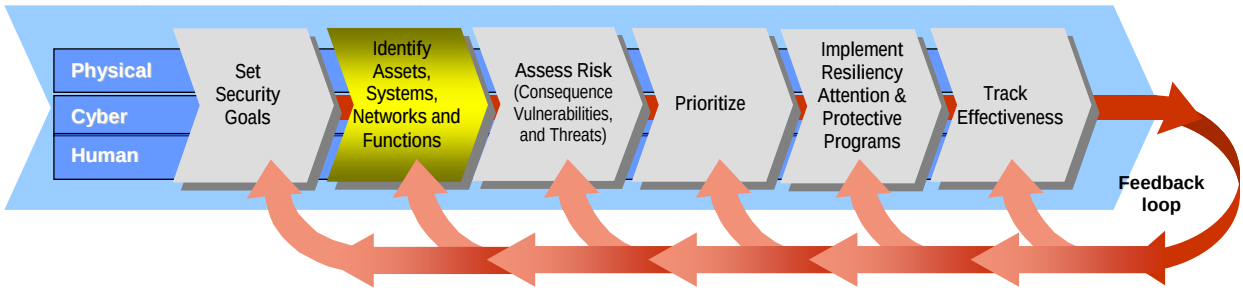
objectives as they apply to their specific sector. The intent is to maintain and sustain critical and essential services that support a normal way of life for the citizens of Washington State.

From a sector perspective, security goals and their supporting objectives do four things:

- Define the perspective and, if appropriate, the capability security partners should attain;
- Express this capability in terms of objective metrics and the timeline required to attain the capability through specific and supporting implementation steps;
- Consider distinct assets, systems, networks, operational processes, business environment, and risk management approaches; and
- Vary according to the specific business characteristics and security landscape of the affected sector, jurisdiction, or locality.

Taken collectively, these goals guide all levels of government and the private sector in tailoring programs and activities to address CIKR protection needs.

Identify Assets, Systems, Networks, and Functions with State Level Impact

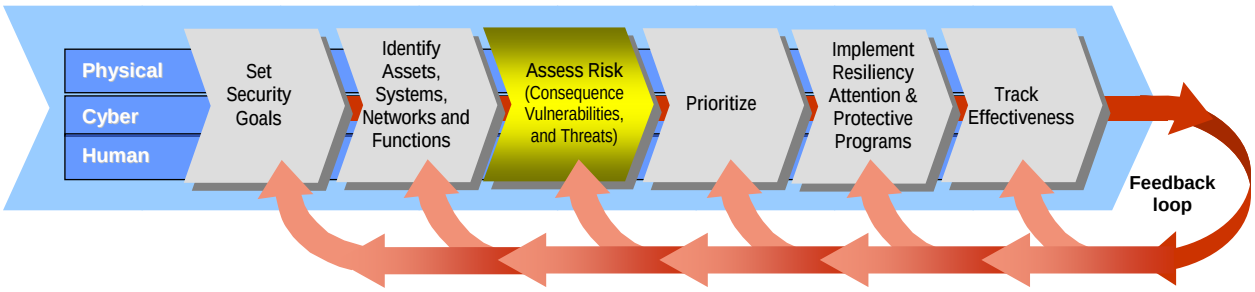


The state Committee on Homeland Security's Infrastructure Protection Sub-Committee (IPSC) utilizes Sector Specific Co-Leads representing public and private sector stakeholders to coordinate selection criteria and identify CIKR having a statewide or broader impact. Sector Specific Co-Leads coordinate criteria in quantifiable and qualifiable terms, to the extent possible. Sector specific criterion may be different for each sector due to the sector uniqueness and/or the prospective of the Sector Specific Co-Leads and their Sector Coordinating Council (SCC).

Sector inventory data is used to assess, plan, identify dependencies and interdependencies, and cascading effects in support of consequence planning.

Sector specific information for the most part is available though open sources such as the internet, annual reports, product flyers and advertisements. In the aggregate form this information becomes sensitive both to the individual site and, possibly, even to the industry as a whole. Consequently, control and access to sector inventories and their underlying data are closely managed. See Appendix 5, Public Disclosure and Security.

Assess Risk



The calculation for risk is based upon the following considerations and input from public and private sector stakeholders through the IPSC.

Risk = Consequence x Vulnerability x Threat

Consequence Also referred to as Impact is the negative effect on public health and safety, the economy, public confidence in institutions and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident. One way in which to gain an appreciation for impact is to envision it in the context of the acronym PEEP (People, Economy, Environment, Property). Below is a "PEEP Box" depicting categories, reporting agencies and impact areas.

IMPACTED COMPONENT	LEAD REPORTING AGENCY(IES)	EXAMPLE IMPACT AREAS
People	Department of Health Department of Health and Social Services Department of Licensing Washington State Patrol	Public Health, Special populations at risk Lives at risk or lost
Economy	Department of Employment Security Department of Revenue Office of the Insurance Commissioner Office of Financial Management Department of Community, Trade & Economic Development	Revenue lost and projected loss Jobs lost / affected
Environment	Department of Ecology Department of Agriculture Washington Department of Fish and Wildlife	Affects on air quality, water purity Affects on domestic animals and wildlife
Property	Department of General Administration Department of Revenue Recovery Section, EMD Department of Natural Resources Washington State Patrol	Loss of state facilities, Loss of revenue, Public and Private Sector Loss, Loss of state lands

Vulnerability The likelihood that a characteristic of or flaw in an asset, system or network's design, location, security posture, process or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or through other intentional

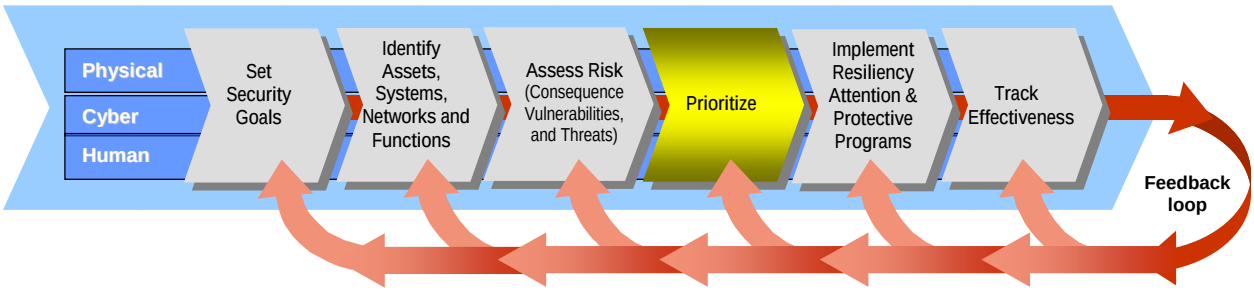
acts, mechanical failures and natural hazards. Vulnerability data can usually be found through owners and operators.

Threat The likelihood that a particular asset, system or network will suffer an attack or an incident. In the context of the risk of terrorism, the threat is based on the analysis of the intent and capability of an adversary. In the context of the risk of terrorism, the threat is based on the analysis of the intent and capability of an adversary; while the context of the threat of a natural disaster or accident is based on the probability of occurrence. Threat information sources are:

- Washington State Hazards Identification and Vulnerability Assessment (HIVA), 2003 (under revision)
- Washington State Hazard Mitigation Plan (Natural Hazards) 2005
- Washington Joint Analytical Center (WAJAC), current criminal and terrorist threat data
- Local law enforcement agencies
- United States Public Private Partnership (usp3)
- Northwest Warning, Alert and Response Network (NWWARN)
- Sector Information Sharing and Analysis Centers (ISAC)

DHS provides resources to assist in the assessment effort such as the Buffer Zone Protection Program (BZPP), Site Assistance Visits (SAV), and training programs that support CIKR protection. Additional resources can be found in Appendix 3B of the National Infrastructure Protection Plan (NIPP) http://www.dhs.gov/xlibrary/ assets/ NIPP_Plan.pdf.

Prioritize CIKR

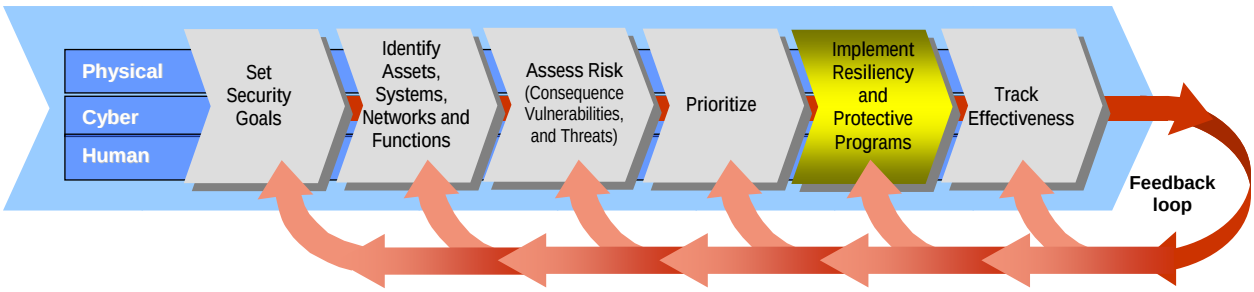


The prioritization of CIKR is primarily utilized for informed decision making having a statewide, regional, national, and/or international impact. Prioritization is used to focus planning, foster coordination, and support effective resource allocation decisions during incident response and restoration activities. The IPSC prioritizes CIKR having a statewide or broader impact. Prioritization is accomplished through the IPSC Prioritization Working Group in collaboration with the Sector Coordinating Councils. This activity is conducted periodically to provide decision makers options for consideration in the allocation of resources. The framework is applicable to risk assessment on an asset, system, network, function, sector, city, county,

university campus, port, state, regional or national basis. Comparing the risk profile for different entities helps identify interdependencies, where risk mitigation is most pressing and to subsequently determine the most cost-effective protective actions, including those related to the cyber and human elements of CIKR. This in turn identifies which CIKR should be given priority for protection and which alternative protective actions represent the best investment based on risk. The prioritization process also provides information that can be used during incident response to help decision makers establish CIKR restoration priorities.

The Infrastructure Protection Sub-Committee (IPSC) uses terrorism, natural disaster, and emergency generated scenarios to identify and prioritize CIKR in the context of ever changing criteria having a statewide impact. Once the highest priority CIKR is identified, options for consideration are provided to decision makers on how to best protect CIKR whose loss or incapacitation would negatively impact the people, economy, environment, or property (PEEP) of the state or result in widespread denial of services in either the public or private sector. A standing list of prioritized CIKR is not maintained over time because the identification and prioritization of CIKR is an ongoing process based upon risk (Risk = Consequence x Vulnerability x Threat) and its fluctuating and changing components.

Implement Resiliency and Protective Programs



The risk assessment and prioritization processes provided the owners and operators of CIKR an opportunity to identify options for enhancing current protection programs where they can realize the greatest cost benefit. A new consideration in this equation is the concept of resiliency. It is not always possible to prevent or mitigate the impacts of disruptions in operations or service no matter whether the cause is natural or human in origin, but it may be possible to lessen the impact and retain the ability to continue business, albeit, at a lesser but acceptable level. Owners, operators and local jurisdiction officials are responsible for implementing mitigation and protective measures. Resources must be directed to areas of greatest priority to enable effective management of risk. By definition, all CIKR assets, systems and networks are important. However, the risk factors of consequences, vulnerability and threat dictate that some assets, systems, networks or functions are more critical than others at certain times and under certain circumstances.

Resiliency Continuum

- Critical Infrastructure / Key Resources Identification
- Critical Infrastructure Protection Plans
  - National
  - State
- Sector Specific Plans
  - National
  - State
- Risk Assessments
- Continuity of Government (COG) Plans
- Continuity of Operations Plans (COOP)
- Comprehensive Emergency Mgmt. Plans (CEMP)
- Business Continuity Plans
  - Essential Functions
  - Vital Services
  - Disaster Recovery

- Deter an event from happening;
- Devalue a target by making it less attractive or too costly to attack;
- Detect an aggressor planning or committing an attack, or the presence of a hazardous device or weapon; and
- Defend against attack by delaying or preventing an aggressor's movement toward the asset, or the use of weapons and explosives.
- Mitigate vulnerabilities or minimize consequences associated with a terrorist attack or other incident

It is generally more cost effective to build resiliency and security into assets, systems and networks than to retrofit. Preventive and protective measures include actions to mitigate the overall risk to CIKR assets, systems, networks, functions, and/or their interconnecting links from the effects of exposure, injury, destruction, incapacitation or exploitation. In the context of the WIPP and NIPP, this includes actions to deter the threat, mitigate vulnerabilities or minimize consequences associated with a terrorist attack or other incident. Protection, which is primarily an owner / law enforcement responsibility, includes a wide range of activities, such as hardening facilities, building resiliency, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting work force surety programs, implementing cyber security measures and comparable initiatives.

> "Resiliency is defined as the capacity of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must." Science: 12 August 2005.

Resilience, by its nature, is based on assessed risk. It can be measured, unlike protection, which is defensive in focus and begs the question —"how much is enough?" Moreover, protection can't be assured despite all the resources that may be poured into preventative, defensive and offensive measures. Meaning sooner or later it will fail.

Critical infrastructure resilience and more broadly, regional disaster resilience, requires a different way of thinking about preparing for and managing disasters, including terrorist attacks, that falls outside of traditional emergency and security plans. Achieving resilience requires a comprehensive, all-hazards, cross-sector, grassroots-to-national level, integrated approach. It

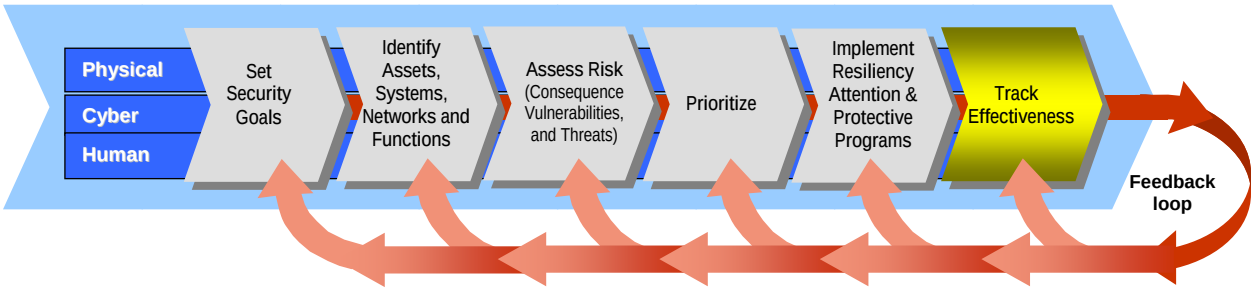
requires cooperation and coordination of key public-private and non-profit stakeholders that have responsibilities or vested interests in improving regional preparedness.

Regional Resilience

Since the September 11th attacks, local, regional, and cross-sector cooperative initiatives have focused on resilience. Increasingly, initiatives come from many sources: business groups, local or state governments, economic development associations or other non-profit entities. Some of the more productive initiatives focus on regional infrastructure interdependencies. These initiatives are unique in that they include as many of the "key stakeholder' organizations with regional responsibilities for essential services or a significant vested interest in regional disaster resilience. They include utilities, commercial businesses (manufacturing, agriculture and food industries, information technology services companies and defense contractors, as well as associations that represent different business interests), nonprofits, community institutions such as schools and churches, academic institutions, and numerous local and state government agencies and regional federal facilities—civilian and defense installations. Law enforcement and other first responder organizations are actively involved, and, in some cases, local and state political officials.

Examples of these interdependencies-focused regional collaborative initiatives are in the Pacific Northwest (the five state-three Canadian jurisdiction Pacific Northwest Partnership for Regional Infrastructure Security and the Puget Sound Partnership for Regional Infrastructure Security); the Washington State Homeland Security Regions, Infrastructure Protection Sub-Committee, and the King County Region-wide Infrastructure Protection Program are well-organized with solid local and/or state government support. Most of these entities conducted interdependencies tabletop exercises and developed action plans to address lessons learned.

Track Effectiveness



Measuring effectiveness is a continuum influenced by technology, threat, resources, and numerous other factors. The end result is a resilient asset, system or network more secure from the impacts of emergencies and disasters, including terrorist attacks. One of the most common tools used to track effectiveness is the exercise. Each exercise type has advantages and disadvantages. Exercises range in the level of planning, training, cost and capability. Exercises are most effective when based upon quantifiable and qualifiable measures.

- **Descriptive Measures** help to understand sector resources and activities. They do not reflect protection performance. Examples include the number of facilities in a jurisdiction or site; the population within a given incident foot print; and the number, nature and location of suppliers in the infrastructure's supply chain.

- **Process (Output) Measures** specific activities against a specific metric, track the progress of a task or report the output of a process. They also demonstrate whether or not the activities performed are representative of progress toward the achievement of CIKR protection goals. Examples include the number of protective programs implemented in a specific fiscal year, the level of investment in each, the number of detection systems installed at a facility in a given sector, the proportion of the infrastructure's workforce that completed training, and the level of response to DHS and/or DHS sponsored data calls for asset information.

- **Outcome Measures** track progress toward a strategic goal through the achievement of beneficial results rather than level of activity. Over time process measures are deemphasized in favor of outcome measures. Examples include the reduction in risk measured by comparing one year of comparative analysis for a specific sector to another and the overall risk mitigation achieved by a particular protection initiative.

- **Ensuring an Effective, Efficient Program Over the Long** requires time to identify gaps and institute countermeasures / capabilities and reevaluate effectiveness. Four questions should be considered and designed into a program's regular review cycle to facilitate and enhance CIKR resiliency and protection activities on an on-going basis, The bottom-line in all fours questions is – *"Are we providing a continuing and evolving "Value-Proposition for public and private security partners?"*

1. Are we doing the right things?

	Did Not Meet	Nearly Met	Met	Exceeded
Are we focusing on the things that will make the most difference in resiliency and protection programs?	☐	☐	☐	☐
Will our program activities, time invested and/or level of effort support Washington Infrastructure Protection Plan (WIPP) and the goals of the Washington Statewide Homeland Security Strategic Plan?	☐	☐	☐	☐
Will our program activities, time invested and/or level of effort support our underlying Sector Specific Plans (SSPs)? (In what way?)	☐	☐	☐	☐
Will we be able to justify what we are doing with our Security Partners?	☐	☐	☐	☐

2. Are we doing things the right way?

	Did Not Meet	Nearly Met	Met	Exceeded
Are we following our Washington Infrastructure Protection Plan's (WIPP) guidelines and principles?	☐	☐	☐	☐
Are we following the National Infrastructure Protection Plan's (NIPP) directives, guidelines, and principles?	☐	☐	☐	☐
Are we ensuring that we will be able to deal with the *future demands* and *risks* to our State's Critical Infrastructure Key Resources (CIKR)?	☐	☐	☐	☐
Does this program and its activities provide leverage for future "timing" with other Federal or State initiatives? (Other Homeland Security opportunities?)	☐	☐	☐	☐
Are we (this program) aligned with other programs, e.g. NRP, NIMS, NIPP, ___, ___?	☐	☐	☐	☐

3. Are we doing things well?

	Did Not Meet	Nearly Met	Met	Exceeded
Do we deliver on commitments, when needed, within estimate / budget, with acceptable quality?	☐	☐	☐	☐
Are our program's Goals, Objectives, and "Action-Items" clearly defined, documented and communicated to Sector Leads?	☐	☐	☐	☐
To what extent have we communicated expectations and requirements to the executives and senior management of our Sector Leads?	☐	☐	☐	☐
Are our Goals and Objectives able to evolve incrementally over time? (Are we continually tracking and following up on our Action-Items?)	☐	☐	☐	☐
Will we be using iterative approaches to obtain our objectives and goals to minimize risks?	☐	☐	☐	☐

4. Are we getting full benefits?

	Did Not Meet	Nearly Met	Met	Exceeded
Are we delivering the full promise, outcomes and benefits for the level of efforts expended (our investment)?	☐	☐	☐	☐
Are we making substantive contributions to enhance the security of the most critical infrastructure in the State of Washington?	☐	☐	☐	☐
Are adequate and appropriate resources being assigned within the Sectors involved or affected?	☐	☐	☐	☐

Towards this end, infrastructure owners and operators should ensure that their assets and systems undergo vulnerability assessments (both physical and cyber), and use risk management to determine prudent prevention and mitigation measures to address impacts under various threat scenarios. These measures and procedures should be incorporated in continuity of operations and business continuity plans that take into account interdependencies with key suppliers and customers. Such measures and procedures could include backup and redundant systems, remote data storage, identification of key personnel and ways to backfill them, etc. Part of a comprehensive contingency strategy should include exercises and drills to test plans, raise awareness, and identify additional protection and preparedness needs on a regular basis. Where necessary, cooperative arrangements with key suppliers and customers should be developed that provide cost-effective security and resiliency for supply chains and services. There also should be a management strategy to ensure availably of, and access to, critical equipment, materials, components and products, including those from cross-border or off-shore sources, in the event of a major disruption or disaster.

To facilitate the above, infrastructure owners and operators should take an active role in local and regional public-private partnerships where they exist and work with their state and local government representatives to create regional collaborations in communities where they do not exist in order to foster disaster resilience. For example, the Partnership for Regional Infrastructure Security provides a cross-sector venue and mechanism for stakeholders in this regard. The Partnership has held four regional infrastructure interdependencies exercises thus far—the Blue Cascades Series—and developed an integrated Action Plan of projects to address lessons learned with stakeholder working groups implementing many of these activities.

- **Education, Training and Exercises:** Responders, emergency and security managers, owners and operators and other CIKR practitioners must ensure that skilled and knowledgeable professionals provide opportunities to understand their infrastructure related responsibilities through training, exercises and other educational forums, conferences, and seminars. Public and private sector owners and operators should implement a security/emergency management briefing/training program that explains CIP goals and objectives, COOP/BCP and other organization plans, and identifies all hazards/risks to the respective organizations.

- **Technology:** Technology can be used to enhance current capabilities and in some instances lower the cost of existing capabilities so that security partners can afford to do more with limited resources.

- **WIPP Updates and Revisions:** The WIPP is available on the Washington Emergency Management Division Website (http://emd.wa.gov). Recommended changes may be submitted online at any time to the Infrastructure Program Office (IPO) IPO@emd.wa.gov) . To remain a viable tool the WIPP will be placed on a recurring review / update schedule parallel to the Washington State Comprehensive Emergency Management Plan (CEMP). However, changes in threats, technology, policies and exercise after-action reports may require more frequent updates. Administration of the WIPP is the responsibility of the EMD IPO.

2. Organizing and Partnering for CIKR Protection

Infrastructure Protection Sub-Committee: The Infrastructure Protection Sub-Committee (IPSC) of the state Committee on Homeland Security (CHS) is responsible for identifying, mapping, assessing and protecting the State's critical infrastructure and key resources (CIKR). This venture incorporates public and private sector co-leads, representation from the Washington Joint Analytical Center (WAJAC), Washington Association of Sheriffs and Police Chiefs (WASPC), Washington State Emergency Management Association (WSEMA), Pacific Northwest Economic Region (PNWER), FBI Fusion Center, DHS Security Protective Security Advisor (PSA), Pacific Northwest National Laboratory (PNNL), and security specialists. Each sector is encouraged to develop a public-private Sector Coordinating Council (SCC) to collaborate and develop a consensus approach to pursing and achieving their sector's CIKR goals.

State-Level Coordination: The EMD IPO produces the WIPP through extensive coordination and collaboration with the IPSC and CIKR stakeholders. The IPO also assists the Sector Co-Leads in developing their Sector Specific Plan (SSP), provides overarching CIP guidance and interfaces with adjacent States and the Department of Homeland Security on CIKR related matters.

Automated Critical Asset Management System (ACAMS): ACAMS is a federal DHS owned and sponsored secure, online database that allows for the input of CIKR asset information, the cataloging, screening, and sorting this data, the production of several reports, and a variety of inquiries useful to the strategic planner and the tactical commander. ACAMS is also PCII protected to ensure that all information submitted to and contained within the system is protected from public release under the Freedom of Information Act (FOIA). Data contained within ACAMS can only be viewed and edited by those authorized State and/or local jurisdictions that have entered and vetted the CIKR asset information, while all data contained within ACAMS can be viewed nationally by DHS and other designated Federal personnel who have a need to know. The system brings jurisdictions into alignment with the NIPP, and acts as a force multiplier as jurisdictions utilize the tool that facilitates public/private partnerships in the development of the assessment process and working partnerships in protecting critical assets. ACAMS is available free of charge to those with public safety responsibilities who have a need to know, receive appropriate instruction and authorization, and comply with Protected Critical Infrastructure Information (PCII) guidelines. The Washington State Infrastructure Protection Office uses ACAMS to store CI Information

Cross Border and International Coordination: Washington State is somewhat unique in that it shares contiguous borders with other states and Canada. Consequently, initiatives to identify, map, assess and protect CIKR outside the State having a direct impact on Washington's economy, environment, property or people is of significant interest. Private/public sector owners/operators and stakeholders have a vested interest in CIKR activities outside the State in which a dependency or interdependency exists and should coordinate related issues through their Sector Coordinating Councils and/or the IPSC. The EMD IPO coordinates directly with British

Columbia and the Department of Homeland Security on behalf of the IPSC for CIKR issues of common concern.

Sector Partnership Coordination: Sector Co-Leads are highly encouraged to develop and foster public-private Sector Coordinating Councils (SCC) similar to those used at the federal level and identified in the National Infrastructure Protection Plan. Due to the unique nature of the IPSC these SCC may be

- Combined public-private councils (CPP),
- State, local, tribal government coordinating councils (SLTGCC),
- Private sector coordinating councils (PSCC), or
- Existing committees, professional organizations with broad sector representation or some other equivalent.

The intent is to ensure the broadest representation in every sector in the state's CIP processes and IPSC. All sectors should have representation from their respective public and private partners and ensure inclusion of the non-profit, not-for-profit and volunteer organizations associated with their sector. In some instances these forums already exist.

Information Sharing: Effective implementation of the WIPP relies on active participation by public and private security partners at all levels in a multi-directional information sharing medium. Forums like US Computer Emergency Readiness Team (US CERT), US Public Private Partnership (USP3), InfraGard, The Infrastructure Security Partnership (TISP), Northwest Warning, Alert and Response Network (NWWARN) and Infrastructure Protection Sub-Committee File Transfer Protocol (IPSC FTP), are examples of such information sharing opportunities available to the State's CIKR stakeholders.

CIKR Data Security: The EMD Infrastructure Program Office (IPO) staff have been trained through the federal DHS PCII (Protected Critical Infrastructure Information) Program Office to handle information consistent with the federal PCII standards, have been accredited to PCII Standards, and are inspected annually to maintain PCII certification. The EMD IPO will apply federal PCII security standards to the receipt, handling, transmission, storage, dissemination and destruction of all CI/KR data.

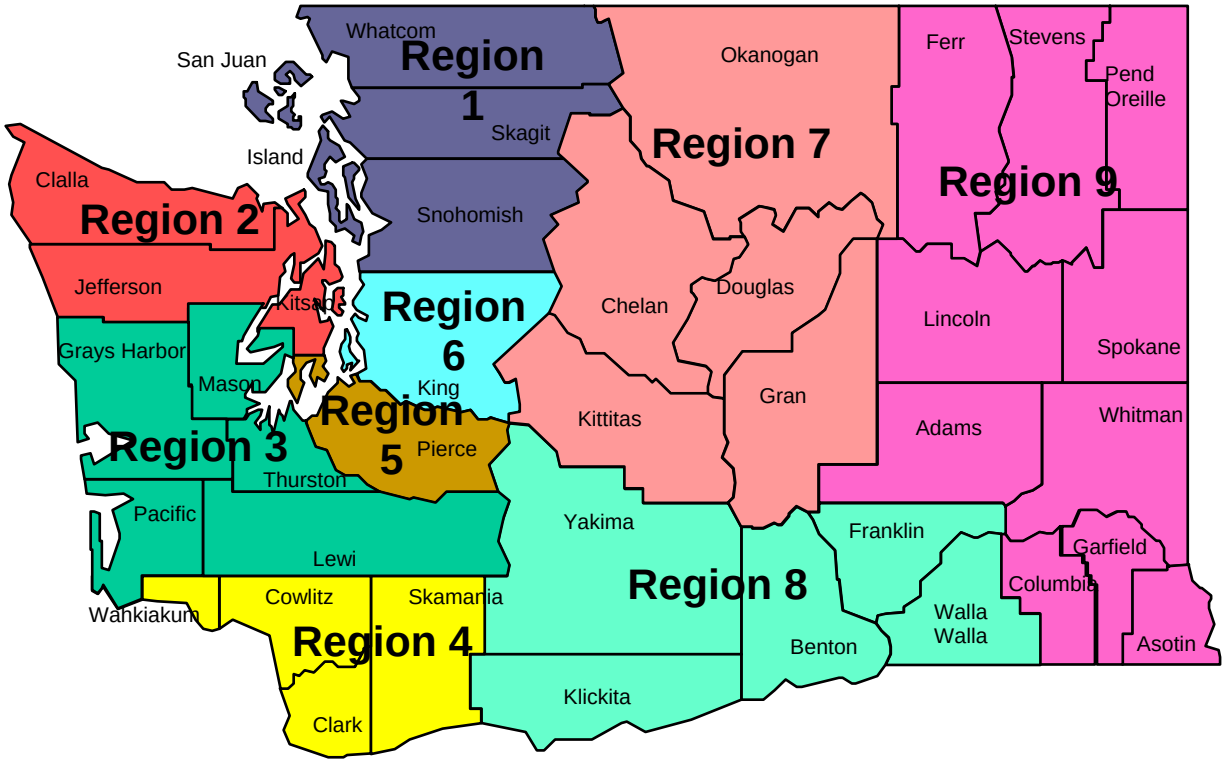
3. CIKR Protection Program Resources

Federal resources allocated for CIKR protection and mitigation efforts are more and more sector specific in their focus and are centered on the Risk-Based Resource Allocation Process identified in Chapter 7 of the NIPP, 2006. Additionally some resources may become available through the State Homeland Security Office on a competitive basis. Guidance regarding access to these resources is published separately and can be found at http://emd.wa.gov/5-prog/wahsas/hls-grant-process.htm.

DHS Federal Grants: The Grant Programs Directorate (GPD) is responsible for providing training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance and other support to assist states and local jurisdictions to prevent, respond to and recover from acts of terrorism. GPD annually publishes a consolidated Infrastructure Protection Programs grant program guidance document which targets specific industries, CIKR sectors or commodity areas. Grant guidance changes annually.

State Grants and Resources: State CIKR related grants are limited in nature and are most often federal funds/resources administered through the EMD Homeland Security Section utilizing federal grant guidance. In some instances there are resources besides dollars that can be used to meet CIKR goals. Local and tribal jurisdictions should coordinate with the IPSC through their State Homeland Security Region or Washington State Emergency Management Agency (WSEMA) representatives, both of whom serve as Organization Representatives on the IPSC. Organization Representatives should coordinate with Sector Co-Leads to identify possible resources when developing infrastructure protection plans. Mitigation grants may, at times, be available to lessen the impacts of emergencies, disasters and terrorist attacks on CIKR. Such grants should be pursued through the local emergency management agency to determine eligibility requirements. Other state agencies may also be able to provide assistance for certain projects, see Appendix 1, Tab B, State and Federal Sector Lead Agencies.

Washington State Homeland Security Regional Grants: Each of the nine Washington State Homeland Security Regions receives Department of Homeland Security (DHS) funding through the State that may be used at the regional and local level to identify, map, assess and protect local jurisdictional and tribal CIKR.



Note: Homeland Security Regions coincide with Local Health Regions for Public Health Emergency Planning and Coordination.

Critical Incident Planning and Mapping System (CIPMS): This program, enacted by the Washington State Legislature, provides for the "Tactical Mapping" of all schools and government buildings in the state. CIPMS is administered through the Washington Association of Sheriffs and Police Chiefs (WASPC) and incorporates a DHS Buffer Zone Planning component. For additional information on how CIPMS can be used to support local CIP efforts, contact WASPC at (360) 486-2380 or view their website at http://www.waspc.org/.

Other Federal Grants: Occasionally federal agencies, other than DHS, will make funds available for very specific CIKR purposes. In the past these have been very specific and of short duration. Guidance is published by the sponsoring agency and often distributed directly to the affected sectors/facilities without notifying the State Homeland Security Office. These programs are available to a wide range of grant recipients, including CIKR owners and operators and State, Local and Tribal governments.

Acronyms and Abbreviations

ACAMS	Automated Critical Asset Management System
BZP	Buffer Zone Program or Buffer Zone Plan
BZPP	Buffer Zone Protection Plan
CAPRA	Critical Asset & Portfolio Risk Analysis
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability
CARVER2	Criticality, Accessibility, Recoverability, Vulnerability, Espyability, Redundancy, 2
CEMP	Comprehensive Emergency Management Plan
CHS	Committee on Homeland Security
CIPMS	Critical Incident Planning and Mapping System
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CIKR	Critical Infrastructure Key Resources
COG	Continuity of Government
COOP	Continuity of Operations
CPP	Combined Public-Private Councils
CWIN	Critical Infrastructure Warning Information Network
DHS	Department of Homeland Security
DIS	Department of Information Systems, Washington
EMD	Emergency Management Division, Washington Military Department
EPA	Environmental Protection Agency
EPCRA	Emergency Planning & Community Right-to-Know Act

FAA	Federal Aviation Administration
FOIA	Freedom of Information Act
FOUO	For Official Use Only
G&T	Grants and Training (now OGP)
GCC	Government Coordinating Council
GPD	Grant Programs Directorate
HIVA	Hazards Identification and Vulnerability Assessment
HLS	Homeland Security
HLS-CAM	Homeland Security-Comprehensive Assessment Model
HSAS	Homeland Security Advisory System
HSPD	Homeland Security Presidential Directive
IA	Office of Information and Analysis
IP	Office of Infrastructure Protection
IPD	Infrastructure Partnerships Division (Department of Homeland Security)
IPO	Infrastructure Program Office (Emergency Management Division)
IPSC	Infrastructure Protection Sub-Committee
IPSC FTP	Infrastructure Protection Sub-Committee File Transfer Protocol
ISAC	Information Sharing and Analysis Center
IT	Information Technology
LEPC	Local Emergency Planning Committee
LE-VAT	Law Enforcement-Vulnerability Assessment Team
MARSEC 1, 2, 3	Marine Security Level 1, 2, or 3
MSHARRPP+V	Mission, Symbolism, History, Accessibility, Recognizability, Recoverability, Population, Proximity, Vulnerability

NADB	National Asset Database
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NRP	National Response Plan
NWWARN	Northwest Warning, Alert and Response Network
OPSEC	Operational Security
Pair-PM	Pair-Wise Methodology plus Program Management
PCII	Protected Critical Infrastructure Information
PNEMA	Pacific Northwest Emergency Management Arrangement
PNWER	Pacific Northwest Economic Region
PPICC	Public-Private Infrastructure Coordinating Council
PSA	Protective Security Advisor
PSCC	Private Sector Coordinating Councils
RAM	Risk Assessment Methodology
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RCW	Revised Code of Washington
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SCADA	Supervisory Control and Data Acquisition
SERC	State Emergency Response Commission
SLTGCC	State, Local, Tribal Government Coordinating Councils
SSA	Sector Specific Agency
SSI	Sensitive Security Information

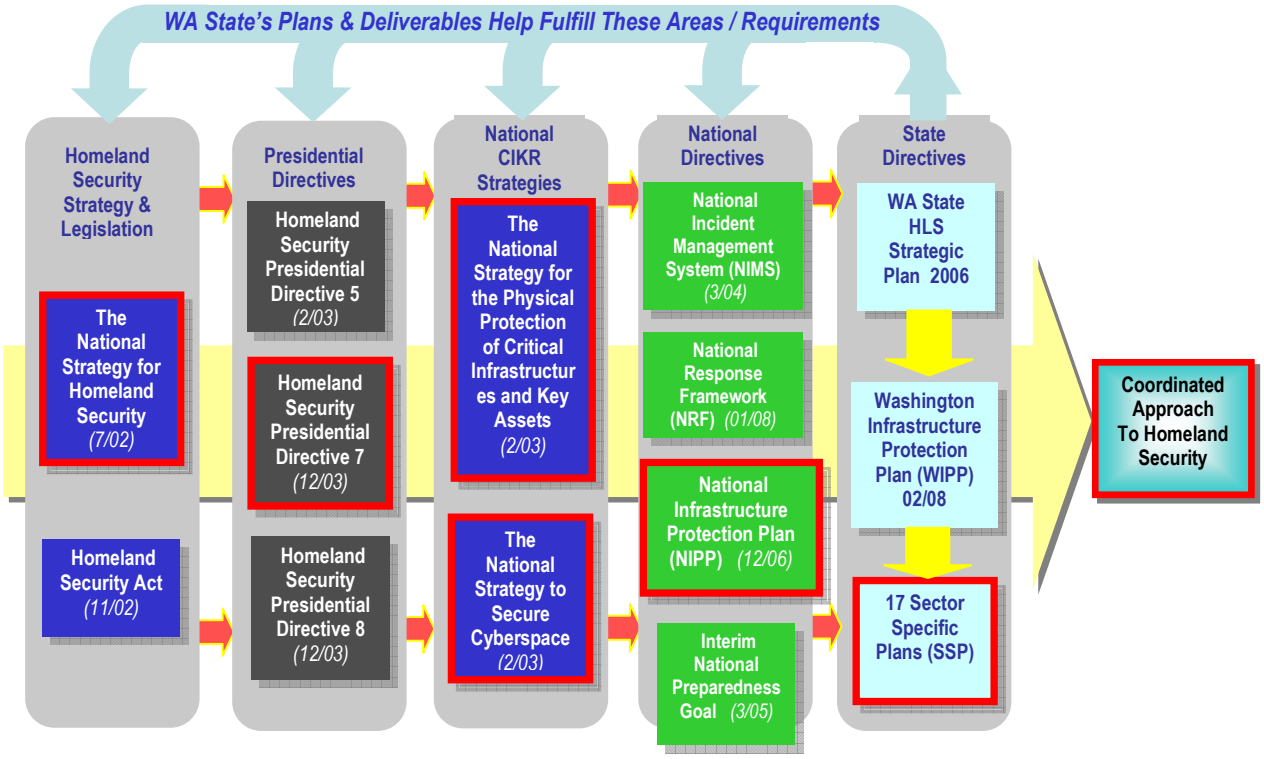
SSP	Sector Specific Plan
SWAT	Special Weapons and Tactics
TISP	The Infrastructure Security Partnership
UASI	Urban Area Security Initiative
US CERT	United States Computer Emergency Readiness Team
USP3	United States Public Private Partnership
VATS	Vessel and Terminal Security
VRPP	Vulnerability Reduction Purchase Plan
VSAT	Vulnerability Self Assessment Tool
WA	Washington
WAJAC	Washington Joint Analytical Center
WSEMA	Washington State Emergency Management Association
WASPC	Washington Association of Sheriffs and Police Chiefs
WIPP	Washington Infrastructure Protection Plan
WMD	Washington Military Department or Weapon(s) of Mass Destruction, depending on context
WSP	Washington State Patrol

Appendix 1
Authorities, Roles and Responsibilities

The Homeland Security Act of 2002, Public Law 107-296, provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the nation's Critical Infrastructure Key Resources (CIKR). The Act assigns DHS the responsibility to develop a comprehensive national plan for securing CIKR and recommending measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government in cooperation with State, local, and tribal government authorities, the private sector and other entities.

The *Washington Statewide Homeland Security Strategic Plan* is the basis for the state Critical Infrastructure Protection (CIP) Program and the structure the Washington Infrastructure Protection Plan.

Homeland Security Strategic Framework



Major General Lowenberg, The Adjutant General, Director, Washington Military Department, states in his preface to the 2005 Edition of the Washington Statewide Homeland Security Strategic Plan:

> "Our collaborative efforts provide a statewide system capable of responding to major disaster events and meeting the expectations of the national preparedness goals articulated in Homeland Security Presidential Directive (HSPD) – 8, The National Infrastructure Plan (HSPD-7), and National Incident Management System (NIMS) implementation of HSPD -5. Work towards these initiatives increases our overall all-hazards response capability and preparedness.

Guiding this process is the Washington Statewide Homeland Security Strategic Plan with implementing action plans, business plans, and progress updates. The strategic planning process provides a framework through which we will strengthen our ability to prevent, defend against, deter, respond to and recover from terrorist attacks, and natural or technological hazards in Washington."

Primary Roles and Responsibilities for CIKR security partners include:

Federal	State, Local and/or Tribal	
☒	☐	**Department of Homeland Security:** Manage the Nation's overall CIKR protection framework and oversee NIPP development and implementation.
☐	☒	**Washington Military Department**: Manage the State's overall CIKR protection framework and oversee WIPP development and implementation to maintain critical/essential services for Continuity of Government (COG), and Continuity of Operations (COOP).
☒	☒	**Sector Specific Agencies:** Implement the NIPP/WIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CIKR sectors in HSPD-7 to maintain critical/essential services for Continuity of Government (COG), and Continuity of Operations (COOP).
☒	☒	**Other Departments, Agencies, and Offices:** Implement specific CIKR protection roles designated in HSPD-7, *The Washington Statewide Homeland Security Strategic Plan*, or other relevant statutes, executive orders, and policy directives to maintain critical/essential services for Continuity of Government (COG), and Continuity of Operations (COOP).
☐	☒	**Local and Tribal Governments:** Develop and implement CIKR protective programs as a component of their overarching homeland security and emergency management programs.
☐	☒	**Dependent and Interdependent States and Provinces:** Partnership across jurisdictional and sector boundaries to address CIKR protection/resiliency issues within a defined geographical or service area.
☐	☒	**Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy or business oversight functions related to various aspects of CIKR operations and protection/resiliency within and across sectors and jurisdictions.
☒	☒	**Private Sector Owners and Operators:** Undertake CIKR protection, resiliency, restoration, coordination, and cooperation activities and provide advice, recommendations and subject matter expertise to the State, Local,

Tribal and Federal Government.

☐ ☒ **Emergency Management Council and Domestic Security Executive Group:** Provide advice, recommendations and expertise to the Governor and state agencies regarding protection policy and activities.

☒ ☒ **Academia and Research Centers:** Provide CIKR protection subject matter expertise, independent analysis, research and development and educational programs.

Noted below are the roles and responsibilities established in the ***Washington Infrastructure Protection Plan (WIPP)*** and stipulated in the ***2006 National Infrastructure Protection Plan (NIPP).***

X = Primary responsibility
+ = Milestone Indicator
n = @ National Level only
O = Support responsibility (may be required to qualify for grants)
NLT = No Later Than
OG/I = On-going/ Iterative

NIPP Chapter or Other Reference	Implementation Actions	Milestone				Security Partner							
		Work Plan Task #1	Work Plan Task #2	Work Plan Task #3	Specific Date	Washington State Infrastructure Program Office	Infrastructure Protection Sub-Committee	Sector Specific Agency (SSA) and supporting agencies	State IPSC Sector-Coordinating Council (SCC)	Private Sector	City, County, Tribal	Working Group 1	New 2
2	**AUTHORITIES, ROLES, AND RESPONSIBILITIES**												
2.1	Review WIPP and establish processes needed to support WIPP implementation.					X	X	X	X	X	X		
2.2	Incorporate WIPP into strategies for cooperation with foreign countries, dependent and interdependent states, and international / multinational organization.					X	O	X	X	O	O		
3	**THE PROTECTION PROGRAM STRATEGY: MANAGING RISK**												
3.1	Develop sector-specific CIKR inventory guidance.					X	X	O	X	O	O		
3.2	Review existing risk assessment methodologies to determine compatibility with the WIPP baseline criteria.					X	X	X	X	X	X		
3.3	Establish timeline for: (1) the development of sector-specific risk methodologies, and (2) for conducting consequence-based top-screening for all CIKR sectors.					X	X	O	X	O	O		

Top-Screening. Tool or process for conducing inspections and/or analysis to determine criticality of a facility and identify potential threats or hazards that could require further evaluation in the interest of national security.

NIPP Chapter or Other Reference	Implementation Actions	Milestone				Security Partner							
		Work Plan Task #1	Work Plan Task #2	Work Plan Task #3	Specific Date	Washington State Infrastructure Program Office	Infrastructure Protection Sub-Committee	Sector Specific Agency (SSA) and supporting agencies	State IPSC Sector-Coordinating Council (SCC)	Private Sector	City, County, Tribal	Working Group 1	New 2
3.4	Conduct and validate consequence assessments of priority CIKR as identified by the top-screening process.					X	X	X	X	X	X		
3.5	Conduct or facilitate vulnerability assessments in priority CIKR sectors and identify cross-sector vulnerabilities.					X	X	X	X	X	X		
3.6	Identify sector specific CIKR methodologies to support comprehensive risk assessments					O	O	O	X	X	O		
3.7	Provide guidance on metrics for annual reporting and national-level, cross-sector comparative analysis.					X	X	O	X	O	O		
4	**ORGANIZING AND PARTNERING FOR CIKR PROTECTION**												
4.1	Establish and maintain Sector Coordinating Councils, in accordance with the WIPP partnership model.					X	O	X	X	X	O		
4.2	Implement policies for vetting and distributing information to security, business continuity and emergency management partners through NWWARN, USP3 and the Washington State Regional Intelligence Fusion Center.					X	X	X	X	X	X		

X = Primary responsibility
+ = Milestone Indicator
n = @ National Level only
O = Support responsibility (may be required to qualify for grants)
NLT = No Later Than
OG/I = On-going/ Iterative

NIPP Chapter or Other Reference	Implementation Actions	Milestone				Security Partner							
		Work Plan Task #1	Work Plan Task #2	Work Plan Task #3	Specific Date	Washington State Infrastructure Program Office	Infrastructure Protection Sub-Committee	Sector Specific Agency (SSA)	State IPSC Sector-Coordinating Council (SCC)	Private Sector	City, County, Tribal	Working Group 1	New 2
4.3	Identify sector-level information-sharing mechanisms and ensure that information protection practices comply with appropriate guidance for protection of classified or sensitive information. Distribute PCII final rule.					X	X	X	X	X	O		
4.4	Develop Annual CIKR Protection Information Requirements Report.					X	O	O	X	O	O		
4.5	Work with the Department of Homeland Security to review the coordinating mechanisms for cross-border CIKR protection and/or information sharing to align with the NIPP.					X	O	O	O	O	O		
5	**INTEGRATING CIKR PROTECTION AS PART OF THE HOMELAND SECURITY MISSION**												
5.1	Coordinate SSP development in collaboration with security partners and submit to WA IPO with appropriate documentation of concurrence.					O	O	X	X	O	O		
5.2	Review and revise CIKR-related plans as needed to reinforce linkage between WIPP CIKR protection and NRP incident management requirements.					X	X	X	X	X	X		
5.3	Review current CIKR protection measures to ensure alignment with HSAS threat conditions and specific threat vectors/scenarios.					X	X	X	X	X	X		

X = Primary responsibility
+ = Milestone Indicator
n = @ National Level only
O = Support responsibility (may be required to qualify for grants)
NLT = No Later Than
OG/I = On-going/ Iterative

NIPP Chapter or Other Reference	Implementation Actions	Milestone				Security Partner							
		Work Plan Task #1	Work Plan Task #2	Work Plan Task #3	Specific Date	Washington State Infrastructure Program Office	Infrastructure Protection Sub-Committee	Sector Specific Agency (SSA)	State IPSC Sector-Coordinating Council (SCC)	Private Sector	City, County, Tribal	Working Group 1	New 2
6	**ENSURING AN EFFECTIVE, EFFICIENT PROGRAM OVER THE LONG RUN**												
6.1	Develop and implement a comprehensive state, local, tribal CIKR protection awareness program.					X	O	O	X	O	X		
6.2	Review and, as appropriate, revise training programs to ensure consistency with WIPP requirements.					X	X	X	X	X	X		
6.3	Provide initial WIPP training to security partners.					X	O	X	X	O	O		
6.4	Encourage CIKR protection and NIPP / NRP integration in state, local, and tribal exercises.					X	O	X	X	X	X		
6.5	Communicate requirements for CIKR-related R&D to National SCCs and GCCs for use in the national R&D planning effort.				July 1 (annually)	O	O	X	X	X	O		
6.6	Identify all databases, data services and sources, and modeling capabilities with CIKR application.					X	X	X	X	X	X		
6.7	Conduct review of the WIPP and SSPs annually in February.					X	X	X	X	X	X		
7	**PROVIDING RESOURCES FOR THE CIKR PROTECTION PROGRAM**												
7.1	Submit Sector CIKR Protection Annual Report to WA IPO.				July 1 (annually)	O	O	O	X	O	O		

X = Primary responsibility **O = Support responsibility (may be required to qualify for grants)**
+ = Milestone Indicator **NLT = No Later Than**
n = @ National Level only **OG/I = On-going/ Iterative**

NIPP Chapter or Other Reference	Implementation Actions	Milestone				Security Partner							
		Work Plan Task #1	Work Plan Task #2	Work Plan Task #3	Specific Date	Washington State Infrastructure Program Office	Infrastructure Protection Sub-Committee	Sector Specific Agency (SSA)	State IPSC Sector-Coordinating Council (SCC)	Private Sector	City, County, Tribal	Working Group 1	New 2
7.2	Submit State CIKR Protection Annual Report to the Governor.				July 1 (annually)	X	O	O	O	O	O		
7.3	Advise state, local, and tribal governments of SSA grant programs and/or other resources that can support NIPP/WIPP implementation.					X	O	X	O	X	O		
7.4	Apply for homeland security grants to address CIKR protection efforts per DHS/OGP guidance.				*	X	O	X	O	X	X		
8	**STATE IPSC WORK PLAN**												
8.1	Collaborate with Security Partners					O	O	X	X	X	O		
8.2	Establish Working Group for dependencies, interdependencies, and single-points-of-failure efforts					O	X	O	O	O	O		
8.3	Identify dependencies, interdependencies and single-points-of-failure					O	O	O	O	O	O	X	
8.4	Prioritize dependencies and interdependencies					O	X	O	O	O	O	X	

X = Primary responsibility **O = Support responsibility (may be required to qualify for grants)**
+ = Milestone Indicator **NLT = No Later Than**
n = @ National Level only **OG/I = On-going/ Iterative**

*Required application deadlines are specified within individual program guidance and may change annually. Dates for submitting grant applications, program requirements, and other required reports to DHS will be specified in annual grant program guidance and application kits. States will work with local and tribal jurisdictions to ensure compliance with all other related reporting requirements.

Tab A
Appendix 1
Washington State Sectors Defined

The following list identifies the state's critical infrastructure/key resource (CIKR) sectors

1 **Agriculture and Food** – Agriculture and related industries account for nearly 13 percent of the state's annual gross product. The state has approximately 37,000 farms producing over 300 commercial crops with a farm gate value of over $5.5 billion. Washington ranks number one in the United States for apples, red raspberries, corn for processing, concord grapes, sweet cherries, pears, tart cherries, lentils and hops; the state ranks second nationally for asparagus, processing peas, dry peas, apricots, fall potatoes and all grapes; and number three in the country for dry onions, trout, wheat, prunes, and plums. Agriculture and food includes supply chains for feed, animals and animal products; crop production and the supply chains for seed, fertilizer, and other necessary related materials; post-harvesting components of the food supply chain from processing, production, and packaging through storage and distribution to retail sales, institutional food services, and restaurant or home consumption.

2 **Banking and Finance** – Included here are physical banking and financial structures, wholesale banking operations, financial markets, regulatory institutions, physical repositories for documents and financial resources. Washington State has an extensive financial community with depository institutions and trust companies that in 2002 had over $102 billion in resources, over 100,000 firms/individuals providing securities investments and advice representing over $579 billion statewide, $5 billion in real estate secured loans and over $879 million in short-term, in-state loans. Statewide, there is a $19 billion insurance industry comprised of over 1,370 insurance companies, with 50 domestic insurers headquartered in the state.

3 **Chemical Industry and Hazardous Materials Industry** – The use of chemicals is a fundamental component of Washington State industry and infrastructure. The industry produces tens of thousands of products, ranging from basic commodities, such as ethylene and sulfuric acid to the most sophisticated drugs and highly specialized high-tech composites used in aircraft and spacecraft. The manufacture and distribution of chemicals occur on a daily basis and are required for all aspects of business and daily life. The economic and strategic value of the industry may make it an attractive target for terrorists. Each year businesses report the storage, processing, and planned and unplanned releases of chemicals or hazardous substances to the Washington State Emergency Response Commission (SERC) as required under the Emergency Planning & Community Right-to-Know Act. For example, in 2006, approximately 3,500 businesses reported 15,250 chemicals and products stored at 30,576 sites throughout Washington State. In a typical year about 300 facilities report nearly a thousand toxic chemicals via the Toxics Release

Inventory Report. This reported data includes 3,431 extremely hazardous substances that pose the greatest threat to human health and safety for the population of Washington State. Approximately 4,500 sites report annually their hazardous waste activities that include production of more than 281 million pounds of hazardous waste. These chemical products and waste are transported through major population centers on Washington State highways and by rail and waterway. The combined quantity of manufactured, processed, transported, and stored hazardous chemicals and waste present a significant threat to the people of Washington State. The threat of harm from a hazardous chemical release is present whether the release is accidental or an act of terrorism.

4 **Defense Industrial Base** – The "defense industrial base" refers to the systems and capability of industry to produce essential material to support national military objectives -- e.g., research & development, training tools, repair parts, ammunition, and chemical defense, food, medical, and fuel supplies. There are several defense contractors within Washington State that produce critical military equipment systems and supplies.

5 **Energy** – Washington State currently has an electricity generating capacity of 26,890 megawatts and generates approximately 97,841,300 megawatt-hours of electricity. The state leads the nation in both installed capacity and annual production of hydroelectricity. The system of dams within the state is key to this capacity. The electricity production in Washington State over the past years was generated in the following distribution, from the following sources: 73% by hydroelectric facilities, 17% by thermal resources, 8% by nuclear power plants, and 2% by renewable energy sources. This sector includes electricity-generating dams, power plants, transmission and distribution systems; oil production, crude oil transport, refining, product transport and distribution, and control and other external support systems; and natural gas exploration and production, transmission and local distribution.

6 **Emergency Services** – Across our nation, "people" are the most valuable emergency services resource. Washington State has over 100,000 professional and volunteer emergency responders in fire, rescue, emergency medical services, 9-1-1, law enforcement and emergency management who are vital to assuring the state's most critical homeland security capabilities. Washington State has 288 police departments, 39 sheriffs' offices, and 8 Washington State Patrol Districts. The state boasts 86 trauma receiving centers distributed throughout the Emergency Medical Services (EMS) system. The Puget Sound area is home to the Federal Emergency Management Administration's (FEMA) Urban Search and Rescue Task Force –1, a Disaster Medical Assistance Team (DMAT), two Metropolitan Medical Response Systems, the 10th Civil Support Team (CST) and Washington National Guard Chemical, Biological, Radiological, Nuclear and conventional High Yield Explosives (CBRNE) Enhanced Response Force Package (NGCERFP) for WMD response. Additionally, the Puget Sound region is designated as one of the 11 sites nationwide for the DHS Prepositioned Equipment Program (PEP).

7 **Information Technology --** The Information Technology (IT) Sector is a key enabler for the State, National and global economies. It is also highly diverse and cuts across all other critical infrastructure sectors. HSPD-7 identified IT as its own critical infrastructure sector, apart from the other sectors, to ensure that the IT industry, as owners and operators of critical products and services, receive the appropriate level of emphasis, commensurate with its risk exposure. By viewing IT as its own sector, the people, physical components, and cyber-based systems that make up the IT sector will receive the consideration necessary to identify and assess CIKR and implement strategic and tactical protective measures. Furthermore, asset classification and risk assessment techniques and methodologies useful in other sectors may not apply to the IT sector. Efforts are currently underway in public/private partnerships to focus on methods and techniques that allow for IT assets and key resources to be viewed in terms of function and capability versus traditional physical asset-focused methodologies.

The recently released Federal Information Processing Standards Publication (FIPS PUB) 199 – Standards for Security Categorization of Federal Information and Information Systems defines Information Technology as "any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information."

Through work conducted at the national IT SSP development process, the Sector identified six critical functions that characterize IT products and services[1]. They are:

- provide IT products and services;
- provide incident management capabilities;
- provide domain name resolution services;
- provide identity management and associated trust support services; and
- provide Internet routing, access and connection services.

These functions are distributed across a broad network of infrastructure and are managed on a proactive basis. These critical IT Sector functions are provided by a combination of entities – often owners and operators and their respective associations – who provide hardware, software, IT systems, and services. IT services include development, integration, operations, communications, and security. Due to the highly integrated nature of the IT Sector and convergence with Telecommunications, it can be difficult to neatly divide and understand the IT Sector.

[1] This differs from how the NIPP characterized the IT Sector. The NIPP perspective consists of seven sub-sectors: Hardware Production, Software Production, IT Service, Internet, Next Generation Networks, Regulatory, and other IT facilities. The NIPP reflects that each sub-sector has unique characteristics, operating models, responsibilities and stakeholders. The national IT SSP reflects the official sector position on the breakdown and characterization of the IT Sector.

8 **Telecommunications** – Voice and data services are vital for business operations and keeping citizens connected to government and each other. This "critical infrastructure" sector affects every resident because of its complex interdependencies and the magnitude of telecommunications and cyber systems within the state.

9 **Postal and Shipping** – The fundamental functions of postal and parcel-shipping organizations in the state economy, e.g., moving items from Point A to Point B, are unique and critical to the state economy. Although the sector's cargo operations are similar to those in the Transportation Sector, the Postal and Shipping Sector is distinct because of its unique activities, processes and facilities as well as the vastly different volumes of operation and customer base. The Postal and Shipping Sector is a primary mover of materials from individual-to-individual, business-to-individual and vice versa and business-to-business. It collects, transports and delivers information, merchandise, written communication and financial transactions. It transfers material as varied as correspondence in the form of cards, letters and packages; magazines and newspapers; and merchandise packaged for transport.

Some of the characteristics that differentiate Postal and Shipping from general cargo operations include:

- End-to-end integrated acceptance, processing, transportation and delivery;
- Large Daily volume;
- Very small- to medium-sized pieces;
- Massive, many-to-many (individual to individual, business to business, etc. relationships);
- Large customer base;
- Very large, centralized, high-volume automated or semi-automated processing facilities;
- Nation-wide (world-wide) networks (including facilities, not just destinations);
- Vast numbers and varieties of intake/collection points and retail operations; and
- Transportation accounts for only a fraction of the cost, effort/activity, and value added in the overall value chain.

10 **Healthcare and Public Health** – The Washington State Department of Health, the 35 local health jurisdictions, medical centers and hospitals, clinics, mental health facilities, long-term care facilities, nursing homes, blood-supply facilities and laboratories are key to the health and welfare of the state's population and visitors. As a whole, the healthcare and public health systems provide vital life saving emergency response capabilities to the state.

11 **Transportation** – The state transportation infrastructure includes aviation, maritime, rail, highways, pipelines and mass transit systems. There is a robust transportation system in Washington State, built upon a network of 20,083 miles of federal, state and local roads. Washington State has the nation's largest fleet of

ferries. The state is also served by approximately 2,075 route miles of Class I railroad track, 1,115 miles of track operated by 17 short-line railroads and two Amtrak Cascade trains. Ship and barge traffic transports imports and exports throughout the Puget Sound and the state's major river systems. Washington State has 127 public airports, three seaplane bases, Seattle-Tacoma and Spokane International Airports and a number of regional transportation airports.

The state is home to several ports vital to the inter-modal movement of cargo regionally, nationally and internationally. Washington has the largest controlled public port system in the world, 76 of which have marine terminals, barge facilities, industrial development, fuel depots, marinas, airports, railroad and military cargo capability. The Ports of Tacoma and Seattle are Washington State's largest seaports and, combined, they make up the second-largest U.S. container load complex in the nation, behind Los Angeles/Long Beach and ahead of New York/New Jersey. The Ports of Tacoma and Seattle import and export millions of containers with goods ranging from agriculture products to electronic equipment. Seattle has a large and growing cruise business, while Tacoma is one of 13 power projection gateways in the US that are vital to worldwide military operations. State ports handle seven percent of all U.S. exports and six percent of all imports representing over $100 billion in trade annually and adding to the state economy by creating one out of every four jobs in Washington State.

12 **Water and Wastewater** – Washington State has over 8,000 lakes, 40,000 rivers, 157 miles of open coastline and hundreds of miles of ground water aquifers. The water and wastewater infrastructure is made up of over 17,000 public water systems and over 300 public wastewater treatment facilities. Protection of the state water supply, drinking water and wastewater infrastructure is vital to public health, safety, recreation, agriculture, fire fighting capability and maintaining the viability of overall state economy.

13 **National Monuments & Icons** – This category includes historical attractions, monuments, cultural centers, nationally-prominent companies, commercial centers, sports stadiums, schools, universities, and parks and recreation areas.

14 **Commercial Assets** – Protecting prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions or enjoy recreational pastimes presents significant challenges. Day-to day protection of such facilities is the responsibility of their commercial owners and operators, in close cooperation with local law enforcement.

The likelihood of terrorists targeting and attacking any specific, prominent commercial facility or activity is difficult to determine. Potential terrorist attack methods range from conventional explosives to chemical, biological or radiological (CBR) weapons of mass destruction. Each facility's vulnerability to attack and/or natural disaster is unique and determined by its engineering design, size, age,

purpose and number of inhabitants. Commercial owners and operators must be responsible for assessing and mitigating their specific facility vulnerabilities and practicing prudent risk management and mitigating measures.

The collaboration between the state, local communities and commercial owners/operators is of vital importance in assuring the protection of business centers and gathering places.

Critical facilities are more vulnerable during special events such as visits by dignitaries, international meetings, conventions and major media attractions. Sporting events such as the World Series, Super Bowl, Basketball Championships, World Cup and Olympic Games provide excellent environments for terrorists to broadcast their causes.

15 **Government Facilities** – Major Army, Navy, Air Force, Coast Guard and National Guard facilities and installations are located with Washington State. These are strategically located to support and deploy forces worldwide, as well as to provide support for state missions. The military components provide employment for over 100,000 civilian and military personnel.

There is also federal government infrastructure in Washington State that is vital to state and national security. Washington State is home to the FEMA Region X Headquarters, the Federal Reserve Regional Headquarters, federal courthouses, Federal Aviation Administration (FAA) facilities and many other important entities.

Washington State government owns almost 11,000 buildings (approximately 5.3 million square feet) and leases over 11 million square feet, and employs over 102,000 people. In addition, local governments serve 39 county jurisdictions and over 281 cities.

Public education is a key component of our governmental capabilities and is comprised of nine Educations Service Districts, three independent districts, and 296 state school districts with over 2,200 school buildings. In addition to being a vital state resource that must be protected, schools provide significant capability as emergency response and recovery facilities for use as command centers, staging areas, shelters and recovery operations centers.

16 **Dams and Levees** – Some of the states' larger and more symbolic dams are major components of other critical infrastructure systems that provide water and electricity to large population areas, agricultural complexes, commercial and sport fishing activities and recreation. There are approximately 1,000 dams in Washington State. Most are small and their failure would not result in significant property damage or loss of life.

17 **Commercial Nuclear Reactors, Materials, and Waste** – The Columbia Generating Station represents about 12% of the state's electrical generation

capacity through the Bonneville Power Administration. Federal regulations require that commercial nuclear power plants maintain rigorous security programs to withstand an attack of specified adversarial strength and capability. Nuclear power plants are also among the most physically hardened structures in the country, designed to withstand extreme events such as hurricanes, tornadoes and earthquakes. Their reinforced engineering design provides inherent protection through such features as robust containment buildings, redundant safety systems and sheltered spent fuel storage facilities.

Significant security enhancements were implemented at the Columbia Generating Station in the aftermath of the September 11 attacks. Steps were taken to enhance surveillance, restrict site access control, physical security of the site, and coordination with law enforcement and military authorities. In addition to augmented security measures, all nuclear power plants have robust security and emergency response plans in place to further protect public health and safety in the unlikely event of a malicious act and/or radioactive release.

18 Critical Manufacturing – To be developed

Tab B
Appendix 1
State and Federal Sector Lead Agencies

Critical Infrastructure Key Resource Sector	State Lead Agency (ies)	Federal Lead Agency (ies)
1. Agriculture and Food	o WA Department of Agriculture	o Department of Agriculture o Department of Health and Human Services
2. Banking and Finance	o WA Department of Financial Institutions o Office of the Insurance Commissioner	o Department of the Treasury
3. Chemical and Hazardous Materials Industry	o WA Military Department, Emergency Management Division o WA Department of Ecology	o Department of Homeland Security, Office of Infrastructure Protection o Department of the Army (CSEP Program)
4. Defense Industrial Base	o WA Military Department	o US Department of Defense
5. Energy	o WA Department of Community Trade and Economic Development, Energy Office o Washington Utility and Transportation Commission	o US Department of Energy
6. Emergency Services	o Washington Association of Sheriffs and Police Chiefs o Washington State Association of Fire Chiefs	o Department of Homeland Security, Office of Infrastructure Protection
7. Information Technology	o WA Department of Information Services	o Department of Homeland Security, Office of Cyber Technology and Telecommunications
8. Telecommunications	o Washington Military Department, Emergency Management Division, Telecommunication Section	o Department of Homeland Security Office of Cyber Technology and Telecommunications o Department of Homeland Security, National Communications System
9. Postal and Shipping	o WA Department of General Administration, Campus Mail	o Department of Homeland Security, Transportation and Shipping, o United States Postal Service
10. Health and Public Health	o WA Department of Health o WA Department of Social and Health Services	o Department of Health and Human Services

11. Transportation	o WA State Department of Transportation o Washington Utility and Transportation Commission	o Transportation Security Administration o United States Coast Guard
12. Water and Wastewater	o WA Department of Health, Office of Drinking Water o WA Department of Ecology, Wastewater Management	o Environmental Protection Agency
13. Monuments and Icons	o WA Parks and Recreation	o Department of the Interior
14. Commercial Assets	o WA Military Department, Emergency Management Division	o Department of Homeland Security, Office of Infrastructure Protection
15. Government Facilities	o WA Department of General Administration o WA Military Department	o Immigration and Customs Enforcement o Federal Protective Service
16. Dam and Levees	o WA Department of Ecology, Dam Safety Program	o Department of Homeland Security, Office of Infrastructure Protection
17. Commercial Nuclear Reactors, Materials, and Waste	o Washington Military Department, Emergency Management Division o Department of Health Office of Radiation Protection o WA Department of Ecology	o Department of Homeland Security, Office of Infrastructure Protection o Nuclear Regulatory Commission o Department of Homeland Security, Federal Emergency Management Agency (REP Program)
18 Critical Manufacturing	o To be determined	o To be determined

Tab C
Appendix 1
Infrastructure Protection Sub-Committee

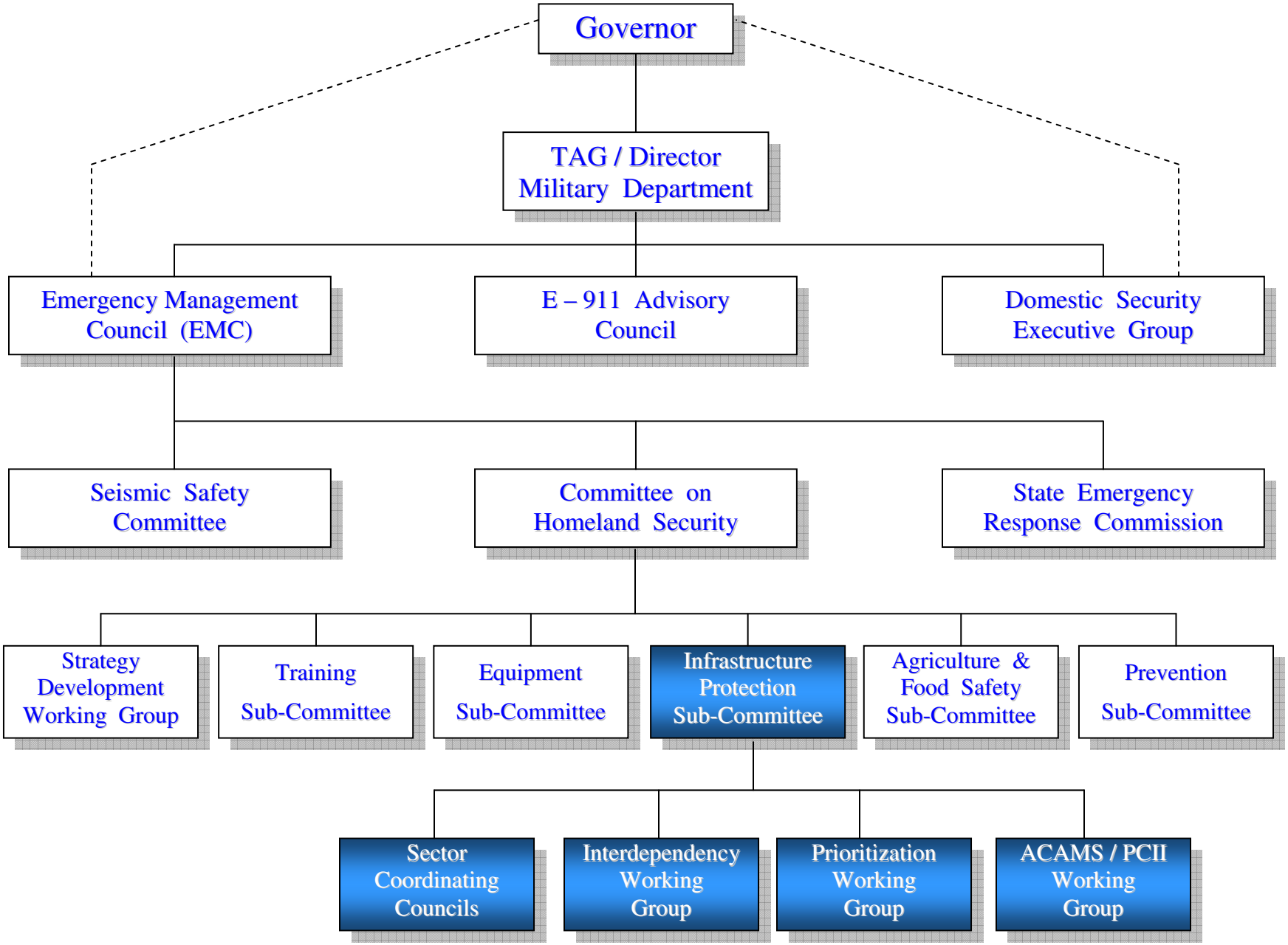
The Washington State Committee on Homeland Security (CHS) established and chartered the Infrastructure Protection Sub-Committee (IPSC) in June of 2004 with the mission of identifying, locating, assessing and protecting critical infrastructure (CI) within Washington State. The IPSC mission also includes the identification of dependencies and interdependencies within and outside the state such that the loss or incapacitation of any component thereof would have a negative impact on the continuity of government (COG), continuity of operations (COOP) and delivery of services within the State.

The Infrastructure Protection Sub-Committee (IPSC) provides the operational mechanism for carrying out the public-private partnership structure. The IPSC provides the framework for public and private owner and operator members of Sector Coordinating Councils (SCC) to engage in intra-government and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities.

Successful execution of the IPSC partnership structure requires an environment in which members of the SCCs can interact freely and share sensitive information and advice about threats, vulnerabilities, protective measures, and lessons learned. IPSC is the mechanism to allow meaningful dialogue on key critical infrastructure and key resource protection / resiliency issues and agreement on mutual action between government and owner / operator entities.

IPSC is a non-decisional body and includes sector members and government members. Sector members are the members of that sector's SCC that are owners and/or operators and the trade associations that represent them. Government members are the State, local and tribal government agencies (or their representative bodies) that comprise the oversight, regulatory, or statutory lead for each sector.

As portrayed in the diagram, IPSC consists of "Working Groups" and Sector Coordinating Councils (See Appendix 1, Tab D) that are composed of public and private sector representatives. For example, there is a Prioritization Working Group made up of IPSC Members (public and private) and IPSC Advisory members. The IPSC may convene or may even participate in joint working groups with other agencies on topics of common concern.


Governor
TAG / Director Military Department
Emergency Management Council (EMC)
E – 911 Advisory Council
Domestic Security Executive Group
Seismic Safety Committee
Committee on Homeland Security
State Emergency Response Commission
Strategy Development Working Group
Training Sub-Committee
Equipment Sub-Committee
Infrastructure Protection Sub-Committee
Agriculture & Food Safety Sub-Committee
Prevention Sub-Committee
Sector Coordinating Councils
Interdependency Working Group
Prioritization Working Group
ACAMS / PCII Working Group

Tab D
Appendix 1
Sector Coordinating Councils (SCC) and Sector Specific Plans (SSP)

Sector Coordinating Council

Vision

SCCs are an enabling mechanism for broad participation by public and private sector security partners, associations and other key sector stakeholders on a regular basis to consider critical issues relevant to Critical Infrastructure Protection (CIP) throughout the State of Washington.

Resiliency attention, incident prevention, and protection of the State of Washington's security, economy, public health, and safety across the various sectors (public and private), can only be actionable and effective when there is participation of public and private sector security partners.

Mission

The primary mission of a SCC is to bring together governments, private sector "sector-specific" companies, associations, and other key sector stakeholders on a regular basis to coordinate strategic activities and communicate broad sector member views associated with resiliency attention, infrastructure protection, response, and recovery that are broadly relevant to the Sector.

A purpose of any State of Washington SCC is to champion and represent a unique partnership and collaboration between each sector's public and private stakeholders as they leverage their unique capabilities to address the complex challenges of Critical Infrastructure Key Resources (CIKR) protection.

Functions

- Organization & Membership

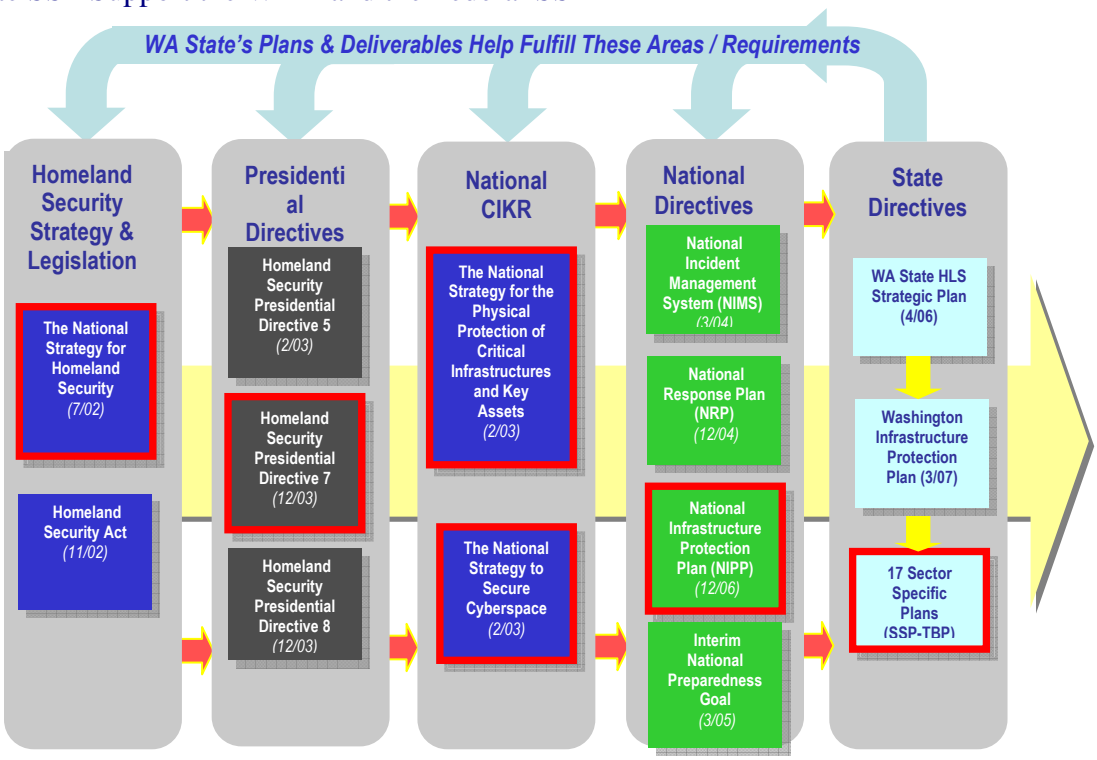
    - Self-organized, self-led, broadly representative of sector owners, operators and agency representatives within the private and public sectors for the particular sector
    - Co-chaired by a sector owner, operator and/or agency representative from the private and public sector, designated by the sector membership
    - Establish criteria for membership; however, membership should be representative of a broad base of sector owners, operators, associations and other entities--both large and small--within the particular sector
    - Seek broad participation and representation consistent with the diversity of the sector

- Roles & Responsibilities

  - Foster and/or facilitate sector-wide activities and initiatives designed to improve security
  - Focused on homeland security and critical infrastructure protection
  - Identify the sector's boundaries
  - Members of the SCC agree to work cooperatively to address the Sector critical infrastructure protection (CIP) in the state on an on-going basis
  - Establish the governance, business case and work processes for the sector coordinating council (SCC)
  - Principal entity for coordinating with the state on a wide range of CIKR protection activities and issues
  - Make the case for and interface with National SCC's on behalf of the state's particular sector
  - Assist in implementing the Washington Infrastructure Protection Plan (WIPP)
  - Enhance public confidence in the resiliency, reliability, and integrity of your sector's infrastructures, and services and security of information
  - Improve Sector coordination with other sector groups and government agencies in the State of Washington and potentially national. (National efforts could include working with national IT Sector members and other governments on CIP issues if appropriate.)
  - Focus on coordination and on strategy and Sector resiliency and protection issues, not on operational issues or performing those functions that fall under the information sharing and analysis roles (known and referred to as Operational Mechanisms)
  - Enable sector owners, operators and agency representatives to interact on a wide range of sector-specific strategies, policies, activities, and issues
  - Represent a primary point of entry for state into the sector for addressing the entire range of CIKR protection strategies, objectives, priorities, activities and issues for that particular sector
  - Serve as a strategic communications and coordination mechanism between CIKR owners, operators, suppliers and state during response and recovery, as determined by the sector
  - Identify, implement and support the information-sharing capabilities and mechanisms that are most appropriate for the sector, ISACs may perform this role if so designated by the SCC
  - Facilitate inclusive organization and coordination of the sector's policy development regarding CIKR protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements
  - Advise on integration of Federal, State, regional, and local planning with private sector initiatives
  - Provide input to the government (state and federal) on sector R&D efforts and requirements
  - Participate in voluntary consensus standards development efforts to ensure that sector perspectives are included in standards that affect CIKR protection
  - Collaborate with the Infrastructure Protection Sub-Committee (IPSC) Sector Co-Leads in developing and maintaining the State Sector Specific Plans in close collaboration with State, local, and tribal homeland security partners with key interests or expertise appropriate to the sector
  - Identify and disseminate sector/sub-sector best practices and lessons learned

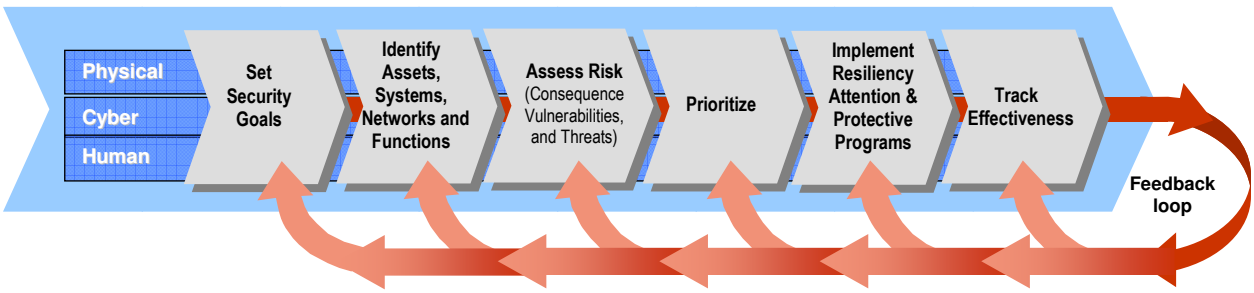
Sector Specific Plans (SSP)

Federal SSP Support the NIPP
State SSP Support the WIPP and the Federal SSP

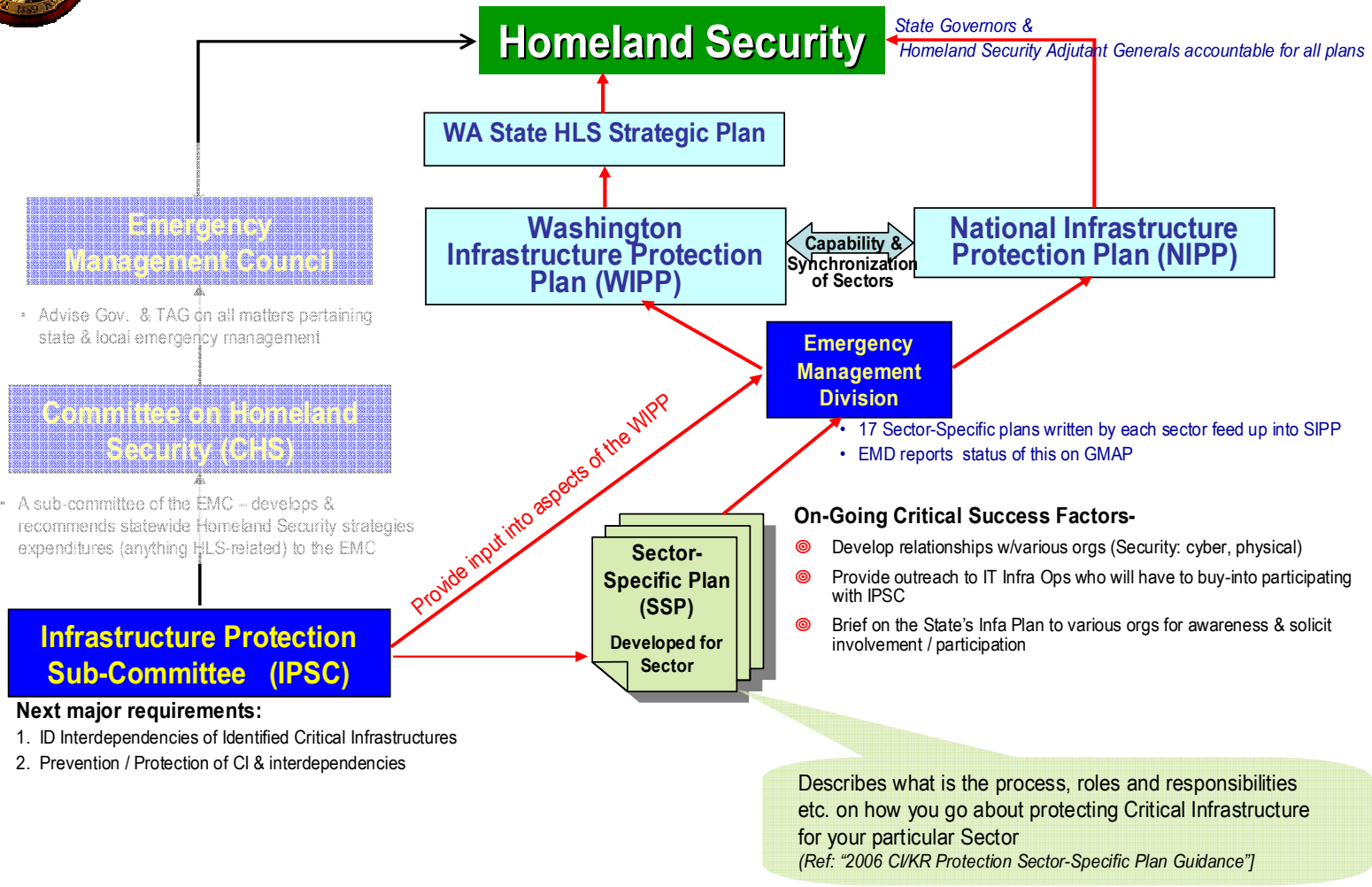


Each Sector Specific Plan should address the following issues as depicted below as they apply to their sector

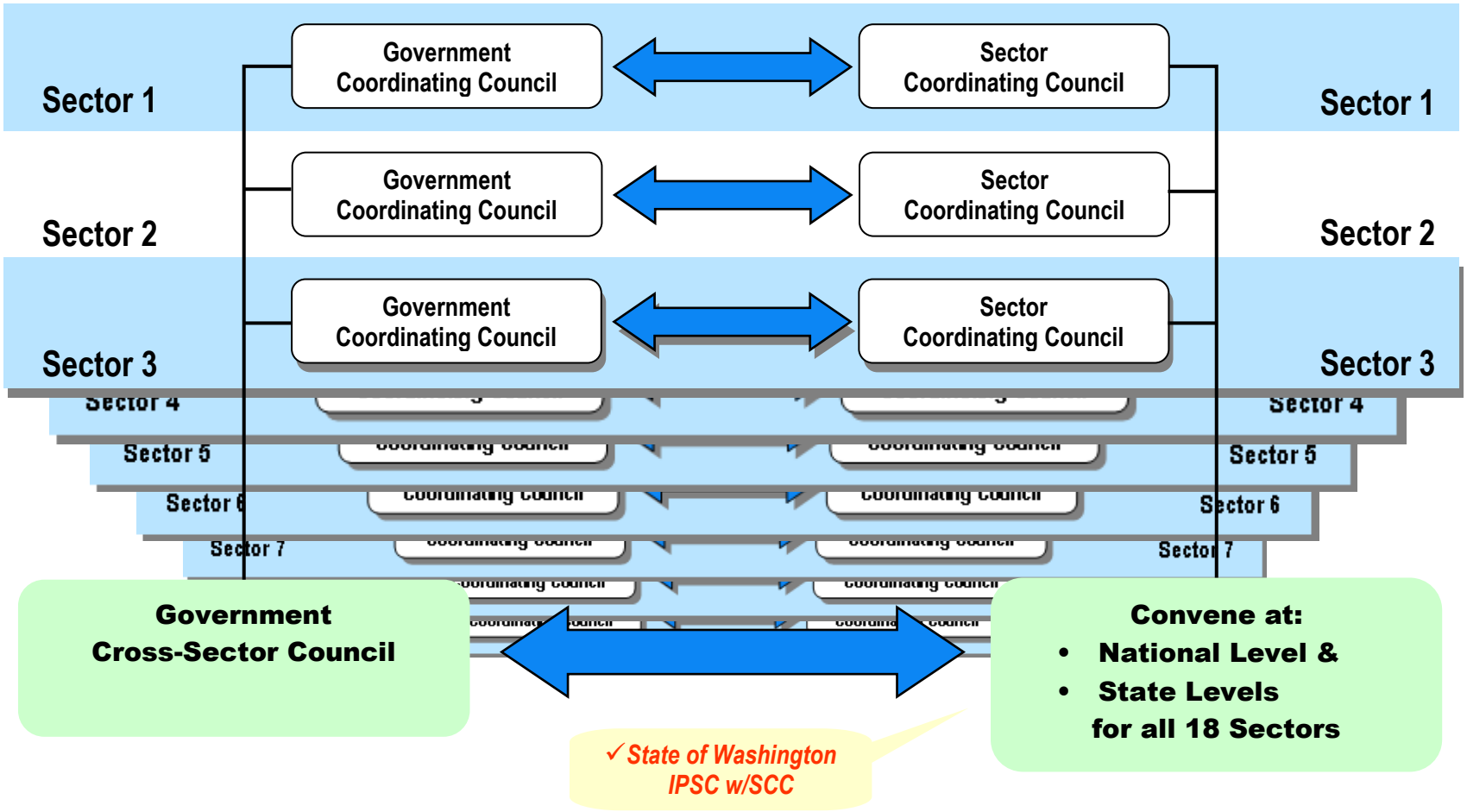
1. Define Sector and Partners (Public and Private) and establish goals
2. Identify Sector Components
3. Assess Risk
4. Prioritize
5. Resiliency Protection
6. Track Effectiveness



On IPSC & Relationships



Sector Partnership Model



Appendix 2
Washington State Infrastructure Taxonomy
(Based on US DHS Taxonomy, November 2006)

1. AGRICULTURE AND FOOD SECTOR
1.1 SUPPLY
1.2 PROCESSING / PACKAGING / PRODUCTION
1.3 AGRICULTURAL AND FOOD PRODUCT STORAGE
1.4 AGRICULTURAL AND FOOD PRODUCT TRANSPORTATION
1.5 AGRICULTURAL AND FOOD PRODUCT DISTRIBUTION
1.6 AGRICULTURE AND FOOD SUPPORTING FACILITIES
1.7 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
1.8 OTHER AGRICULTURE AND FOOD

2. BANKING AND FINANCE SECTOR
2.1 BANKING AND CREDIT
2.2 SECURITIES, COMMODITIES, AND FINANCIAL INVESTMENTS
2.3 INSURANCE CARRIERS

3. CHEMICAL AND HAZARDOUS MATERIALS INDUSTRY SECTOR
3.1 CHEMICAL MANUFACTURING PLANTS
3.2 HAZARDOUS CHEMICAL TRANSPORT
3.3 HAZARDOUS CHEMICAL STORAGE / STOCKPILE / UTILIZATION / DISTRIBUTION
3.4 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
3.5 OTHER HAZARDOUS CHEMICAL FACILITIES

4. DEFENSE INDUSTRIAL BASE SECTOR
4.1 SHIPBUILDING INDUSTRY
4.2 AIRCRAFT INDUSTRY
4.3 MISSILE INDUSTRY
4.4 SPACE INDUSTRY
4.5 COMBAT VEHICLE INDUSTRY
4.6 AMMUNITION INDUSTRY
4.7 WEAPONS INDUSTRY
4.8 TROOP SUPPORT INDUSTRY
4.9 INFORMATION TECHNOLOGY INDUSTRY
4.10 ELECTRONICS INDUSTRY
4.11 ELECTRICAL INDUSTRY COMMODITIES
4.12 ELECTRONIC INDUSTRY COMMODITIES
4.13 MECHANICAL INDUSTRY COMMODITIES
4.14 STRUCTURAL INDUSTRY COMMODITIES

5. ENERGY SECTOR
5.1 ELECTRICITY
5.2 PETROLEUM
5.3 NATURAL GAS
5.4 COAL
5.5 ETHANOL
5.6 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS

6. EMERGENCY SERVICES SECTOR
6.1 LAW ENFORCEMENT
6.2 FIRE, RESCUE, AND EMERGENCY SERVICES
6.3 SEARCH AND RESCUE
6.4 EMERGENCY MEDICAL SERVICES
6.5 EMERGENCY MANAGEMENT
6.6 OTHER EMERGENCY SERVICES

7. INFORMATION TECHNOLOGY SECTOR
7.1 HARDWARE PRODUCTION
7.2 SOFTWARE PRODUCTION
7.3 INFORMATION TECHNOLOGY SERVICES
7.4 INTERNET
7.5 NEXT GENERATION NETWORKS
7.6 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
7.7 OTHER INFORMATION TECHNOLOGY FACILITIES

8. TELECOMMUNICATIONS SECTOR
8.1 WIRED TELECOMMUNICATIONS
8.2 WIRELESS TELECOMMUNICATIONS
8.3 SATELLITE TELECOMMUNICATIONS
8.4 INTERNET
8.5 INFORMATION SERVICES
8.6 NEXT GENERATION NETWORKS
8.7 REGULATORY, OVERSIGHT, INDUSTRY ORGANIZATIONS
8.8 OTHER TELECOMMUNICATION FACILITIES

9. POSTAL AND SHIPPING SECTOR
9.1 U.S. POSTAL SERVICE
9.2 COURIERS
9.3 OTHER POSTAL AND SHIPPING

10. HEALTHCARE AND PUBLIC HEALTH SECTOR

10.1 DIRECT PATIENT HEALTHCARE
10.2 PUBLIC HEALTH AGENCIES
10.3 HEALTHCARE EDUCATIONAL FACILITIES
10.4 HEALTH SUPPORTING FACILITIES
10.5 END-OF-LIFE FACILITIES
10.6 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
10.7 OTHER HEALTHCARE AND PUBLIC HEALTH FACILITIES

11. TRANSPORTATION SECTOR

11.1 AVIATION
11.2 RAILROAD
11.3 ROAD
11.4 MARITIME
11.5 MASS TRANSIT
11.6 PIPELINES
11.7 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS

12. WATER AND WASTE WATER SECTOR

12.1 RAW WATER SUPPLY
12.2 RAW WATER TRANSMISSION
12.3 RAW WATER STORAGE
12.4 WATER TREATMENT FACILITIES
12.5 TREATED (FINISHED) WATER STORAGE
12.6 TREATED WATER DISTRIBUTION SYSTEMS
12.7 TREATED WATER MONITORING SYSTEMS
12.8 TREATED WATER DISTRIBUTION CONTROL CENTERS
12.9 WASTEWATER FACILITIES
12.10 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS

13. MONUMENTS AND ICONS SECTOR

13.1 NATIONAL MONUMENT/ICON STRUCTURES
13.2 NATIONAL MONUMENT/ICON GEOGRAPHIC AREAS
13.3 NATIONAL MONUMENT/ICON DOCUMENTS AND OBJECTS
13.4 OTHER NATIONAL MONUMENTS AND ICONS

14. COMMERCIAL FACILITIES SECTOR

14.1 ENTERTAINMENT AND MEDIA FACILITIES
14.2 GAMBLING FACILITIES / CASINOS (RESORTS)
14.3 LODGING FACILITIES
14.4 OUTDOOR EVENTS FACILITIES

14.5 PUBLIC ASSEMBLY / SPORTS LEAGUES FACILITIES
14.6 PUBLIC ASSEMBLY / OTHER FACILITIES
14.7 REAL ESTATE FACILITIES
14.8 RETAIL FACILITIES
14.9 INDUSTRIAL ASSETS
14.10 COMMUNITY ORGANIZATION FACILITIES
14.11 OTHER COMMERCIAL FACILITIES

15. GOVERNMENT FACILITIES SECTOR

15.1 PERSONNEL-ORIENTED GOVERNMENT FACILITIES
15.2 SERVICE ORIENTED GOVERNMENT FACILITIES
15.3 GOVERNMENT RESEARCH FACILITIES
15.4 GOVERNMENT STORAGE AND PRESERVATION FACILITIES
15.5 GOVERNMENT SENSOR AND MONITORING SYSTEMS
15.6 GOVERNMENT SPACE SYSTEMS
15.7 MILITARY FACILITIES
15.8 OTHER GOVERNMENT FACILITIES

16. DAMS AND LEVEES SECTOR

16.1 DAM PROJECTS
16.2 NAVIGATION LOCKS
16.3 MINE TAILINGS DAMS
16.4 HURRICANE BARRIERS
16.5 RIVER CONTROL STRUCTURES
16.6 LEVEES
16.7 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
16.8 OTHER DAM FACILITIES

17. COMMERCIAL NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR

17.1 NUCLEAR POWER PLANTS
17.2 RESEARCH, TRAINING, AND TEST REACTORS
17.3 NUCLEAR FUEL CYCLE FACILITIES
17.4 RADIOACTIVE WASTE MANAGEMENT
17.5 NUCLEAR MATERIALS TRANSPORT
17.6 DEACTIVATED NUCLEAR FACILITIES
17.7 RADIOACTIVE MATERIAL USERS
17.8 RADIOACTIVE SOURCE PRODUCTION AND DISTRIBUTION FACILITIES
17.9 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
17.10 OTHER NUCLEAR FACILITIES

18.1 CRITICAL MANUFACTURING

19.1 PRIMARY METAL MANUFACTURING
19.2 MACHINERY MANUFACTURING
19.3 ELECTRICAL EQUIPMENT, APLIANCE, AND COMPONENT MANUFACTURIN
19.4 TRANSPORTATION EQUIPMENT MANUFACTURING

Appendix 3
Information Sharing and Analysis Centers (ISAC) Listing

Information Sharing and Analysis Centers (ISACs) are a direct result of Presidential Decision Directive 63. The directive requested the public and private sector create a partnership to share important information about physical and cyber threats, vulnerabilities, intrusions and anomalies within and between industry sectors, and the National Infrastructure Protection Center (NIPC) and events to help protect the critical infrastructure of the United States. There are ISACs for many of the 17 Critical Infrastructures Key Resources (CIKR) sectors. Some but not all sectors have an ISAC while some sectors have multiple ISACs.

For additional information you may want to browse the ISAC Council.org website at
http://www.isaccouncil.org/sites /

Aviation ISAC (Airports Council International—North America)
http://www.aci-na.org

Chemical Industry Information Sharing and Analysis Center –
http://chemicalisac.chemtrec.com

Communications Information Sharing and Analysis Center
http://www.ncs.gov/ncc/main.html

Electricity Sector Information Sharing and Analysis Center –
http://www.esisac.com

Emergency Management and Response Information Sharing and Analysis Center –
http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/index.shtm

Energy Information Sharing and Analysis Center –
http://www.energyisac.com/index.cfm

Emergency Management and Response ISAC (US Fire Administration, Federal Emergency Management Association)
http://www.usfa.fema.gov/fire-service/cipc/cipc-new.shtm

Financial Services Information Sharing and Analysis Center –
http://www.fsisac.com

Food ISAC (Food Marketing Institute)
http://www.fmi.org/isac

The Highway Information Sharing and Analysis Center –
http://www.highwayisac.org

Indian Health Service ISAC
http://www.ihs.gov/Cio/ISAC/index.cfm

Information Technology - Information Sharing and Analysis Center –
http://www.it-isac.org

Multi-State Information Sharing and Analysis Center
http://www.msisac.org

Public Transit Information Sharing and Analysis Center –
http://www.surfacetransportationisac.org/APTA.asp

Real Estate Information Sharing and Analysis Center
http://www.reisac.org/

Research and Education Networking Information Sharing and Analysis Center
http://www.ren-isac.net/

Supply Chain Information Sharing and Analysis Center
https://secure.sc-investigate.net/SC-ISAC

Surface Transportation Information Sharing and Analysis Center -
http://www.surfacetransportationisac.org

Truck ISAC (American Trucking Associations)
http://www.truckline.com

Water Information Sharing and Analysis Center
http://www.WaterISAC.org

ISACs for the Following Sectors do not currently exist.

Sector	ISAC	Operating Organization	Government Department
3	Defense Industrial Base	NA	U.S. Department of Defense
9	Postal and Shipping	NA	U.S. Department of Homeland Security
13	Monuments and Icons	NA	National Park Service, U.S. Department of the the Interior
15	Government Facilities	NA	U.S. General Services Administration
16	Dams and Levees	NA	U.S. Army Corps of Engineers
17	Nuclear Facilities	NA	U.S. Department of Energy

Appendix 4
NIPP Baseline Criteria for Assessment Methodologies

The purpose of this appendix is to specify the baseline criteria for methodologies used to support all levels of comparative risk analysis under the NIPP framework. Many owners and operators conduct vulnerability and/or risk assessments on assets, systems, and networks under their control. DHS and the SSAs will take advantage of these activities by using the results of previous assessments whenever possible. However, assessments to date vary widely both within and across sectors in terms of their assumptions, comprehensiveness, objectivity, inclusion of threat and consequence considerations, physical and cyber dependencies and other characteristics. In order to use previous assessment results for comparative risk analysis nationally, the assessment methodologies used must be tested against NIPP baseline criteria.

Baseline Criteria

There are eight criteria that constitute the state baseline, categorized generally into two different groups. The first group tests the methodology to ensure it will be credible with objective users of the analysis produced by methodology; the second group tests the methodology to ensure it will be comparable with other standard methodologies used in comparative sector or national risk assessments. (Note: The national criteria only address seven criteria. Washington State has added an eighth element – skilled practitioners)

To be credible, a methodology must have a sound basis (it must have integrity); it also must be complete and the analytic method and associated assumptions must be defensible. These factors reflect the first three elements of the criteria. To be comparable, the methodology must be documented, transparent, reproducible, and accurate; these factors reflect the last four elements of the criteria.

The eighth and final factor in a sound methodology is the use of skilled practitioners.

The following questions provide a simple way to determine which aspects of a given methodology meet the baseline criteria. The questions also provide a guide for how a methodology may be improved or changed to meet the baseline criteria. A methodology meets the requirements of the baseline criteria when all of the questions can be answered in the affirmative.

Is the Methodology Credible?

- **Integrity (sound basis):** Is the methodology based on documented risk analysis and security vulnerability analysis? Does it specifically address:
  - Consequences?
  - Vulnerability?
  - Threat?

- **Complete**: Does the methodology provide reasonably complete results via a quantitative, qualitative, systematic, and rigorous process that:
  - Provides numerical values for estimated consequences, vulnerability, and threat whenever possible, or uses scales when numerical values are not practical?
  - Specifically addresses both public health and safety and direct economic consequences?
  - Considers existing protective measures and their effects on vulnerabilities as a baseline?
  - Examines physical, cyber, and human vulnerabilities?
  - Applies the worst-reasonable-case standard when assessing consequences and choosing threat scenarios?
  - Uses threat-based vulnerability assessments?

- **Defensible:** Is the methodology thorough and does it use the recognized methods of the professional disciplines relevant to the analysis? Does it adequately address the relevant concerns of government, the CIKR workforce, and the public?

Is the Methodology Comparable to Other Methodologies?

- **Documented:** Does the methodology provide clear and sufficient documentation of the analysis process and the products that result from its use?

- **Transparent:** Is the methodology easily understandable to others as to:
  - Assumptions used?
  - Key definitions?
  - Units of measurement?
  - How it is to be accomplished?
  - Basis for expert judgments and risk decisions?

- **Reproducible:** Does the methodology provide results that are reproducible or verifiable by equivalently experienced or knowledgeable personnel?

- **Accurate:** Is the methodology free from significant errors or omissions so that the results are suitable to assist in decision making?

  Given the unique nature of the individual CIKR sectors and the assets, systems and networks that comprise them, details of the baseline criteria must be tailored to each sector. DHS will work with the SSAs and other sector security partners to accomplish this tailoring; however, the baseline criteria above are generally applicable to each sector.

  Existing assessments or methodologies will be considered by DHS as meeting the NIPP Baseline Criteria and, therefore, are suitable for national and sector-level comparative risk analysis if they can provide an affirmative response to the questions above. Assessment or methodology evaluations will be done in coordination with the SSA, SCC, and GCC, as appropriate.

- **Skilled Practitioners:**
  - Do they have more than a working knowledge of the methodology?
  - Are they trained subject matter experts in physical security?
  - Are they trained in the identification of dependencies and interdependencies?

Specific Aspects of the NIPP Baseline Criteria

Based on classical risk analysis: As outlined in the NIPP, Chapter 3, risk analysis consists of three primary elements: consequence, vulnerability, and threat. To be considered credible, a proposed methodology must include all three of these components of risk.

Provides numerical values when possible; uses scales when necessary: Risk typically can be measured either quantitatively (i.e., numerically) or qualitatively (i.e., descriptively). Public health and safety and economic impacts generally lend themselves to quantitative measurement (e.g., number of lives lost, cost in dollars of rebuilding or restoring an asset), whereas psychological and governance impacts are often measured qualitatively. Accurate numerical estimates should be used whenever possible whenever quantitatively measuring consequences and associated risk. When it is not practical to use such estimates, scales should be used to reflect the assessed outcome using either numerical ranges (for quantitative metrics) or detailed descriptions (for qualitative metrics). The use of numerical ranges and/or detailed descriptions is necessary because terms such as "low" or "high" are subject to varied interpretation by different users. DHS will provide sample ranges and descriptive language to security partners and work with them to establish "translators" that facilitate the conversion of results using other methodologies to standard scales that support national comparative risk analysis.

Consider human and direct economic consequences: HSPD-7 establishes the consequences of interest having national significance which DHS will use in national comparative risk analysis. These consequences can be divided into four main categories: human, economic, public confidence and government capability. Because accurately estimating consequences other than direct injury, loss of life and economic effects is complex and often beyond the scope of an individual owner/operator's expertise, this element of the baseline criteria requires assessment methodologies that address the following two types of impact at a minimum:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries).
- **Economic Impact:** Direct effects on the national, State, tribal or local economy (e.g., cost to rebuild facility, system, or network; cost to respond to and recover from attack; other clearly definable incident costs resulting from unavailability of product or service; or long-term costs due to environmental damage).

Consider existing protective measures and their impacts as the baseline: In evaluating the extent to which an asset, system or network is vulnerable or an attack is likely, an assessment should consider the existing measures that are in place to reduce the asset, system, or network's exposure to the relevant threat scenarios. Specifically, security specialists should examine the

ability of an asset, system or network's existing security profile to deter, detect, devalue, defend against, mitigate, respond to and recover from the most relevant threat scenarios.

Use worst-reasonable-case standard: Risk assessments are significantly influenced by the estimated or assumed level of success or severity of a given threat scenario (e.g., worst case, worst reasonable case, most likely). For the purposes of national comparative risk assessments, methodologies should use a worst-reasonable-case scenario.

Examine physical, cyber, and human vulnerabilities: When evaluating risk, many vulnerability assessments focus solely on physical security; however, physical security is only one aspect of a robust vulnerability assessment. Vulnerability assessments should also assess personnel security and other human security issues, cyber security and network architecture issues, operational security and infrastructure dependencies and interdependencies.

Scenario-based vulnerability assessments: The suite of tools that DHS develops and uses for vulnerability assessments are scenario based, meaning that the assessments measure the susceptibility of an identified asset, system or network to a specific threat scenario (e.g., successful detonation of a nuclear bomb, successful detonation of a car bomb, etc.). This allows the assessment to be informed in general terms by potential adversary tactics and attack vectors. Consequently, vulnerability assessment methodologies used to support cross-sector comparative risk analyses should be scenario based, and certain specific scenarios or their equivalent should be used. In light of the distinct characteristics associated with different types of assets, systems or networks, DHS will work with sector partners to identify which threat scenarios are most appropriate in the context of the sector-specific landscape.

Defensible on logical grounds: In order to produce analysis that is credible to those who must use its results, a methodology must adhere to the recognized methods of the professional disciplines that are relevant to the method of analysis (e.g., economics, engineering, medical profession) and it must reasonably and adequately address the concerns raised by the three groups who may be directly affected by the decisions based on its results: (1) governments at all levels, (2) the CIKR workforce, and (3) the public at large.

Documentation is necessary to enable comparison with other methodologies in use: Written documentation that is clear and sufficiently complete to allow a comparison of strengths and weaknesses with respect to other methodologies used in the national comparative risk assessment is necessary. This should include a description of assumptions, definitions, units of measurement, time horizon, the general order and steps of the assessment, calculations and the basis for any expert judgments that the methodology relies on that are not readily apparent.

Need to be easily understandable: In addition to the existence of written documentation, a methodology must be easily understandable to others with appropriate knowledge and experience. This means that:

- Assumptions must be stated;

- Key definitions must be provided;
- Units of measurement must be specified;
- Analytic process by which the methodology is executed must be specified; and
- Basis for expert judgments used in lieu of explicit calculations or analysis must be provided.

As with any deliberate process, the results of applying the methodology must be reproducible or verifiable by others of requisite knowledge and experience levels. The methodology must be sufficiently defined and deliberate so that any qualified person could replicate the results it produces. It must not depend on hidden judgments or opinions.

Must be free from logical errors of omission or commission: The results of risk assessments will be used to make informed decisions regarding homeland security. Therefore, the accuracy of the methodology must meet a high standard. While estimates and approximations often must be used, the tradeoff between practicality and accuracy must be carefully taken into account and, in no case, should logical or mathematical errors be accepted.

Tab A
Appendix 4
Assessment Tools

ACAMS (Automated Critical Asset Management System) ACAMS is a DHS owned and sponsored CIKR inventory system used to secure, store and retrieve vital data. ACAMS provides:

- Reporting capability for local and national-level data calls on critical infrastructure
- Automated generation of Buffer Zone Protection Plans
- Uses CARVER and MSHARRPP+V assessment tools
- Automated generation pre-incident operational plans for local first responders
- Durable search capabilities to customize information in response to situational needs

CAPRA (Critical Asset & Portfolio Risk Analysis) CAPRA is a University of Maryland / Maryland Emergency Management joint venture. It is a methodology and process that can be used to quantitatively assess risks for a single asset, a portfolio of assets or a region to a natural disaster or human caused event. Additional information can be obtained by contacting Dr. Bilal Ayyub, 301.299.9375 or Ayyub@BMAEEngineering.com.

CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability) is an analytical tool that, if studied and used correctly, will help you get into that pro-active mindset and help you protect the assets of your Critical Infrastructure and Key Resource sites. CARVER is used to analyze and evaluate your sites' actual PHYSICAL assets (e.g., rail yards, rolling stock, engines, transformers, fuel storage, etc.).

CARVER2web (Criticality, Accessibility, Recoverability, Vulnerability, Espyability, Redundancy) is available free-of-charge to government agencies and educational institutions. The CARVER2web infrastructure analysis system allows for comparison of different types of critical infrastructure using a non-technical methodology. It allows government officials to rank the importance of CIKR in a selected jurisdiction.

HLS-CAM (Homeland Security-Comprehensive Assessment Model) was developed specifically for the National Guard. It is a full up program presently in use by the WA Army National Guard for a number of facilities throughout the state. This tool may not be available to entities outside the military.

MSHARRPP+V (Mission, Symbolism, History, Accessibility, Recognizability, Recoverability, Population, Proximity + Vulnerability) is a prioritization model designed specifically for critical assets.

PairPM (Pairwise Program Management) combines risk management with program management in a process for assessing infrastructure risk. For additional information on PairPM go to the Setracon, Inc. website at: http://www.setracon.com/PAIR-PM.pdf.

RAMCAP (Risk Analysis and Management for Critical Asset Protection) the DHS sponsored, RAMCAP methodology consists of several analysis phases with multiple steps in each phase. The grouping of the steps into phases has been established primarily based on the organizations that are expected to have primary responsibility. In other words, it is anticipated that there would be a "handoff" of material and responsibility between phases. However, it is important to have significant interaction among all stakeholders within each phase. For example, while it is anticipated that DHS, working with other government agencies, will have the primary responsibility for identifying critical assets and the nature of potential threats to those assets, it should be recognized that this process requires interaction with asset owners. Additional information is at http://www.esisac.com/publicdocs/assessment_methods/AppB_RAMCAP.pdf

RAM-W (Risk Assessment Methodology for Water) the course employs the Sandia Labs RAM model and though designed for water, RAM-W is applicable to communities and their facilities across the board.

Sandia Labs RAM Series (Contact information)

RAM-D	Dams (Cal Yeager, 508-844-4986)
RAM-C	Communities (Cal Yeager, 508-844-4986)
RAM-W	Water (water treatment and wastewater) (Jeffrey Danneels, 505-284-3897)
RAM-WSM	Small Water Utilities (Mark Grace at AWWA, 303-347-6193) Large Water Utilities (EPA Website)
RAM-T	High Voltage Electric Transmission Lines, modified and used for oil lines (linear activities) (Betty Biringer, 505-844-3985)
RAM-CF	Chemical Facilities (Cal Yeager 505-844-4986)
RAM-FE	Fossil Energy (Tommy Woodall 505-844-7541)
RAM-PART	Property Analysis and Ranking Tool (Regina Hunter 505-844-5837)
SEA	Security Evaluation Assessment, Primarily for USAF/Navy Facilities Security VA (Randy Peterson 505-844-5792)
SS	School Security (Gordon Smith 1-888-577-4849)

VAM	VAM for Corrections, focus is prisons escapes and contraband (Chris Robertson or Ivan Waddoups, 505-844-4776)

Security Engineering This program requires a week long class on how to conduct assessments with protection in mind. It explains how to focus construction to withstand given threats and how to upgrade existing structures to resist known threats (bombs, explosives, etc.). It is somewhat technical in the application of formulas and determination of different factors. Orientation is primarily on the military but has broader application. Course materials provide some standard price lists and good reference material. The point of contact is Ms. Kelly Palmer, 703- 607-9198, at the National Guard Bureau.

VSAT Water and Wastewater (Vulnerability Self Assessment Tool) self assessment tool requires a two day training seminar. For more info: info@VSATusers.net or visit www.VSATusers.net <http://www.vsatusers.net/> . To order, contact AMSA at 202-833-2672. The EPA paid for all water systems nation-wide to conduct assessments using this tool a few years ago. VSAT is sector specific.

NOTE: This is not an all inclusive list nor does this listing constitute endorsement.

If you are aware of additional critical infrastructure sector ISACs, critical infrastructure information points, or other industry recognized assessment tools please send that information to Jeff Parsons at j.parsons@emd.wa.gov or call 253-512-7065.

Appendix 5
Public Disclosure and Security

The security of critical infrastructure key resources (CIKR) data collected in support of the statewide critical infrastructure protection (CIP) program is of vital concern to facility owners, operators, managers and responders. Therefore it is of the utmost importance that all precautions are taken to protect the data. Best practices dictate that plans and procedures are in place to ensure CIKR data security. The state's CIP Program employs the federal Protected Critical Infrastructure Information (PCII) Program procedures and protocols for the receipt, storage, dissemination, transmission, and destruction of CIKR data and related products. Requests for public disclosure of CIKR records will be handled pursuant to Washington State's Public Records Act (ch. 42.56 RCW) and applicable federal law.

IPO Office staff are trained and PCII certified by the DHS PCII Program Offices on CIKR handling procedures. Additionally, each staff member has a security clearance and undergone a background investigation. PCII is the primary means through which the IPO Office protects CIKR data. Violations of PCII handling protocols may result in disciplinary action, dismissal, loss of security clearance, fine and or imprisonment under federal law and similar censure under state law.

RCW 42.56.420

The following information relating to security is exempt from disclosure under this chapter:

(1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and

(b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism;

(2) Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility or any individual's safety;

(3) Information compiled by school districts or schools in the development of their comprehensive safe school plans under RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school;

(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans,

security risk assessments, and security test results to the extent that they identify specific system vulnerabilities; and

(5) The security section of transportation system safety and security program plans required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180.

Protected Critical Infrastructure Information (PCII)

The PCII Program, part of the Department of Homeland Security (DHS), Infrastructure Partnerships Division (IPD) encourages private industry to share its sensitive CIKR related business information with the Federal government. PCII is an information-protection tool that facilitates information sharing between the government and the private sector. DHS and other Federal, State and local analysts use PCII in pursuit of a more secure homeland, focusing primarily on:

- Analyzing and securing critical infrastructure and protected systems,
- Identifying vulnerabilities and developing risk assessments, and
- Enhancing recovery preparedness measures.

The Critical Infrastructure Information Act of 2002 protects CIKR data which is voluntarily submitted from public disclosure, provided it meets submission requirements. This program protects CIKR data from:

- The Freedom of Information Act,
- State and local disclosure laws, and
- Use in civil litigation.

These procedures govern the receipt, validation, handling, storage, marking and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security. This rule applies to all Federal agencies, all United States Government contractors, and State, local and other governmental entities that handle, use, store or have access to critical infrastructure information that enjoys protection under the Critical Infrastructure Information Act of 2002.

Federal Authorities

- Critical Infrastructure Information Act of 2002, subtitle B of Title II of the Homeland Security Act of 2002 (Public Law 107-296, 116 Stat. 2135, sections 211-215), codified at 6 U.S.C. §§1310134, and available through http://www.dhs.gov/xlibrary/assets/CII_Act.pdf.
- Procedures for Handling Protected Critical Infrastructure Information, 6 CFR Part 29, Final Rule published September 1, 2006 at 71 FR 52261-52277, and available through http://www.dhs.gov/xinfoshare/laws/gc_1158333877680.shtm.

FOR OFFICIAL USE ONLY

INSTRUCTIONS

Infrastructure Protection Office
Emergency Management Division (EMD)
Washington Military Department

STATE PUBLIC DISCLOSURE EXEMPTIONS

The attached materials contain critical infrastructure and/or key resource information (including compiled underlying data collected in preparation of or essential to specific and unique vulnerability assessments or specific and unique response or deployment plans), that has been assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, the public disclosure of which would have a substantial likelihood of threatening public safety. As such, this information should be exempt from public disclosure pursuant to RCW 42.56.420(1)(a). This material may also be exempt from disclosure pursuant to RCW 42.56.420(1)(b), applicable to certain records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for potential acts of terrorism.

INFORMATION HANDLING

The attached materials will be disclosed by EMD only to authorized recipients who have signed the "Request/Receipt for Critical Infrastructure Key Resources (CIKR) Database Information" and who have a "need-to-know". The recipient agrees to use the information for authorized purposes only; to share the information only after approval from the Director of EMD; to copy the material only when essential for internal authorized use; to protect the confidentiality of the material; and when unattended, to store the material in a locked container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

Infrastructure Protection Office
Emergency Management Division (EMD)
Washington Military Department

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Department of Homeland Security

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

Department of Homeland Security

FOR OFFICIAL USE ONLY

MD 11042.1