

Washington State Sector Specific Plan for Critical Energy Infrastructure

November 2011

Washington State Energy Coordinating Council

October 31, 2011

FROM: Mark Anderson, Washington State Department of Commerce
Mary Robinson, Puget Sound Energy

SUBJECT: Release of Sector Specific Plan

We are pleased to present the Washington State Sector Specific Plan for Critical Energy Infrastructure, a work product of the Washington State Energy Coordinating Council (ECC).

This Sector Specific Plan (SSP) is the culmination of many individuals' work over the past two years in determining how to protect energy infrastructure critical to Washington State.

The SSP builds on three major plans:

The National Infrastructure Protection Plan (NIPP) developed by the federal Department of Homeland Security. The plan establishes a Risk Management framework for identifying and protecting all critical infrastructure and key resources in the U.S.

The federal Energy Sector-Specific Plan developed by the US Department of Energy in conjunction with public and private sector energy partners. The plan details how the NIPP risk management framework is applied in identifying and protecting critical infrastructure and key resources for energy. The federal Energy SSP is the model for our state plan.

The Washington Infrastructure Protection Plan developed by the Infrastructure Protection Sub-Committee (IPSC) of the Washington State Committee on Homeland Security. The plan builds on the NIPP and provides a basis for integrating all state critical infrastructure and key resource protection efforts under a single state program.

The ECC is made up of representatives of public and private oil, natural gas and electric utility companies doing business in the State of Washington, and employees of key state agencies with energy emergency and security responsibilities. The ECC brings together companies that previously made up separate oil, natural gas and electric utility working groups. We believe this will result in efficient infrastructure protection work, consistent policies and programs, and quality solutions for dealing with interdependencies between the various energy sub-sectors.

We would like to thank our peers on the IPSC for their support of our energy sector infrastructure work and the agencies and companies and their representatives on the ECC for their work and support in addressing sensitive and serious issues in the development of this SSP. Finally, we would like to thank our managers at the State Department of Commerce and Puget Sound Energy. Their support and patience has been critical as we struggled with the development of this SSP and the difficult issues that arise when a state has vital interests in the corporate expertise, investment and responsibility for securely operating the electric grids and fuel supplies on which this state and country run.

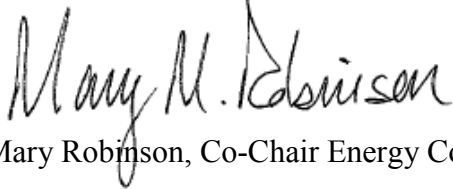
We are deeply appreciative that US Department of Energy funded this effort through an American Recovery and Reinvestment Act grant to the Department of Commerce.

This SSP is a working plan that now needs to be implemented. Our greatest thanks is reserved for the ongoing partnership needed to ensure that energy infrastructure critical to Washington is accurately identified and appropriately protected.

We hope the steps we have taken and will take in the future to protect this critical infrastructure will never be tested, but if tested, will be resilient and able to support us always.

A handwritten signature in black ink that reads "Mark R. Anderson". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

Mark Anderson, Co-Chair Energy Coordinating Council

A handwritten signature in black ink that reads "Mary M. Robinson". The signature is cursive and somewhat stylized, with the first letters being larger and more prominent.

Mary Robinson, Co-Chair Energy Coordinating Council

Table of Contents

Executive Summary 5

Introduction 7

Sector Vision and Goals 14

Sector Profile 15

Critical Infrastructure/Key Resource Partners 17

Identify Assets, Systems, and Networks; Assess Risks; and Prioritize
Infrastructure 21

Identify Issues; Implement Programs and Strategies; and Measure
Effectiveness 26

Appendix A: Coordinating Council 46

Appendix B: Federal and State Laws Protecting CI Data and Information 47

Executive Summary

Background

Before the terrorist attacks on the Twin Towers in New York City on September 11, 2001, state governments' emergency plans focused on preparedness and response. After the attacks States' began to consider how to implement security measures to prevent attacks and protect critical infrastructure.

In Washington State, a Committee on Homeland Security was formed with a standing committee called the Infrastructure Protection Subcommittee (IPSC).¹ The mission of the IPSC, as stated in the Washington Infrastructure Protection Plan (WIPP) is to "Work with our public and private sector partners to identify and protect critical infrastructure and key resources against all hazards."²

The IPSC determined that each of 18 federally designated infrastructure sectors should establish a Coordinating Council, and develop and implement a Sector Specific Plan (SSP) to address the identification and protection of that sector's Critical Infrastructure and Key Resources (CIKR). In 2010, the Energy Sector representatives on the IPSC established the Energy Coordinating Council (ECC) that has produced this SSP.

The ECC is the primary forum where the State/Energy Industry partnership will be implemented; in accordance with this SSP, which is an annex to the Washington State Energy Assurance and Emergency Preparedness Plan.³

The SSP requires Commerce and the ECC to prepare a biennial report on SSP implementation beginning in December 2012. The SSP is a living document that will be updated continuously as needed, and formally at least every four years.

¹ See section titled "CIKR Partners" for Washington State organizational structure dealing with terrorist issues. CIKR stands for Critical Infrastructure / Key Resources.

² Washington Infrastructure Protection Plan, State Military Department, 2008, page following the Forward.

³ Find both plans on the Commerce Energy Emergencies and Security website:

<http://www.commerce.wa.gov/site/975/default.aspx>. Funding for the SSP was provided by the US Department of Energy through a stimulus grant (American Recovery and Reinvestment Act of 2009, grant number DE-OE0000060). The grant required an update of the State's energy contingency plans and Commerce selected to develop the SSP to meet the grant requirements.

Scope

The energy infrastructure addressed by this SSP includes most major energy resources (e.g. oil, coal, natural gas, wind) and processes (energy storage, transportation, distillation, generation, distribution). Most state level CIKR is owned and operated by major oil, natural gas and electric utility companies. Small and independent companies more rarely have infrastructure that rises to state level CIKR addressed by this SSP.

- Oil refiners in the state control crude supply and storage facilities, refineries, and refined product storage, distribution and sales facilities. Small and independently owned wholesale and retail facilities rarely raise to state level CIKR.
- Natural gas companies own and operate a combination of natural gas storage, transmission, and distribution facilities.
- Electric utilities own and operate multiple energy storage, generating and transmission and distribution facilities. Independent power producers may have facilities that raise to state level CIKR.

Certain energy infrastructure is NOT addressed by this SSP and includes:

- Nuclear Power Plants (Nuclear Power Sector);
- Dams that do not generate electricity (Dams Sector);⁴ and
- Oil Tankers (Transportation Sector).⁵

While the above infrastructure is not specifically addressed by this SSP, many of those resources are owned and/or operated by the same companies that are ECC members, or that have closely related businesses. These represent linkages between ECC members and SSP CIKR identification and protection programs. Linkages include:

- Bonneville Power Administration (BPA), an ECC member that markets all the power from the State's lone nuclear plant (Columbia Generating Station – owned and operated by Energy Northwest) and all the federal hydropower dams (owned and operated by either the Army Corps of Engineers or the Bureau of Reclamation);
- Northwest Electric Utilities, that own and operate the remaining hydroelectric facilities in the State; and
- Oil Refiners and Marketers that own or lease crude and refined product oil tankers and barges to supply their refineries and wholesale and retail markets.

⁴ The Dams Sector Specific Plan may also cover hydroelectric dams, but they are also included in the scope of this SSP because they make up such a large and important part of the electricity system in the Pacific Northwest and are inseparably incorporated into the critical infrastructure protection plans of state and regional utility companies.

⁵ Crude oil and refined product pipelines also are address nationally in the Transportation Sector, but are addressed by the Energy Sector (and this SSP) in Washington State.

General Approach

The National Infrastructure Protection Plan (NIPP) produced by the Department of Homeland Security (DHS) uses a risk management approach to identify and protect CIKR. All other supporting plans do the same; including the Washington Infrastructure Protection Plan (WIPP) and the federal energy SSP upon which this SSP is based.⁶

The State Energy SSP adopts some elements of the federal Energy SSP directly, and uses other elements for reference. In addition, information is provided that is unique to Washington State and the region. However, this SSP does not duplicate every element of the federal SSP. For example, it does not contain energy sector profiles because there are many other existing documents (and websites) that already do that in detail. The heart of the SSP is an issues section that identifies key issues and mitigation programs and measures to address those issues and to evaluate their effectiveness. The issue areas are:

1. Data and Information Sharing
2. Communications
3. Mapping CI and Mitigation Analysis
4. Interdependencies
5. Local Energy Assurance
6. Infrastructure Out of State, Critical to Washington
7. Application of Federal and State Resources
8. Emergency Exercises
9. Emergency Response, Restoration and Recovery
10. Biennial CI Report and SSP Updates

The SSP recognizes some important factors about energy CIKR identification and protection.

- The State role is one of support and coordination. Nearly the entire energy infrastructure in the State is owned and operated by public or private companies. They have the primary task of identifying and protecting CIKR.
- Energy companies have not been sitting on their hands; all have undertaken major efforts to identify and protect CIKR. Ensuring CIKR identification and protection under this SSP may mean in many cases simply reporting on what companies have already done.
- Much important energy infrastructure sits out in the open and is spread broadly across the countryside for all to see. Measures to prevent attacks and protect it can be prohibitively

⁶ Energy Sector Specific Plan, an Annex to the National Infrastructure Protection Plan, US Department of Energy, 2010 (produced in consultation with other federal agencies and public and private energy companies).

expensive. An appropriate “protective” mitigation measure may be to improve emergency response preparedness and capabilities.⁷

SSP Implementation

Energy company representatives on the ECC have volunteered to take the lead on certain issues. The co-chairs have the lead for remaining issue areas. The ECC, with assistance from company leads and the co-chairs will look at each issue area, identify any problems to address, develop mitigation programs as necessary, implement those programs and evaluate their effectiveness. As said previously, for any issue area there may be no substantial remaining problems and reporting is all that is required. For other areas, mitigation programs are underway and evaluation is required. For some areas, problems must still be identified as well as mitigation programs to address them.

⁷ Traditional measures that may be too expensive to implement include duplicating facilities, hardening facilities, hiding facilities, guarding facilities, and the like.

Introduction

SSP Development Directives and Partnership

This Energy Sector Specific Plan for Critical Energy Infrastructure (SSP) was developed in response to numerous encouragements and determinations by federal and state authorities. Most recently, in Washington, the Infrastructure Protection Subcommittee of the Committee on Homeland Security (CHS) directed its sector leads to establish Coordinating Councils and Sector Specific Plans.⁸ Because most critical energy infrastructure is owned and operated by private companies or local public entities, such as municipal utilities, it requires a voluntary partnership between the energy industry and Washington State to develop and implement the SSP. This partnership is the Washington State Energy Sector Coordinating Council (ECC).⁹

The US Department of Homeland Security (DHS) has encouraged every state to develop a general state infrastructure protection plan (SIPP), and more specific sector specific plans (SSP).¹⁰ These state plans should reflect and support federal infrastructure protection plans.

The Washington Infrastructure Protection Plan (WIPP), developed by the state Infrastructure Protection Subcommittee (IPSC), reflects and supports the National Infrastructure Protection Plan (NIPP), developed by the DHS.

This SSP, The Washington Energy Sector Specific Plan for Critical Energy Infrastructure (herein called SSP) developed by the ECC, reflects and supports the federal Energy Sector-Specific Plan, developed by the US Department of Energy (DOE).¹¹

All four plans (NIPP, WIPP, federal energy SSP, Washington energy SSP) can be found on the Commerce web site at:

<http://www.commerce.wa.gov/site/975/default.aspx>

⁸ See organizational chart, Appendix A, page 44, of Washington Statewide Homeland Security Strategic Plan 2006 – 2011. Located here: <http://www.emd.wa.gov/plans/documents/WAHLSStrategic2006-2011.pdf>

⁹ See appendix A for a description of the ECC and the list of member organizations.

¹⁰ Washington recognizes 18 federally designated infrastructure sectors. See http://www.emd.wa.gov/plans/2008_WIPP.pdf, page iv.

¹¹ Energy Sector-Specific Plan, an Annex to the National Infrastructure Protection Plan, US Department of Energy, DHS, 2010.

SSP Purpose and Contents

This SSP was produced to accomplish the following:

- Establish a comprehensive plan that, when implemented, ensures that critical energy infrastructure in Washington state, or in nearby states and provinces that Washington depends on, is identified and “appropriately protected.”¹²
- Add a critical infrastructure security component to existing state energy contingency plans. This SSP represents that security component, and will complement the existing Washington State Energy Assurance and Emergency Preparedness Plan, and other supporting documents.¹³

Though this SSP is supposed to reflect and support the federal energy SSP, it does not replicate the federal SSP in every detail. For example, the federal SSP describes each energy subsector in the US, its components and processes. But this SSP does not describe the unique hydropower assets in Washington because they are described elsewhere, for example in documents of the Northwest Power and Conservation Council. Thought not repeated here, those characteristics, and others, are important for the development of security and emergency response plans, and were considered in the development of this SSP.

The following table compares the contents of the federal energy SSP with this SSP:

Table 1 Federal SSP and State SSP Comparison

Federal Energy SSP	Washington State Energy SSP
Executive Summary Vision Statement for the Energy Sector Sector Security Goals Energy Sector Profile and Assets CIKR Assessment and Prioritization Protective Programs and Performance Measurement Energy SSP Process and Responsibilities	Similar
Introduction	Similar
Sector Profile, Vision and Goals Sector Vision and Goals Vision Statement	Washington’s Energy SSP adopts the Sector Vision and Goals of the Federal SSP.

¹² “Appropriate protection” includes a range of actions, from building fences and hiring guards to the implementation of cyber security standards. Because much energy infrastructure is scattered across the countryside in plain view, making traditional protective measures prohibitively expensive, appropriate protection may also mean taking steps to reduce the consequences of its loss (such as looping transmission lines) or enhancing emergency response plans to restore energy systems more quickly and efficiently. Also, “ensuring critical energy infrastructure is identified and protected” may mean recognizing that an energy company has already done it, not initiating a new identification and protection effort. In addition, while the protection of critical infrastructure in other states and provinces cannot truly be ensured by agencies and industries in Washington State, we can ensure that communications about critical infrastructure are made to the appropriate companies and government entities in other states and provinces.

¹³ The contingency plan and many other supporting documents can be found on the Department of Commerce web site at: <http://www.commerce.wa.gov/site/975/default.aspx>

<ul style="list-style-type: none"> Goals Sector Profile Electricity <ul style="list-style-type: none"> Electricity Generation Electricity Transmission, Distribution and Control Systems Petroleum <ul style="list-style-type: none"> Crude Oil Petroleum Processing, Product Transport, and Storage Petroleum Control Systems Natural Gas <ul style="list-style-type: none"> Natural Gas Prod., Proc., Trans., Dist. and Storage Liquefied Natural Gas Facilities Natural Gas Control Systems Gas Market Centers Energy Sector Interdependencies Energy Sector Resilience CIKR Partners <ul style="list-style-type: none"> Relationships with Industry Owner/Operators and Organizations Sector Coordinating Councils Relationships with Government Agencies <ul style="list-style-type: none"> Government Coordinating Council Relationships with Other Federal Departments and Agencies Relationships with State, Local, Tribal & Territorial Agencies Interaction and Communication Among Public and Private Sectors Value Proposition 	<p>Washington’s Energy Sector Profile is not included in the SSP.</p> <p>The State’s electricity profile is best found in documents of the Northwest Power and Conservation Council.¹⁴</p> <p>The State’s Petroleum and Natural Gas profiles are best found in numerous government and industry documents.¹⁵</p> <p>Energy sector interdependencies are dealt with in the SSP Issues section, under Interdependencies.</p> <p>Washington’s energy SSP discusses CIKR government and industry partnership issues in the Introduction.</p> <p>Washington’s energy SSP adopts the federal Value Proposition.</p>
<p>Identify Assets, Systems, Networks and Functions</p> <ul style="list-style-type: none"> Defining Information Parameters <ul style="list-style-type: none"> Energy Assets and Systems Defining Energy Asset and System Parameters Information Collection and Sharing Existing Energy Sector Information Resources <ul style="list-style-type: none"> Electric Generation and Transmission Information Petroleum Asset Information Natural Gas Asset Information Protection of Collected Data Collecting Infrastructure Information Verifying and Updating Infrastructure Information 	<p>Washington’s energy SSP discusses CIKR identification issues in the Introduction.</p> <p>The SSP discusses information collection and sharing in the Issues section under Information Collection and Sharing.</p>
<p>Assess Risks</p> <ul style="list-style-type: none"> Use of Risk Assessment in the Sector Screening Infrastructure Assessing Consequences Assessing Threats Assessing Vulnerabilities 	<p>Washington’s energy SSP discusses risk assessment issues in the Issues section under Risk Assessment.</p>

¹⁴ See <http://www.nwcouncil.org/>

¹⁵ See <http://www.atg.wa.gov/gasstudy.aspx>

<p>Prioritize Infrastructure</p>	<p>Washington’s energy SSP discusses prioritization issues in both the Introduction and in the Issues Section under Prioritization.</p>
<p>Develop and Implement Protective Programs, & Resilience Strategies</p> <ul style="list-style-type: none"> Overview of Sector Protective Programs Process for Evaluating, Prioritizing Needs, & Implementing Programs Enhanced Information Sharing and Needs Assessment Developing and Implementing Focused Programs <ul style="list-style-type: none"> Program Development and Sector Goals Information Sharing and Communication Industry Programs Government Programs Physical and Cyber Security Industry Resilience Programs <ul style="list-style-type: none"> Electricity Oil and Natural Gas Government Programs International Programs Coordination and Planning <ul style="list-style-type: none"> Coordination with Industry Coordination with Federal Government Agencies Coordination with States and Localities Regional Coordination International Coordination Public Confidence Program Performance, Gaps and Challenges 	<p>Development and implementation of protective programs and resiliency strategies is the key focus of Washington’s energy SSP.</p> <p>All programs and strategies are identified and discussed in the Issues Section under each Issue area.</p>
<p>Measure Effectiveness</p> <ul style="list-style-type: none"> Key Risk Mitigation Activities CIKR Performance Measurement <ul style="list-style-type: none"> Metrics <ul style="list-style-type: none"> Energy CIP Metrics Process for Measuring Effectiveness Electricity Subsector Metrics Oil and Natural Gas Subsector Metrics Information Collection and Verification Reporting <ul style="list-style-type: none"> Using Metrics for Continuous Improvement 	<p>Effectiveness measures are included in the discussion of programs and strategies because it is the success of those programs and strategies that is being measured (See Issues section)</p>
<p>CIKR Protection R&D</p> <ul style="list-style-type: none"> Overview of Sector R&D Energy Sector R&D <ul style="list-style-type: none"> Cyber security R&D Requirements Cyber security Programs Cyber security Capability Gaps Physical Security R&D Regulations Sector R&D Plans R&D Management Processes ARRA 2009 	<p>Washington’s energy SSP does not deal thoroughly with CIKR R& D. Federal R&D identification, etc., is generally thought sufficient for addressing state R&D concerns. Where Washington State identifies R&D issues (primarily from the federal discussion), they are dealt with under specific programs and strategies like with effectiveness measures in the Issues Section.</p>
<p>Managing and Coordinating SSP Responsibilities</p> <ul style="list-style-type: none"> Program Management Approach Processes and Responsibilities <ul style="list-style-type: none"> SSP Maintenance and Update Annual Reporting 	<p>Washington’s energy SSP addresses coordination, management, roles and responsibilities in the Introduction section generally. Specific assignments are articulated in the Issues section under each</p>

<p>Resources and Budgets Training and Education Information Sharing and Protection Implementing the Partnership Model Partnership Coordination and Efficiency</p>	<p>issue area.</p>
<p>Appendix 1 Glossary of Key Terms Appendix 2 List of Acronyms and Abbreviations Appendix 3 Sources and References Appendix 4 Authorities Authorities Affecting Multiple Segments of the Energy Sector Authorities Affecting Electric Power Authorities Affecting Natural Gas Authorities Affecting Petroleum Appendix 5 Asset Ownership Appendix 6 Energy SCC and GCC Membership Appendix 7 Transportation Systems SSP Appendix 8 Asset Classes</p>	<p>Washington’s energy SSP generally adopts the appendices of the federal energy SSP. State specific supporting information is attached in appendices. Generally, however, the kind of information provided in the federal appendices is contained in other documents not attached to the state’s energy SSP.</p>

Sector Vision and Goals

The Washington Energy Sector Coordinating Council adopts the following sector vision and security goals directly from the federal energy SSP.

Energy Sector Vision Statement

The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private partners at all levels of industry and government.

Energy Sector Security Goals

Information Sharing and Communication

Goal 1: Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange among trusted public and private sector partners.

Physical and Cyber Security

Goal 2: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resilience.

Coordination and Planning

Goal 3: Conduct comprehensive emergency, disaster, and continuity of business planning-including training and exercises-to enhance reliability and emergency response.

Goal 4: Clearly define and clarify CIP roles and responsibilities among all Federal, State, local, and private sector partners, and work to create efficiency and improved coordination throughout the partnership.

Goal 5: Understand key sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations.

Public Confidence

Goal 6: Strengthen partner and public confidence in the sector's ability to manage risk and implement effective security, reliability, and recovery efforts.

Sector Profile

The federal energy SSP has an extensive chapter describing the profile of the energy sector in the United States. The national energy profile is not repeated here, but provides an important context for understanding both the federal energy SSP and this SSP.

While much of the energy sector profile for Washington and the Pacific Northwest is the same as the national profile, there are important differences. For example, there is no oil or natural gas production in the state. The closest natural gas production is in British Columbia and closest oil production is in Alberta. We have the largest hydroelectric system in the world and a high voltage transmission grid operated by federal agencies.¹⁶ To truly understand our energy assurance risks and options, one must understand Washington's and the region's energy profile. Washington and Pacific Northwest energy profile information is not included in this SSP, but is available in other documents. See below for links to key sector profile documents.

Energy (all sources)

- Washington State Energy Supply Disruption Tracking System (WAESDTS), State Department of Commerce.¹⁷
- US Department of Energy, Energy Information Administration. Energy and Electricity. Find at <http://www.eia.gov/state/state-energy-profiles.cfm?sid=WA>
- US Department of Energy, Energy Information Administration. State Energy Data System. See transportation consumption estimates. Find at http://www.eia.gov/state/seds/seds-states.cfm?q_state_a=WA&q_state=Washington#undefined

Electricity

- Northwest Power and Conservation Council. Sixth Northwest Conservation and Electric Power Plan. Find at <http://www.nwcouncil.org/energy/powerplan/6/default.htm>
- Pacific Northwest Utilities Conference Committee. 2011 Northwest Regional Forecast. Find at <http://www.pnucc.org/nwregionalforecast.html>

¹⁶ The Federal Columbia River Power System (FCRPS) referenced here includes the entire Columbia River drainage (e.g. includes Snake River dams) located in the Pacific Northwest region, not just in Washington. Many major dams in the drainage are owned and operated by the Corps of Engineers, U.S. Army (key navigation dams with locks) or by the Bureau of Reclamation, Department of the Interior (key irrigation dams). The power from these dams is transmitted and sold by a third federal agency the Bonneville Power Administration, Department of Energy.

¹⁷ Database of public and private energy infrastructure property of iMapData Inc. WAESDTS is accessed by Commerce and Emergency Management Division (EMD) during response to energy supply emergencies.

- Bonneville Power Administration. Columbia River Treaty. Find at <http://www.crt2014-2024review.gov/>

Natural Gas

- http://www.northwest.williams.com/NWP_Portal/TBD
- <http://www.gastransmissionnw.com/>
http://www.gastransmissionnw.com/aboutus/company_facts.html
- <http://pse.com/aboutpse/EnergySupply/Pages/Natural-Gas-Supply.aspx>
- <http://www.avistautilities.com/services/gas/Pages/default.aspx>

Petroleum

- Washington State Attorney General, Washington State 2007-2008 Gasoline Prices Study. Find at <http://www.atg.wa.gov/gasstudy.aspx>
- Washington Utilities and Transportation Commission, Pipeline Safety Division. See Pipeline Maps. Find at <http://www.utc.wa.gov/regulatedIndustries/transportation/pipeline/Pages/pipelineMaps.aspx>

Critical Infrastructure/Key Resource Partners

“No single government agency, industry group, or company can secure the entire energy infrastructure. Collaboration at all levels is essential to securing an interdependent infrastructure that is owned, operated, hosted, and regulated by many entities. Voluntary partnerships help facilitate the useful exchange of security-related information and maximize the effectiveness of infrastructure protection and resilience efforts. They also promote the cooperation necessary to speed restoration and recovery with activities such as equipment and personnel sharing.” “The Energy SSP provides the basis for close and effective coordination among all sector partners.” [Energy SSP for CI Resilience, p. 27]

Washington Infrastructure Protection Organizational Structure¹⁸

The Washington State Emergency Management Council (EMC) is the overarching body that addresses all potential disasters in Washington.¹⁹

A standing committee of the EMC is the state Committee on Homeland Security (CHS). The CHS is the overarching body that addresses all potential terrorism issues in the State.

A key standing committee of the CHS is the Infrastructure Protection Subcommittee (IPSC), which addresses critical infrastructure protection in Washington.²⁰ The IPSC recognizes 18 federally designated infrastructure sectors, of which energy is one, with three key subsectors: oil, natural gas, and electricity. Each sector has a public or government sector lead and a private or industry sector lead.²¹ The two energy sector leads initiated the establishment of the Energy Sector Coordinating Council that is co-chaired by Commerce and Puget Sound Energy.

The ECC is made up of representatives from electricity, natural gas, and petroleum products suppliers that do business in the state of Washington, and state agency representatives with energy policy responsibilities.²²

State Agencies

¹⁸ See organizational chart, Appendix A, page 44 of Washington Statewide Homeland Security Strategic Plan 2006 – 2011. Located here: <http://www.emd.wa.gov/plans/documents/WAHLSStrategic2006-2011.pdf>

¹⁹ See <http://www.emd.wa.gov/about/WashingtonMilitaryDepartmentEmergencyManagementDivision-AboutUs-EmergencyManagementCo.shtml> See also RCW 38.52.040. The Director of the State Military Department is the Governor’s designee and federal liaison for addressing all terrorist related issues in Washington State. In that capacity, the Director is Washington’s Homeland Security Advisor, the Coordinator for the Executive Security Council, the Coordinator for the state Emergency Management Council (EMC), and oversees the state National Guard and Military Department Emergency Management Division (EMD). The Director in 2011 (first edition of SSP) is Major General Timothy J. Lowenberg.

²⁰ For information about the IPSC, see the WIPP at - http://www.emd.wa.gov/plans/2008_WIPP.pdf

²¹ As of 2011 (first edition of SSP) the energy sector leads were: Mark Anderson, Sr. Energy Policy Specialist, Department of Commerce; and Mary Robinson, Manager of Business Continuity, Puget Sound Energy.

²² ECC membership can be found in Appendix A.

The state **Military Department Emergency Management Division (EMD)** has primary responsibility for general emergency planning and response in the state, and for coordination with local emergency management agencies, first responders, and federal agency liaisons. During an actual emergency, EMD activates the State Emergency Operations Center (EOC) to coordinate state response. During an emergency with implications for energy infrastructure and energy supply Department of Commerce representatives staff the Energy Desk in the State EOC.²³ An energy sector industry representative may also support the Energy Desk during State EOC activation.

The **Washington State Department of Commerce**, Energy Office, is the State Energy Office for purposes of the US Department of Energy. Commerce has statutory responsibility for the development, maintenance and implementation of state energy assurance and contingency plans.²⁴ This makes Commerce the Emergency Support Function (ESF) #12 coordinator (ESF #12 is Energy). A Commerce staff person is also the primary Energy Emergency Assurance Coordinator (EEAC) for the State.²⁵ Most years, a representative of the Energy Policy Division is a member of the National Association of State Energy Officials (NASEO) Energy Data and Security Committee.

The **Washington Utilities and Transportation Commission (WUTC)** is the utility regulator for the state of Washington. Washington, through the WUTC, is one of only a few states that have regulatory authority over pipeline safety. This makes the WUTC a key resource for addressing energy assurance issues, including critical infrastructure and emergency response that involve crude oil, petroleum products, and natural gas pipelines. At the federal level, pipelines are considered a transportation infrastructure so the federal energy SSP does not address them. In Washington, energy product pipelines are considered part of the energy sector and this SSP does address them. The WUTC is a supporting agency for ESF #12 (Energy).

The state **Office of Financial Management (OFM)**, Executive Policy Group, has liaison staff that interacts with federal agencies and members of Congress, state and local government agencies, and directly with private citizens, companies and organizations, to address energy assurance issues. The Commerce Energy Policy Division staff, OFM liaisons, and federal liaisons for energy assurance communicate on a regular basis when there are potential or existing energy assurance concerns. During actual energy emergencies, Commerce provides emergency response recommendations to the Executive, and leads emergency response teams that implement Executive directives.

²³ Commerce is Emergency Support Function (ESF) #12 (Energy) Coordinator for the State. The Washington Utilities and Transportation Commission (WUTC) is a key ESF #12 supporting agency.

²⁴ RCW 43.21F

²⁵ The EEAC position is liaison to the USDOE for purposes of sharing state energy emergency information with the federal government and receiving national and international energy emergency information from the federal government.

Key state legislators and their staff are briefed and consulted as necessary about energy assurance issues. By statute, the Joint Committee on Energy Supply and Energy Conservation is convened when there is either a declaration of Energy Supply Alert or Energy Emergency. This legislative committee reviews and advises on the Governor's response plans, and has certain authorities over the extension of Alerts and Emergencies.²⁶

Local Governments

Washington is a home rule state, meaning local governments have autonomous authority and EMD cannot direct their actions in planning for or responding to emergencies.²⁷ Nevertheless, EMD and local emergency responders plan together, exercise together, and coordinate their emergency response activities together under the National Incident Management System (NIMS).

Commerce works as necessary with both the Association of Washington Cities and the Washington State Association of Counties communicating about energy emergency planning and response.

See Issues Section, Issue 5: Local Energy Assurance.

Tribal Governments

Tribes operate as sovereign governments. Generally, there have not been major interactions between tribes and the State in planning for critical energy infrastructure identification and protection. They do coordinate emergency planning and response efforts with State first responders and local governments in their tribal areas. In addition, they work closely with energy companies that serve their communities.

See Issues Section, Issue 5: Local Energy Assurance.

Private Sector and the Energy Industry

Washington established a single state Energy Coordinating Council to address critical energy infrastructure issues at the state level that are addressed nationally by two industry coordinating councils and by the Energy Sector Government Coordinating Council.²⁸ The state ECC includes membership from all energy sub-sectors (electricity, oil, natural gas)

²⁶ RCW 43.21G

²⁷ While generally true, in the worst emergencies Chapter 43.21G RCW grants the governor extraordinary powers to mandate actions to the public sector under an Energy Supply Alert (declared by executive order) and to the private sector under a declared Energy Emergency.

²⁸ At the national level, electricity has a separate coordinating council, and oil and gas together have a separate coordinating council. Also at the national level there is a government coordinating council. In Washington there is no real equivalent to the government coordinating council, and all the energy subsectors (electricity, oil, gas) have been put into a single coordinating council.

and key state agencies. The Department of Commerce provides basic coordination and staff work for the ECC. Industry representatives provide input from their companies in particular and their industries in general.

The state ECC is the primary forum through which the partnership between the State of Washington and its energy service providers address critical energy infrastructure issues.

“Efficiently and effectively securing the Energy Sector necessitates significant investment from all security partners. These investments require expenditures of time, energy, money, and other resources. While these expenditures typically are executively or legislatively mandated for government, private sector participation is mostly voluntary. Beyond existing regulatory requirements, participation by the private sector has been significant in the Energy Sector.”²⁹

The following points were adopted for this SSP directly from the federal energy SSP.

Reasons for private sector security partners to participate include opportunities to:

- Complement existing trade association and sector activities and programs, both voluntary and regulated;
- Share credible, timely, actionable threat information and predictive/trend analyses where possible;
- Apply a risk-based and prudent business approach for protecting assets that builds on existing industry practices and methodologies;
- Support flexible allocation of protective resources based on threats, consequences, and vulnerabilities;
- Improve risk management through exposure to effective practices and risk management tools;
- Provide a forum for reaching out to peers and addressing interdependencies;
- Provide a platform for coordination and communication between government and industry regarding protective actions and risk management activities;
- Build and further strengthen existing trusted relationships with private and public sector partners; and
- Inform government regarding impediments to protecting energy assets.

²⁹ Energy Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, 2010, p24.

Identify Assets, Systems, and Networks; Assess Risks; and Prioritize Infrastructure

Washington State is Well Along in the Process

Energy assets, systems, and networks that are critical to the State of Washington have already been identified, assessed, and prioritized to a great degree through two processes: activities by energy infrastructure owners and operators; and activities by the State IPSC in partnership with the industry.³⁰

Washington State has employed a number of processes, tools, and criteria to filter out facilities with a low state security risk and focus on facilities that are truly critical. The efforts to identify CI were for this purpose, to determine what priority infrastructure is. The earliest efforts were a common sense based application of scale - larger power plants, and pipelines with greater throughput, were listed as critical. It soon became clear, however, that scale was not always a good measure. For example, the largest natural gas pipeline in Washington bypasses the state almost completely, running from Canada through Washington to serve markets to the South; the pipeline hardly matters for energy supply to Washington State.³¹ More sophisticated criteria and analytical processes have been employed since, and additional analyses are planned.

In 2005, the energy sector leads on the IPSC, established three energy sub-sector working groups (oil, natural gas, and electricity). These groups were the focal point for communicating about and implementing the State and energy industry partnership for CI identification and protection. The three working groups have since merged into the state Energy Sector Coordinating Council. Over the next few years, the working groups developed recommendations for processes, criteria, and standards for identifying energy infrastructure critical to the State, and what to do with that information.

Each working group met and produced their top 15 list. The top ten energy CIs in the state were identified using the three sub-sector lists by the IPSC energy sector leads, the public sector alternate, and a representative of the Bonneville Power Administration. These top ten, along with the sub-sectors' top 15, became candidates for priority risk assessments. For example, the top ten facilities in each of the 18 infrastructure sectors are scheduled to

³⁰ The effort to identify critical infrastructure, assess its risks, and prioritize it, is not a purely sequential process. Identification, assessment, and prioritization happen in parallel, and are iterative processes, as well as sequential. While the federal energy SSP addresses these issues in separate chapters, this SSP considers them together. The federal energy SSP also has extensive chapters on CI/KR identification, risk assessment and prioritization. Much of the text is descriptive and accurately characterizes what Washington State and energy suppliers are doing to address infrastructure protection. Understanding the federal energy SSP is important to understanding what is taking place in Washington.

³¹ Of course attacks on the pipeline could be a threat to health and safety, and cause environmental damage. Also, the pipeline is connected with a transportation pipeline that does serve Washington and could be an alternative source of energy in times of short supply.

undergo vulnerability assessments through the Buffer Zone Protection Program (BZPP) consisting of a Buffer Zone Assessment, CARVER Critical Asset Prioritization, Tactical Plan Development, and Washington State Fusion Center Threat Assessment. Some, but not all of these assessments, are funded by DHS or Urban Area Security Initiative (UASI) grants.³²

In 2007 and 2008, the IPSC conducted a number of exercises to prioritize sectors. Priority sectors would be first in line for state resources and recommendations to federal agencies for CI risk assessments, i.e. the top ten facilities in a high priority sector would be assessed before the top ten facilities in a lower priority sector.³³

Eventually, the IPSC identified the threats/hazards to the State of Washington, developed and prioritized a Consequence of Action listing, and using a Pair-Wise Analysis rank ordered 17 sectors (now 18) based on the consequences of their loss.

Threats such as nuclear detonation (10 kilotons), pandemic influenza (biological disease outbreak), a major earthquake, floods, terrorist attacks, etc., were rated for threat, impact, and likelihood. Affects on the sectors were estimated, with the result that the Transportation Sector and the Energy Sector rated #1 and #2 respectively as the most critical sectors in the state.³⁴ The energy sector is considered by Washington State a top priority and a candidate for early assessments and protection.

As of the date of this publication, nine of the top ten energy facilities have completed the BZPP assessment with the final facility scheduled for assessment in 2011.³⁵ As mentioned above, priority CI will undergo additional analyses including interdependencies, supply chains, and “co-locations.” The “co-locations” analyses identify CI from different infrastructure sectors in the same geographic area. These analyses reveal areas where the juxtaposition of CI creates greater vulnerability and consequence assessments – raising the risk level for the area and all the facilities located there. For example a bridge under which important transmission lines, pipelines, or telecommunications lines are attached. The bridge itself may or may not be critical for transportation purposes, but it becomes critical because of the CI beneath it. Companies and organizations in other sectors may not be aware of the criticality of companion infrastructure or the existence of nearby CI that raises the risk to their own facilities.

Regardless of State efforts, the State of Washington recognizes that CIKR identification, risk assessment, and prioritization are primarily the purview of individual energy companies using industry generated standards.

³² Department of Homeland Security. Urban Areas Security Initiative *US Department of Homeland Security Office for Domestic Preparedness*.

³³ This has been applied generally; some CI facilities in lower priority sectors have been assessed before all the CI in higher priority sectors.

³⁴ Energy clearly would have been number 1, except that DHS directives have removed nuclear plants and dams from the energy sector (each have their own), and oil tankers and fuel pipelines were removed from the energy sector and categorized as transportation infrastructure.

³⁵ The State of Washington is scheduling other energy infrastructure for BZPP assessments if they are independently identified as critical by DHS, or local jurisdictions.

Assessment Criteria

The following criteria for assessment of consequences and system characteristics are from the federal energy SSP.³⁶

The consequences considered for the national-level comparative risk assessment are based on the criteria set forth in Homeland Security Presidential Directive (HSPD)-7. These criteria are divided into four main categories:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Direct and indirect effects on the economy (e.g., costs resulting from disruption of products or services, costs to respond to and recover from the disruption, costs to rebuild the asset, and long-term costs due to environmental damage);
- **Impact on Public Confidence:** Effect on public morale and confidence in national economic and political institutions; and
- **Impact on Government Capability:** Effect on government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

The Energy Sector has identified six general asset or system characteristics as important parameters for evaluating the vulnerabilities of the Energy Sector infrastructure and developing risk management programs.

- **Physical and location attributes.** These assist the Energy Sector to develop consequence, vulnerability, and protective strategies.
- **Cyber attributes.** Cyber systems that link and help monitor and control the energy systems are increasingly recognized as a potential vulnerability.
- **Volumetric or throughput attributes.** These define the extent of the damage, depending on the utilized capacity of the system, or points where the system may be capacity constrained.
- **Temporal/load profile attributes.** The Energy Sector has a strong temporal or time-dependent dimension affected by the season of the year and/or time of day.

³⁶ Assessing Consequences from Energy Sector-Specific Plan, 2010, p. 34. System Characteristics from p. 27.

- **Human attributes.** Highly trained and skilled personnel are key factors in a comprehensive Energy Sector security plan. The availability of skilled and experienced technical talent is a concern in the Energy Sector. Sustaining essential technical knowledge is critical to maintaining the sector’s safety, reliability, and security.
- **Importance of asset or system to the energy network.** Disruption of a particular gas pipeline or storage facility could impact the ability of numerous power generation assets to function because of lack of fuel, which could in turn affect key telecommunications facilities, water treatment facilities, transportation facilities, or other critical infrastructure.

Electricity Industry

According to the federal SSP, “maintaining reliability requires trained and skilled operators, sophisticated computers and communications, and careful planning and design. NERC and its eight Regional Reliability Councils have developed system operating and planning standards, based on seven key concepts, for ensuring the reliability of the four grids:

1. Balance power generation and demand continuously.
2. Balance reactive power supply and demand to maintain scheduled voltages.
3. Monitor flows over transmission lines and other facilities to ensure that thermal (heating) limits are not exceeded.
4. Keep the system in a stable condition.
5. Operate the system so that it remains in a reliable condition even if a contingency occurs, such as the loss of a key generator or transmission facility (the “N-1 criterion”).
6. Plan, design, and maintain the system to operate reliably.
7. Prepare for and respond to emergencies.”³⁷

Electric industry standards are developed by the North American Electricity Reliability Corporation (NERC) and approved and enforced by the Federal Energy Regulatory Commission (FERC).

³⁷ Energy Sector-Specific Plan, 2010, p26.

NERC has developed 180 reliability standards addressing issues from Resource and Demand Balancing to Personnel Performance, Training and Qualifications. Nine standards address CIP specifically.³⁸

Oil and Natural Gas Industry

According to the federal energy SSP, the oil and natural gas subsector has identified the following priorities:

- Assess security vulnerabilities at single-point assets such as refineries, storage terminals, and other buildings, as well as networked features such as pipelines and cyber systems; and
- Work toward resilient and secure cyber networks and SCADA systems to detect and respond to cyber attacks.³⁹

Reliability standards for the oil and gas industries are developed by the American Petroleum Institute (API). In addition, the American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), and APGA worked together to develop and release security guidelines.⁴⁰ These guidelines provide an approach for vulnerability assessment, a critical facility definition, detection/deterrent methods, response and recovery guidance, cyber security information, and relevant operational standards. The industry security guidelines incorporate a risk-based approach for natural gas companies to consider when identifying critical facilities and determining appropriate actions.

³⁸ www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection. "Cyber Security Standards CIP-001 through 009, have been approved by FERC and address the following requirements:

- Identification of critical assets and critical cyber assets
- Physical and cyber protection of critical cyber assets related to reliable operation of the bulk electric systems;
- Sabotage and incident reporting.

NERC's CIPC has issued a summary of several electric power vulnerability assessment methodologies, including a variation of DOE's Vulnerability and Risk Analysis Program methodology, in a suite of potential vulnerability assessment tools that electric power companies should consider using." [federal SSP]

³⁹ Energy Sector-Specific Plan, 2010, p46

⁴⁰ "Security Guidelines: Natural Gas Industry, Transmission and Distribution," Interstate Natural Gas Association of America, American Gas Association, American Public Gas Association, 2002.

Identify Issues; Implement Programs and Strategies; and Measure Effectiveness

PROCESS

This SSP should be considered a living document, with planned updates every four years, but also subject to minor changes continuously as programs are conceived and implemented. Much work in program development and implementation remains to be done.

During the SSP drafting process individual ECC representatives volunteered to take the lead in specific issue areas. Going forward, the ECC Co-chairs will work with the industry leads to develop and recommend a schedule for addressing issues. Based on that schedule, the ECC will initiate implementation of the SSP.

For example, water supply and wastewater infrastructure representatives on the IPSC and the Water Coordinating Council have requested a meeting with the ECC to discuss interdependencies between water and energy.

As another example, it is a priority for Commerce to ensure oil and natural gas supply shortages can be tracked on the new Washington State Energy Supply Disruption Tracking System that will be fully operational in October 2011 tracking power outages. This will address issues #3 (Mapping CI and Mitigation Analysis) and #9 (Emergency Response, Restoration and Recovery). See Issues List below.

As issues are addressed Commerce will track program development, implementation of mitigation measures, and report on evaluation results for inclusion in the Biennial CIKR Report, and for updates to the SSP.

In the following issues section, problems are categorized and described by unboxed text; mitigation programs and evaluation processes are described in text boxes.

Issues List

1. Data and Information Sharing
2. Communications
3. Mapping CI and Mitigation Analysis
4. Interdependencies
5. Local Energy Assurance
6. Infrastructure Out of State, Critical to Washington
7. Application of Federal and State Resources
8. Emergency Exercises
9. Emergency Response, Restoration and Recovery
10. Biennial CIKR Report and SSP Updates

Issue 1: Data and Information Sharing

Most energy infrastructure in Washington is owned and operated either by private companies, or by local government agencies such as Public Utility Districts (PUD) and municipal power companies. Virtually none is owned or operated by the State. These private and industry entities have serious concerns about providing significant data and information to the State about their most critical facilities, networks, and systems. They are concerned about the release of sensitive information, which may put their energy facilities and services at risk. Some are concerned that information about the risks to their infrastructure will result in legal suits or regulatory mandates that will increase costs or reduce control over their own assets.

The State however, like the federal government, has a “need to know” about critical energy infrastructure, from the simple understanding that energy companies are adequately protecting their infrastructure, to the appropriate allocation of government funds applied to infrastructure protection.

Both the federal government and the State have taken a number of measures to secure relevant data and information. Key steps were to enact laws exempting such information from public disclosure. A second key step in Washington was to limit the kind and amount of information energy companies need to provide to that which is absolutely necessary and not overly sensitive (see details below).⁴¹

While there continues to be some concern about sharing energy CIKR data and information with the State, the issue has essentially been resolved to the satisfaction of all involved, at least as it regards the identification and prioritization of critical facilities and basic information about them. Serious concerns remain about the sharing of more detailed information, information about individual facilities’ system impacts (e.g. consequences of loss) and vulnerabilities, and the companies’ protective decisions. Generally, however, Washington State does not require such specific information. Should such data and information become important to the State, they will initiate dialogue with the ECC to develop acceptable solutions.

Federal DHS Data Calls

Each year, DHS conducts a CIKR data call, asking states to provide them with CIKR data and information. The calls come with instructions for the kind and level of data to provide, which has significantly coalesced in recent years into a relatively set standard. The last few years, Washington has generally coordinated its own efforts to gather CIKR data with the DHS data calls. Often infrastructure designated as critical from a national perspective is deemed critical for the state as well.

⁴¹ See Appendix B for copies of the federal and state laws.

When DHS conducts a data call, the energy sector leads on the IPSC gather and submit the requested data and information. For the first data call, the energy sector leads called energy companies together to identify and prioritize the data. For subsequent data calls, energy sector leads have asked energy companies whether the existing lists are still accurate and to verify the information about them. That information has been submitted to DHS. (NOTE: for the most recent years, the lists from DHS have been accurate for Washington State.)

State Data Requests

Originally, in about 2005, the State asked energy companies to help them develop criteria for what infrastructure was critical to the state. Criteria were developed, and infrastructure was identified that fit the criteria. Discussions between the State and energy companies (and all other sectors) were held in an attempt to determine what information should be shared with the State. After significant discussions, and over a number of years, a solution was developed. The State legislature passed a law generally protecting CIKR data and information from disclosure, and energy companies agreed to provide the State with a limited amount of data and information. As time has passed, the State has generally kept its data requests in line with that provided DHS. Data and information shared with DHS is protected by federal law, that shared with the state is protected by state law.

Program

As has been established, energy companies, in conjunction with a DHS data call, or every two years at least, will provide the State basic data and information about changes in infrastructure criticality and priority, and associated information (such as capacity, contact information, etc.). DHS or State data requests that vary significantly from what has been established will be run by the ECC for discussion and response.

Evaluation

Energy Sector leads on the IPSC will conduct an annual assessment of data and information reporting concerns, looking for significant inaccuracies, incomplete data, conflicting data, complaints by energy companies, etc. Should findings point to serious data and information problems, Commerce will schedule a discussion with the ECC.

Industry CIKR Data and Information

In addition to the more general data and information requested by DHS and the State, there are industry and industry/federal government programs and standards for the identification and protection of CIKR.

Electricity Industry

As discussed above, the North American Electric Reliability Corporation (NERC) sets standards for transmission system reliability. The mandatory standards are enforced by the Federal Energy Regulatory Commission (FERC), and in the West administered by the Western Electricity Coordinating Council (WECC). Generating and transmission entities are subject to the standards, some of which address CI. These planning and operating standards are reinforced through compliance audits, sanctions, and penalties that are enforceable across North America.

The State expects standards to be reasonable and effective and hopes for high levels of compliance by subject entities. As the Washington State representative on the Western Interconnection Regional Advisory Board (WIRAB), Commerce has access to WECC reliability information and a voice in advising FERC on the NERC standards.

Program

- Annually, Commerce will identify all in-state subject entities, and monitor compliance.
- Commerce will identify key compliance concerns. If the concerns relate to industry patterns, for example if a high number of entities are struggling with the same requirements, Commerce will raise the issue with the ECC and discuss strategies for success and whether the State can assist in any way.
- If the concerns are about an individual utility or generator, Commerce will contact the appropriate regulator, or the entity itself in the case of an Independent Power Producer (IPP), to discuss its concerns. Commerce will ask whether the State can assist in any way.
- Periodically, as issues arise, Commerce will report to the ECC on WIRAB activities, and will discuss with the ECC whether there is anything the State can do through WIRAB to ensure reasonable and effective standards are developed and that they are administered and enforced in a reasonable and effective way.

Evaluation

The program itself is essentially an evaluation process. Commerce will regularly ask the ECC if program goals are being met, and if not, develop appropriate solutions with the ECC.

Oil and Gas Industries

A combination of standards and guidelines produced by different government agencies and industry associations direct CI protection in these industries. Following are key examples.

- “Guidelines for Developing and Implementing Security Plans for Petroleum Pipelines,” American Petroleum Institute (API), 2002.

- “Security Guidelines for the Petroleum Industry,” Third Edition, API, April 2005.
- “Chemical Industry Anti-Terrorism Standards, Interim Final Rule,” DHS-2006-0073, RIN 1601-AA41, 6 CFR Part 27, DHS, 2011
- “API Recommended Practice 70, Security for Offshore Oil and Natural Gas Operations,” API, 2003.
- “Transportation Worker Identification Credential (TWIC) program,” addresses personnel security in the maritime industry, DHS. Find program at: http://www.tsa.gov/what_we_do/layers/twic/index.shtm
- “Security Guidelines: Natural Gas Industry Transmission and Distribution,” American Gas Association (AGA), Interstate Natural Gas Association of America (INGA), and American Public Gas Association (APGA), 2002.

Again, as with electricity standards, the State expects standards and guidelines to be reasonable and effective and hopes for high levels of compliance. How will the state know this is being achieved?

Program

- A number of different state agencies have access to oil company facilities, including the Military Department, Washington National Guard, EMD, and the Washington State Patrol (WSP). The WUTC Division of Pipeline Safety has access to and information about pipeline and terminal facilities. Commerce will communicate with these agencies to see if there are any concerns about oil and petroleum product facilities. Generally, Commerce will contact individual companies if concerns are raised.
- Commerce will schedule specific CIKR discussions with the ECC to see if there are ways the State can assist oil, petroleum product, and natural gas companies in their CI identification and protection efforts.

Evaluation

- Program must be better conceived before an evaluation process can be developed.

Issue 2: Communications

There are multiple types of communications important to CIKR protections, for example, company to company “best practices,” government to industry security warnings, and industry to government CIKR status reports. The following types of communication are addressed in this SSP:

- State to industry communications (e.g. reporting requests, real time warnings);
- Industry to State communications (e.g. CI status, reporting concerns);
- Company to company communications (e.g. best practices, regulatory risks); and
- State and industry communications to others (e.g. customers, other sectors).

The key for this SSP is to identify the types of communications required and the medium by which those communications will be made.

State to Industry Communications

The State has access to a number of sources of data and information helpful to industry’s CIP efforts. These include analyses and best practices reported by the federal government and other States, the availability of government programs and funding to assist in industry’s CIP efforts, and risk warnings (both long term and real time threats).

Program

Commerce will take the lead in providing general government generated CIKR information about analyses, best practices, programs and funding to industry. To do so, Commerce will pass the information to the private/industry sector lead on the IPSC (also co-chair of the ECC) who will determine what should be passed on to the industry, and to whom.

The Washington State Fusion Center has the responsibility to contact industry and energy companies about long term and real time threats as necessary.⁴² They use multiple media such as the Northwest Warning Alert and Response Network (NW-WARN) for general information and personal contact with selected energy companies as appropriate.

⁴² Fusion centers bring together key law enforcement agencies such as the FBI & Washington State Patrol (WSP) along with terrorism consultant analysts to locate and analyze intelligence about threats to infrastructure and to share analytical results with law enforcement and infrastructure owners and operators (such as electric utilities).

Evaluation

ECC members agree to raise concerns about State to industry communications to the ECC. If concerns are not raised, the ECC will assume that communications are working and appropriate. If concerns are raised, Commerce will schedule a discussion by the ECC.

Industry to State Communications

The State of Washington has a need to know about several aspects of energy CIKR, including:

- The identification and prioritization of CIKR (dealt with in the Data and Information Sharing section above);
- Energy supply problems, impacts, and estimates of supply and service restoration (dealt with in the Emergency Response Section below);
- Status of CIKR protective efforts; and
- Reports of suspicious activity and incidents.

Program

Commerce, working with the ECC, will develop a basic biennial survey for energy companies to report to the State the status of their CIKR identification and protection efforts. The survey will be constructed to acquire very basic information, such as:

- Status of CIKR identification and prioritization;
- Status of risk assessments;
- Status of identification of mitigation actions;
- Status of mitigation implementation; and
- A simple schedule of expected actions going forward, including updates and reassessments.

Reports will provide sufficient information to allow the State to understand that quality and thorough analyses are being conducted. Reports will also indicate to what degree mitigation actions rely on response and restoration versus prevention.

Evaluation

Commerce will review reports and provide a briefing to the ECC. Any general concerns (such as industry patterns) will be scheduled for ECC discussion. If the concerns are for an individual company, Commerce will contact the company directly, or the appropriate regulator to notify it of its concerns. Commerce will ask whether the State can assist in any way.

Company to Company Communications

The CIKR identification and protection efforts of all energy companies should be enhanced when companies share information about best practices, threat warnings, suspicious activity and incidents, and government activities. This occurs through informal, trusted networks and affiliations with working groups (e.g., WECC Physical Security Work Group, AGA/EEI Security Committees, etc.)⁴³

Program

Commerce will work with PSE to list and describe the key ways energy companies communicate this information. A draft list will be provided the ECC for discussion. A final list will be sent to all major energy companies in Washington.

Evaluation

Commerce will include questions about this program in its biennial survey.

Industry and State Communications to Customers and Others

There may be multiple audiences with whom the ECC wishes to communicate. For example, the electricity sector may have key messages about its CIKR efforts that it wants to communicate to other sectors, or to energy customers, or to other governments.

Program

The Co-chairs or ECC members will raise external communications issues with the ECC for discussion. The ECC will identify target audiences, messages, media and processes for communicating CIKR identification and protection information to

⁴³ EEI is Edison Electric Institute.

others.

Evaluation

ECC members will report any concerns about the appropriateness and effectiveness of external communications. Commerce will schedule the concerns for discussion by the ECC. The ECC will develop appropriate solutions as necessary.

Issue 3: Mapping CI and Mitigation Analysis

Geographic Information System (GIS) mapping of CI data is a key State goal to support mitigation analyses and response operations. The following analyses are anticipated:

- Priority Analysis – Where is the most critical infrastructure?
- Density Analysis – Are there places where energy CI exists in large numbers?
- Co-locations Analysis – Are there places where energy CI is juxtaposed to CI from other sectors?

Mapping priority analysis will allow the State to quickly locate the highest priority CI in the State; for risk and threat analysis, for imminent attack defense, and for protection and restoration prioritization during and after incidents. The State has not yet determined how it will implement such defensive and protective efforts.

Mapping density analysis and co-locations analysis will allow the State (and industry) to identify critical areas, where area wide mitigation efforts may be advisable in lieu of or in addition to individual facility mitigation actions.

Program

Commerce will track the State’s progress in GIS mapping of energy and other sectors CI, and in the conduct of CI analyses. Commerce will periodically report such progress to the ECC, and schedule discussion as necessary. As with other relevant communications, Commerce will report the ECCs’ concerns to the Infrastructure Protection (IP) program at EMD, and to the IPSC.

Evaluation

The mapping program is essentially a program of EMD, not of the energy sector. The ECC’s “program” at this time is to track EMD’s program.

Issue 4: Interdependencies

The interdependencies of all CI sectors is commonly understood to be important information to have and, at the same time, information that has not been developed on a widespread basis, at least formally. The following issues are key:

- Just in time supply chain practices make interdependencies more important, because key products and services the energy industry relies on for continuity of operations may not be readily available without explicit efforts to ensure it; and
- Energy, and electricity particularly, represent top priority infrastructure upon which all other sectors profoundly depend, making it extremely important that the energy industry addresses its own dependencies and understands how others depend on it, so that extremely key supplies and services can be assured.

Program

The IPSC energy sector leads will develop, in consultation with the ECC, processes to discuss interdependency issues with key sector representatives. The IPSC energy leads will set up meetings as appropriate with other sector representatives and with their coordinating councils. The sector leads will report findings back to the ECC, and to the IPSC and IP program at EMD as necessary.

Evaluation

The energy sector leads, working with other sector leads, and the State IP program managers, will review the interdependency findings. Concerns and issues will be developed to discuss with each sector coordinating council. Responses will dictate any additional steps to take.

Program

Commerce, working with the ECC, will develop a basic biennial survey for energy companies to report to the State the status of their Continuity of Operations Plans. The survey will be constructed to acquire very basic information, such as:

- Status of company COOP plans (e.g. percent complete);
- Actions planned and a brief implementation schedule if COOP plans are not complete; and
- When COOP plans will next be updated?

Reports will provide sufficient information to allow the State to understand that quality and thorough plans have been produced. The biennial survey will be conducted in

conjunction with the survey on CI identification and protection status.

Evaluation

Commerce will review reports and provide a briefing to the ECC. Any general concerns (such as industry patterns) will be scheduled for ECC discussion. If the concerns are for an individual company, Commerce will contact the company directly, or the appropriate regulator to notify it of its concerns. Commerce will ask whether the State can assist in any way.

Issue 5: Local Energy Assurance

The State assumes that federal energy assurance activities will be conducted by federal agencies, except as they implement programs through the states, or local governments, or directly with energy companies. The issue of concern is addressing local energy assurance issues (as opposed to federal or state programs operating through local governments).

The State encourages energy companies to contact local jurisdictions in which they have major operations to see what energy assurance concerns they have in regards to energy CI. There may be, for example, infrastructure of importance to the local jurisdictions that is of less concern to the State or federal government. For example, a local industry may be absolutely critical to the economic health of a small town. The State encourages energy companies to discuss CI issues with local jurisdictions and to see if local concerns can be addressed.

Tribal governments also exist in localized areas within and beside utility service territories. Their petroleum product supplies are drawn from regular market suppliers. In general, they have some of the same concerns that cities and counties do. The State encourages energy companies to contact tribal jurisdictions in which they have major operations to see what energy assurance concerns they have in regards to energy CI.

Program

The ECC co-chairs will periodically identify issues of local energy assurance (EA) concerns through meetings, exercises, documents and so forth, and share such information with the ECC as appropriate. On a biennial basis, or more often as necessary, Commerce will schedule a discussion with the ECC about local EA issues. The ECC will identify key issues of concern (if any), and develop, if possible, ways to resolve those issues.

Evaluation

On a biennial basis, in conjunction with other biennial actions, the ECC will assess whether local EA issues are being sufficiently resolved through the Ad Hoc program (above), or whether EA issues represent significant on-going concerns. If it remains a problem, the ECC will attempt to identify alternative ways to address the local issues.

Issue 6: Infrastructure Out of State, Critical to Washington

It is no secret that Washington State relies heavily on energy infrastructure outside its borders. We rely on large energy storage dams in the upper Columbia River basin in British Columbia. We rely on oil production in Alaska, California, Canada, and other foreign nations for all of our crude oil supply. We rely on British Columbia and Rocky Mountain states for all of our natural gas supply. And we rely on the energy infrastructure in all these places to produce that energy and get it to us.

In the State's early discussions with energy companies about CI, Commerce learned about specific out of state corridors, facilities, networks and systems that Washington depends on. While the State lacks the authority to take protective actions elsewhere, there may be ways to influence it, both through State actions and through the actions of individual energy companies that are directly dependent on those resources and facilities for their own energy supplies and services.

Program

The ECC will identify process and implementation options to identify infrastructure outside the State that is critical to the State, and, if necessary, ways to assure or enhance its protection.⁴⁴ As with Washington's own CI, the solution may simply be for owners and operators of that infrastructure to communicate their recognition of Washington's concerns and, if appropriate, report on the status of its protection.

Evaluation

The ECC will evaluate the results of the process in meeting the program's goals; e. g. CI is identified, and its protection is underway/completed. If unsatisfactory, the ECC will attempt to identify alternative solutions.

⁴⁴ For example, Commerce, EMD, and some key energy companies are working with British Columbia counterparts to strategize cross border CI identification and protective efforts.

Issue 7: Application of Federal and State Resources

There are a number of federal programs, offered directly from federal agencies or passed through state or local governments, meant to assist energy companies in their CI protection efforts. For example, the Buffer Zone Protection Program (BZPP) is a DHS risk assessment program that attempts to identify vulnerabilities to areas surrounding CI. DHS contractors work with energy companies and local law enforcement to implement the program and report findings and recommendations to the companies.

Program

Commerce, working with the EMD IP program, will compile a list (and descriptions) of all known CI funding opportunities. The ECC will review and edit the list, and recommend actions for taking advantage of the program and funding opportunities. Actions recommended may be as simple as communicating the information to energy companies. Commerce will update the list annually.

Evaluation

ECC members that take advantage of such programs or funding will report their experiences to the ECC. Commerce will record comments provided and work with the ECC to consider appropriate actions. For example the ECC may want to communicate their experiences to other energy companies, or have Commerce or the ECC provide feedback to program representatives or grantors.

Issue 8: Emergency Exercises

The most important thing to do to prepare for energy emergencies is to develop response plans. Testing those plans through exercises is the next most important thing. The U.S. Department of Energy, Commerce, and the ECC encourage all energy companies in Washington State to regularly conduct or participate in such exercises.

Emergency response plans can address many kinds of emergencies, from spills to earthquakes or floods to energy supply shortages. As infrastructure has become more interdependent, and energy infrastructure has become more important, the importance of response plans and exercises has increased greatly. Especially in the case of certain CI, where preventative measures are either impractical or too expensive, response becomes the mitigation action of choice, and so response capability has increased in importance.

Program

Commerce, working with the ECC, will develop a prioritized list of key threat/disaster scenarios relating to energy CI, and develop options, including funding, for exercising those scenarios.⁴⁵ Commerce will develop an initial target schedule and update and maintain it as necessary.

Evaluation

After major energy emergencies requiring State response, Commerce and affected energy companies will report their experiences to the ECC. Lessons learned will be incorporated into plans for future exercises.

⁴⁵ A number of exercises are already planned, or recently have been conducted. Commerce conducted two in-state exercises in June and August 2011 to test the new WAESDTS. A large regional (multistate) exercise conducted by USDOE is also planned for November 29 & 30, 2011, in Phoenix AZ. All three exercises are required under a grant Commerce received from the USDOE using American Reinvestment and Restoration Act (ARRA) funds. Some ECC utilities participated in the intrastate exercises. Others may be invited to the Intrastate Exercise at the discretion of the US Department of Energy.

Issue 9: Emergency Response, Restoration, and Recovery

The federal Department of Homeland Security (DHS) has made enhancement of emergency response capabilities a top priority – especially for critical energy infrastructure. Not only would a resilient system result in reduced negative impacts (to life/health, economy, etc.), DHS believes if terrorists knew a system would be quickly and fully restored, it would discourage attacks. In addition, because response and restoration are the mitigation actions of choice for “protecting” some critical energy infrastructure, having superlative response and restoration capabilities is imperative.⁴⁶ Also, having high quality response and restoration capabilities means better energy system reliability regardless of whether facility failure is due to human actions or natural disasters.

All major energy companies in Washington have emergency response plans, whether a requirement of their regulator or governing board, or because it is a critical necessity. The Department of Commerce is required by statute to develop and update energy contingency plans governing state response.⁴⁷ The Washington State Energy Assurance and Emergency Preparedness Plan is available on the Commerce web site at:

<http://www.commerce.wa.gov/site/975/default.aspx>

A key responsibility of Commerce during energy emergencies is to determine the nature, extent, and potential duration of the emergency. During disasters, Commerce staffs the Energy Desk in the State Emergency Operations Center and advises the State on the energy situation and how the State might assist energy companies in their response efforts. The only way Commerce can do its job is with the concurrence and support of the industry.

In 2009, Commerce received a grant from the US Department of Energy to develop a map based energy supply disruption tracking system.⁴⁸ At the time of this writing, Commerce anticipates that the Washington Energy Supply Disruption Tracking System (WAESDTS) will be fully operational to track power outages by October 1, 2011.

The WAESDTS will have the following capabilities:

- Map the locations of all critical infrastructure;
- Map the locations of all major energy production, processing, transportation, control and storage facilities;
- Map and track power outages; and

⁴⁶ As discussed elsewhere in this SSP, many important electric system facilities are visibly scattered all across the landscape. They cannot cost effectively be hidden, hardened, duplicated, or substituted for, preferred protective measures. The way to best “protect” them is to have the capability to restore their services rapidly.

⁴⁷ RCW 43.21F.045(a).

⁴⁸ Grant was from the American Reinvestment and Restoration Act of 2009 (stimulus funds). Grant number DE-OE000060.

- Map and track solid, liquid, and gaseous fuel supply constraints.

Program

Commerce will periodically update its contingency plan. All energy companies will be provided an opportunity for input and comment.

Annually, each Fall, Commerce will send out a Storm Preparedness Day e-mail to contact all energy companies in the State with information about updating their emergency contact information, and preparing for the storm season.

The ECC will periodically communicate to all energy companies in the State its support for partnership between the State and energy companies in energy emergency response and restoration and encourage participation in developing State plans, providing energy supply disruption information, updating plans and contact information, and participating in energy emergency exercises.

Evaluation

ECC members will keep the ECC informed when they hear any concerns about how the State and energy companies are working together (or not) to prepare for energy emergency response. The ECC will discuss alternatives for addressing any concerns. After events that include major energy shortages or outages, the ECC will briefly review what happened for lessons learned. Lessons learned will be shared with the appropriate energy companies.

Issue 10: Biennial CIKR Report and SSP Updates

This SSP will need to be reviewed and updated periodically.

Program

- Every two years, Commerce will produce a biennial CIKR report on all the programs included in this SSP. The ECC will review drafts of the report and approve a ECC version that will be shared with all energy companies in the State and with appropriate government agencies. Sensitive data and information will be protected in the process.
- The ECC will maintain a continuous review policy and make changes to this SSP as necessary. Should major changes be necessary, the ECC will develop a review process and schedule its implementation.
- With Commerce as the lead, the ECC will schedule a complete review and SSP update every 4 years, or when the USDOE produces an update of the federal energy SSP.

Appendix A: Coordinating Council

State Agencies
Department of Commerce
Washington Utilities & Transportation Commission
Electric Utilities
Avista Utilities
Bonneville Power Administration
Clark Public Utilities
PacifiCorp
Puget Sound Energy
Seattle City Light
Snohomish Co. PUD #1
Natural Gas Companies
Avista Utilities
Puget Sound Energy
Williams Pipeline
Oil Companies
BP
BP - Olympic Pipeline
ConocoPhillips
ExxonMobil
Shell – Puget Sound

Appendix B: Federal and State Laws Protecting CI Data and Information

Federal Law

[From the federal SSP]⁴⁹

The Energy Sector expects that all data and information voluntarily provided to DHS or DOE by industry will be protected from release by Protected Critical Infrastructure Information (PCII) or other appropriate classification procedures. The Energy Sector will work with the PCII Program Office within the DHS Office of Infrastructure Protection (OIP) to apply provisions of the CII Act, and the implementing regulations contained in 6 CFR Part 29, to critical infrastructure information that is not customarily in the public domain and is voluntarily submitted to DHS. Other government sector security partners will work to protect sensitive information from unintended release. DOE will not request or hold sensitive critical energy infrastructure information beyond what it currently holds or collects unless and until it can protect this information from release, and will use any such information for national infrastructure protection purposes only. The Energy Sector will also work with State, local, and tribal authorities to ensure that information provided to those non-Federal authorities is also appropriately protected from release and not used for purposes other than infrastructure protection and recovery. Through NARUC, States are developing models for information sharing and protection in the State regulatory context, and public utility commissions are engaging in training and network-building that will enable each State to provide the right information to the right parties when needed.

State Law

In Washington State in 2005, the legislature passed a law addressing the disclosure of data and information of a security nature. Data and information gathered in the development of this Sector Specific Plan and in its implementation is covered by this law which is contained in the Public Records Act, Chapter 42.56 RCW (Revised Code of Washington). The law follows:

Revised Code of Washington, 42.56.420 Security

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,

⁴⁹ Energy Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, US Department of Energy, DHS, 2010

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, or secure facility for persons civilly confined under chapter 71.09 RCW, 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, secure facility for persons civilly confined under chapter 71.09 RCW, 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.