Biennial Report on Critical Energy Infrastructure and Key Resources, Washington State

Washington State Energy Coordinating Council
March 2013

April 3, 2013

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

SUBJECT: Release of Biennial Report on Critical Energy Infrastructure

We are pleased to present the first Biennial Report on Critical Energy Infrastructure, Washington State, a product of the Washington State Energy Coordinating Council (ECC). The report is a requirement of the state's Sector Specific Plan for Critical Energy Infrastructure (SSP). The subject of the report is the status of implementation activities in ten issue areas of the SSP over the reporting period.

This is the first report after adoption of the SSP in November 2011, and covers a short reporting period of a little over a year. Subsequent reports are expected to cover more extensive implementation over a longer period.

The report is intended to provide an understanding of the primary efforts being taken to identify and protect energy infrastructure critical to the State of Washington. It will inform ongoing efforts, and should raise public confidence in the process and results.

Special thanks to the 13 oil, natural gas, and electric utility companies that have joined the Department of Commerce and the Utilities and Transportation Commission to form the ECC, and to partner with the agencies to identify and protect energy infrastructure that is critical to the State.

Special thanks as well to the 30 energy companies that provided survey responses to support development of this initial biennial report.

Sincerely,

Mark Anderson, Co-Chair Energy Coordinating Council

Mary Robinson, Co-Chair Energy Coordinating Council

Table of Contents

Executive Summary

This Biennial Report is intended to provide an understanding of the primary efforts being taken to identify and protect energy infrastructure critical to the State of Washington. It will inform ongoing efforts, and should raise public confidence in the process and results.

The report is a requirement of the Washington State *Sector Specific Plan for Critical Energy Infrastructure* (SSP), which is an implementation plan describing how the State and energy companies partner together to identify and protect critical energy infrastructure. The SSP is a product of the Energy Coordinating Council (ECC), a public/private entity, established specifically for the purpose of writing and implementing the SSP.

The SSP identifies ten issue areas with problems to address, and recommends subsequent mitigation and evaluation programs. The report provides a brief description of those programs and their status. As this is the initial report, addressing a short reporting period, significant elements of the SSP remain to be implemented.

Issue areas of significant State/Energy Industry partnership during the reporting period include:

- Completion of mapping of all major electricity, natural gas and oil industry infrastructure in the state, and identification as critical/not critical (oil and natural gas infrastructure was added in 2012).
- Conduct by the State of the Evergreen Earthquake Series Exercises simulating fuel and power disruptions. Commerce and a number of energy companies participated in both planning and exercise play.
- Significant attention was paid to the report itself. A survey was created and a report concept and format developed and approved. In subsequent years, these can be modified, rather than recreated.

Data and information reported in the plan came from ECC discussions, research by Commerce, and results of a Critical Infrastructure, Key Resources (CIKR) survey. The survey was sent to 59 electric utilities serving Washington, all oil refiners and petroleum product pipeline operators in the state, and major natural gas transmission and distribution companies.

Survey responders included most major energy companies in the state, supplying electricity to almost 90 percent of electricity customers, all users of petroleum fuels, and just under 80 percent of natural gas customers. Therefore energy infrastructure that is critical to the state is almost assuredly addressed by the survey and report.

- Thirteen of 21 survey responders indicated that they have CIKR, and all have taken steps to identify and protect it.
- Most of the work that needs to be done to identify and protect *existing* CIKR has been done. Eight of the 13 companies (61.5%) agreed that “Facilities and processes have been secured. We do not see the need for extensive, additional efforts.” Four of the 13 (30.8%)

said they were "80 percent of the way there." Only a single company thought the majority of their work was still ahead.

- When asked about the amount of time it takes to identify and protect CIKR, the investment it requires, and the complexity of the work, 12 of 13 companies (92.3%) indicated moderate to high in all categories, with most responses in the medium-high and high when taken together. Nearly all the companies indicated that CIKR identification and protection represents an effort that is complex, takes significant time, and costs a lot. It is not known to what degree this will continue, but in the electric utility industry, for example, compliance with Critical Infrastructure Protection (CIP) standards represents a major, ongoing requirement.

Looking forward over the next two years, the ECC has identified a number of areas for focused State/Industry partnership.

- Regarding Data and Information Sharing, the State will participate in at least one full National Critical Infrastructure Protection Program (NCIPP) Data Call, and will work with energy companies to ensure reported data are complete and accurate.
- Under the auspices of the newly reorganized state Infrastructure Protection Subcommittee (IPSC), Commerce, per the SSP, will facilitate sector discussions between Energy and Transportation, and Energy and Water.
- Also under the IPSC, Commerce will encourage the conduct of key Critical Infrastructure (CI) mitigation analyses by the State, including density analysis (where priority CI exists in large numbers) and co-locations analysis (where energy CI is juxtaposed to CI for other sectors). Results will be shared with energy CI owners and operators to inform ongoing mitigation efforts.

Purpose and Scope

This *Biennial Report on Critical Energy Infrastructure and Key Resources* is a requirement of the *Washington State Sector Specific Plan for Critical Energy Infrastructure* (SSP). Both the SSP and the report are products of the Washington State Energy Coordinating Council (ECC), a public/private entity, established specifically for the purpose of writing and implementing the SSP.[1] The report is due every other January. This 2013 edition is the first.

The SSP directs, in broad terms, the partnership between the State of Washington and suppliers of energy and energy services in the state, in their joint responsibility to identify and protect energy infrastructure and key resources that are critical to the state.[2] The subject of the report is

[1] The first edition of the SSP was produced by the ECC in November, 2011. The ECC is described in more detail in the SSP itself, and in the Background section of this report. ECC members are listed in the SSP.
[2] Critical Infrastructure primarily as reported to the State Infrastructure Protection Subcommittee for State and Federal monitoring purposes. Infrastructure may also be "critical" to an energy company itself or to a local

the status of the SSP's implementation activities in ten issue areas over the reporting period. The report is intended to inform future implementation efforts and SSP updates.

This first edition reviews the brief period from adoption of the SSP in November, 2011 to December 2012. Subsequent editions are planned to review each two-year period between reports. Because this is the first report, there is a greater focus on background information than is anticipated for subsequent reports. Because the reporting period is short, and implementation is just beginning, there is less to report on than is expected for future reports.

The SSP establishes a significant work effort to achieve its goals, with the expectation that implementation will occur over time, with different foci during any two-year period. For this initial reporting period, there only has been time to begin implementation in a few of the issue areas.[3] In addition, some requirements of the SSP, such as the conduct of a biennial Critical Infrastructure, Key Resources (CIKR) survey (to support the report), required the initial development of the survey, which took significant time. In subsequent years, the survey can be revised for use. The following statement is from the SSP, and explains the nature of its implementation.

> *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. ...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.*[4]

To truly understand the implications of this report, the reader should become familiar with the SSP itself, which can be found on the Energy Emergencies and Security Program website of the Washington State Department of Commerce (Commerce).

Background

The following background information can be found in much greater scope and detail in the SSP.

Before the terrorist attacks 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). The mission of the IPSC, as stated in the *Washington Infrastructure Protection Plan* (WIPP) is to "Work with our public and private

---

community, yet not rise to the level of state or federal concern. Mitigation programs of the SSP may help to protect these facilities and systems as well. Key Resources may include personnel.

[3] Just over a year to begin implementation of the plan, gather information, produce, and complete the report.

[4] SSP, page 8

sector partners to identify and protect critical infrastructure and key resources against all hazards."[5]

The IPSC determined that each of 18 federally designated infrastructure sectors should establish a Coordinating Council, and develop and implement a Sector Specific Plan 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 Washington State Energy Coordinating Council (ECC). The ECC is made up of representatives of local public utilities and private oil, natural gas, and electric utility companies doing business in the State of Washington, and employees of state agencies with energy emergency and security responsibilities.[6] The ECC is the primary forum where the state/energy industry partnership to identify and protect energy CIKR is being implemented.

The SSP is the implementation plan for that partnership and was produced by the ECC in accordance with the *National Infrastructure Protection Plan* (NIPP), the *Washington Infrastructure Protection Plan* (WIPP) and the *National Energy Sector Specific Plan*.[7] The NIPP establishes a risk management approach to identify and protect CIKR, which all subordinate plans follow, and the national energy SSP provided a sector specific model for producing the state energy SSP.

The SSP recognizes the following key factors about CIKR identification and protection.

- The State role is one of support and coordination. Nearly all energy infrastructure in the state is owned and operated by private companies or local public utilities. They have the primary task of identifying and protecting CIKR.

- All energy companies have undertaken major efforts to identify and protect CIKR. Ensuring CIKR identification and protection 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 expensive. An appropriate "protective" mitigation measure may be to improve emergency response preparedness and capabilities.

Energy Sector Vision Statement

The following vision statement was adopted for the state SSP from the national energy SSP.

[5] Washington State Infrastructure Protection Plan, Washington Military Department, February 2008.
[6] Washington State Department of Commerce and Washington Utilities and Transportation Commission.
[7] All three plans are available on the Energy Emergencies and Security Program website of the Washington State Department of Commerce.

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

The following energy sector security goals were adopted for the state SSP from the national energy SSP.

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.[8]

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.

Assessment Criteria

The following criteria for assessment of consequences were adopted for the state SSP from the national energy SSP.

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:

[8] CIP – Critical Infrastructure Protection

• **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.

System Characteristics for Identifying Infrastructure Vulnerabilities

The following System Characteristics were adopted for the state SSP from the national energy SSP.

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.
- **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.

Status of Implementation Efforts

The SSP organizes implementation actions into ten issue areas, as follows:

1. Data and Information Sharing
2. Communications
3. Mapping Critical Infrastructure 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

The SSP identifies concerns and establishes, or recommends the need for, mitigation programs, and a plan for evaluating program effectiveness in each area. Each program and evaluation plan is reproduced in this report with a brief discussion of the issue and a status report.[9]

Issue areas, like mitigation programs and evaluation plans, are expected to change over time, as new information arises, as lessons learned are shared, and as evaluation reports are processed. Cyber security, for example, is not addressed as a separate issue, because cyber systems, like personnel, extend into all issue areas. Yet cyber security is increasingly referenced in and of itself as a major security concern. It may make sense to revise the SSP to include cyber security as a distinct issue area.

Status Summary

When the SSP was completed in November 2011, state and energy company CIKR efforts were already underway, with future efforts planned. For example, the State was preparing to conduct a series of major earthquake exercises during the summer of 2012, the Department of Commerce was implementing its new Washington State Energy Supply Disruption Tracking System (WAESDTS), and each energy company was working on its own security enhancements. Most electric utilities were deeply involved in addressing compliance requirements for meeting federal transmission reliability standards.[10] CIKR efforts were not informed by the SSP at that time.

Nevertheless, CIKR efforts over the reporting period can be described in reference to the ten issue areas of the SSP. The focus of the State and energy companies' partnership efforts was in the following areas.

- Mapping Critical Infrastructure and Mitigation Analysis

[9] A detailed discussion of issue area concerns is in the SSP but is not included in this report.

[10] Standards developed by the North American Electric Reliability Corporation (NERC) for the Federal Energy Regulatory Commission (FERC).

During 2012, the Washington Energy Supply Disruption Tracking System (WAESDTS) was completed. Oil and natural gas infrastructure was mapped, so fuel supply disruptions can be tracked alongside power outages.

Commerce reported to the ECC in 2012 that all critical energy infrastructure in Washington had been mapped by the State Infrastructure Protection Program at the Military Department, Emergency Management Division. Mitigation analyses are ongoing, however some key analyses such as the co-locations of different sector CI have not been done.

- Emergency Exercises
  The State conducted the Evergreen Earthquake Exercise Series consisting of functional, logistics and tabletop exercises. This was a major FEMA/State collaboration involving federal, state, and local government agencies, and major energy companies in the Puget Sound region.

- Biennial CIKR Report and SSP Updates
  Every biennial report period, by definition, will include a focus on the biennial report. During this initial, short period, extra time was required to develop a report concept, produce and conduct an initial survey, conduct analyses and draft an initial report.

Issue by Issue Status

1. Data and Information Sharing

States and the federal government need to know some things about the criticality of infrastructure, because governments have key roles to play in ensuring the security of the state. Infrastructure owners and operators must share the information, which may be sensitive for both security and proprietary reasons. It is feared that governments' information transparency laws, such as the Freedom of Information Act, will put the data and information at risk of public dissemination. This became a serious issue soon after governments first began to assert their need to know.

Both the federal government and Washington State have addressed this issue through dialogue with infrastructure owners and by adopting legislation to protect the confidence of security data.[11] Washington State, as well, through the IPSC, worked diligently to define what limited information was truly required by the State.

[11] Both the federal and state laws are included in appendices in the SSP.

The SSP says that this issue "…has essentially been resolved," so that the state/industry partnership to identify and protect CIKR can proceed. Nevertheless, data and information sharing will remain a sensitive issue requiring due diligence by all involved.

Program (State Data Requests)

"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."

Status

Commerce has conducted data calls in conjunction with the state Military Department, Emergency Management Division (EMD), Infrastructure Protection Program since their inception. In 2012, DHS decided not to hold a full National Critical Infrastructure Protection Program (NCIPP) Data Call. Instead, data were reviewed for technical changes.

A full NCIFF Data Call is planned for 2013 and expected to be initiated by DHS in March. Commerce will participate and communicate with energy companies to update existing CIKR information and determine whether there should be facilities removed or added to the database, or changes in priority. Unless DHS significantly changes criteria, Commerce anticipates minimal non-technical changes to CIKR in the database.

Commerce will follow the SSP directions for implementing evaluation of the process.

Program (Industry CIKR Data and Information - Electricity Industry)

"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 Western Interconnection Regional Advisory Board (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."[12]

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."

Status

Electric utility compliance with transmission standards regulated by the Federal Energy Regulatory Commission (FERC) is a major issue, one of the largest and most sensitive regulatory endeavors in electric utility history. Electric utilities face mandatory, enforceable, reliability standards, that are numerous, detailed, and complex, and for which demonstration of compliance has become a difficult, time and resource consuming endeavor. During 2011 and 2012, states making up the Western Interconnection Regional Advisory Board (WIRAB), worked with the Western Interstate Energy Board (WIEB) of the Western Governors Association (WGA), and the Western Energy Coordinating Council (WECC) to develop a pilot online, interactive, Standards Compliance Tool, so that each state's utilities' compliance could be monitored. It was anticipated that one of the standards' regulatory organizations would implement the tool permanently.[13]

In 2012, FERC agreed to implement the tool. However as of this writing, the task has not been completed. In addition, FERC has indicated that the set of Critical Infrastructure Protection (CIP) standards will not be made available to everyone on the tool. It is not clear at this time whether states will be able to utilize the tool to monitor utilities' CIP compliance, which was the intent of this section of the SSP. Commerce will continue to monitor development of the tool, and as the state representative on the WIRAB will continue to push for access to the CIP data and

[12] WIRAB is the Western Interconnection Regional Advisory Board, responsible to advise the Federal Energy Regulatory Commission (FERC) on reliability standards development and implementation. Commerce is the Washington State Representative on WIRAB.

[13] Either the regulator (FERC), the Electric Reliability Organization that writes the standards – the North American Electric Reliability Corporation (NERC), or the regional enforcement organization (WECC).

information. If CIP data are not made available to the states, the SSP will be adjusted to drop this program requirement.

Program (Industry CIKR Data and Information – Oil and Natural Gas Industries)

"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 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."

Status

Commerce has not yet initiated this program. Commerce has contacted WSDOT for the purpose of discussing interdependency issues (see Issue # 4, below). That may be a good starting point for implementing the program.

2. Communications

The SSP addresses four types of communications important to CIKR protections that are separate from the data and information that is shared with the State through data calls.

- 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 goal is to identify the types of communications required and the medium by which those communications will be made, and then to carry them out.

Program – State to Industry Communications

"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."

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."

Status

Most government to industry communications of import to CI is conducted directly from DHS to energy companies, through their partnership programs and existing industry information sharing forums. Commerce only passed on a few items during the reporting period. This would be a good issue for the IPSC to address, and Commerce will raise the issue at the first 2013 IPSC meeting.

ECC members indicated in late 2012 that they thought they were receiving or had access to most important government information regarding CI.

No issues raised by ECC member companies.

Program – Industry to State Communications

"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."

Status

See Survey Section (below) for full discussion of survey process, content, and results. We started collecting survey responses in September 2012.

The main issue of concern raised through the survey process was some discrepancy between information the State and federal governments have and what energy companies reported. More companies reported having infrastructure that was critical to the United States than that was critical to Washington State. That seems intuitively wrong. We would expect there would be more infrastructure critical to the State than to the federal government, or at least the same amount. In addition, a number of companies said they did not have CIKR, yet the inventory created for the State through the DHS Data Calls included some of their facilities.

The discrepancy may be due entirely for technical reasons, e.g. different interpretations of survey questions. During the 2013 Data Call planned for March, Commerce will communicate with all the relevant companies to clarify any discrepancies.

Program – Company to Company Communications

"Commerce will work with Puget Sound Energy (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."

Status: Not implemented.

Program – Industry and State Communications to Customers and Others

"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 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."

Status: Not implemented.

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?

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."

Status

As of 2012, all state CI have been mapped by EMD. In addition, all major energy infrastructure in the state has been mapped and identified for tracking on the Washington Energy Supply Disruption Tracking System (WAEDSTS). Oil and natural gas facilities were added during 2012.

Priority, Density, and Co-Locations Analyses have not been conducted by Commerce at this time, alone or in conjunction with any other state agency. Other agencies may have done so.

Commerce intends to inquire of the IPSC in 2013 about a potential schedule for the conduct of the various analyses.[14]

Other types of analyses, such as Buffer Zone Protection Program vulnerability analyses, are being continually conducted (year after year) by the State in conjunction with the federal Department of Homeland Security, and in partnership with energy companies.[15]

4. Interdependencies

Energy supplies and services have become increasingly dependent on other infrastructure sectors as other sectors have become increasingly dependent on energy, both in terms of the number of dependencies and their importance.

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.

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 important 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."

[14] Commerce is a member of the IPSC Executive Committee, which is a newly formed body, coming out of the recent IPSC reorganization. It's first meeting is anticipated late winter or early spring, 2013.
[15] Examples are provided in the SSP. Contact the state Military Department, Emergency Management Division, Infrastructure Protection Program for complete information.

Status

This program element represents a major undertaking. It will take years to address all the interdependency issues between energy and the other 17 infrastructure sectors, and upstream and downstream of energy supplies and services. This does not mean there has been no effort in this area to date. Individual companies work with both the suppliers they depend on, and the customers they serve. In addition, there have been many interdependency discussions between IPSC sector representatives, and through numerous seminars, workshops and exercises where interdependency issues have been discussed and tested. What has not occurred yet is a formal interaction between the ECC and other sector coordinating councils.

The ECC co-chairs have identified the transportation sector as of primary importance when it comes to energy interdependencies. Transportation has been identified as the highest priority infrastructure sector in the state by the IPSC (energy is the second highest). So ensuring the transportation sector has the energy it needs is of ultimate priority. At the same time, the energy sector depends on transportation capabilities to operate, maintain, and restore its systems during emergencies.

In late 2012, Commerce initiated the discussion about interdependencies with the Washington State Department of Transportation. The current plan is to discuss interdependencies during 2013 in the process of developing a state Emergency Fuel Distribution Implementation Plan (due Fall, 2013), however interdependency issues will be discussed beyond fuel distribution. ECC member companies will be included in the process where appropriate.

The SSP notes that water sector representatives on the IPSC have made it a priority to discuss interdependencies with energy sector representatives. Commerce will set up an initial discussion early in 2013.

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 (COOPs). 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."

Status

See Survey Section (below) for full discussion of survey process, content, and results.

5. Local Energy Assurance

The State has worked with cities and counties in various ways over the years to prepare for and respond to energy emergencies, primarily to address storms. Commerce generally works directly with energy companies during disaster response, but can become involved with cities and counties' response efforts if necessary. The nature of energy supply and services (the State provides none), limits the assistance the State can provide to local jurisdictions beyond coordination with energy company restoration efforts. The State has provided no critical *energy* infrastructure protection assistance to cities, counties or Tribes.[16] The SSP recognizes that there may be a need to do so, however what would be the nature of that assistance is unknown. Identification of issues of concern is needed.

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."

[16] Tribes are sovereign states, yet their energy issues are often similar to those of cities and counties. They represent distinct geographic areas in the state and generally receive energy supplies and services from the companies and public utilities that serve local jurisdictions.

Status

In 2009, USDOE offered Local Energy Assurance Planning (LEAP) grants under the American Recovery and Reinvestment Act (ARRA). No cities or counties in Washington received a LEAP grant (did not apply or was denied). A number of other Pacific Northwest states received LEAP grants. In 2012, the City of Portland completed its LEAP grant and produced the *Portland Local Energy Assurance Plan, June 2012*. That report has been provided to a number of ECC member companies with the request to review and report back to the ECC, which has not yet occurred. Commerce hopes to use this process to kick off its discussion of LEAP issues in 2013. It is not certain at this time that there will be any issues of concern for the ECC to address.

6. Infrastructure Out of State, Critical to Washington

Washington State relies heavily on energy infrastructure outside its borders. As within the state, some of those facilities may be critical. While the State lacks authority to take protective actions elsewhere, identifying those facilities and then communicating and working with the appropriate entities outside the state may at least initiate processes that will result in their protection, or perhaps provide assurances that they are well protected.

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. 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."

Status

While individual companies have taken steps to identify such CI, it has not been done in a formal way by the ECC. A previous effort by the Infrastructure Protection Sub-Committee (IPSC) identified a number of such CI, though that work has not been fully followed up. Over the past couple of years, Commerce has communicated with both company and government representatives in Canada and neighboring states about certain key facilities.

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."

Status

In 2012 Commerce initiated a search for CI funding opportunities, and involved EMD in the process. A final list has not been developed.

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. 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. 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."

Status

A prioritized list of key threat/disaster scenarios related to energy CI has not been developed at this time. In 2012, the State conducted the Evergreen Earthquake Exercise Series, that included functional, logistics, and tabletop exercises addressing both response and recovery issues. Commerce participated in exercise design, conduct and as a participant in both functional and tabletop exercises, which represented a significant effort. A number of energy companies participated as well.

Commerce did not arrange for companies to share their experiences with the ECC after the January 2012 storm; however, lessons learned were incorporated into the Evergreen Earthquake Exercise Series functional exercise.

In addition, Commerce participated in an AAR process for the earthquake exercises and reported a number of major lessons learned about energy emergency preparedness:

- Additional trained staff are needed to assist in energy emergency response as Emergency Support Function (ESF) 12 Coordinators.[17]
- A template is needed to allow the Governor to immediately declare an Energy Supply Alert, or Energy Emergency, and
- An Emergency Fuel Distribution Implementation Plan is needed to facilitate emergency fuel management and distribution articulated in the state energy assurance plan.

Commerce conducted a seminar to train additional ESF 12 Coordinators on December 19, 2012 that included staff from Commerce, WUTC and EMD. An emergency declaration template will be produced in the process of developing the Emergency Fuel Distribution Implementation Plan.

[17] ESF 12 is the Emergency Support Function for Energy. Commerce is the ESF 12 Coordinator for State response to energy emergencies.

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.), if terrorists know a system will be quickly and fully restored, it will 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. In addition, 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.

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."

Status

The *Washington State Energy Assurance and Emergency Preparedness Plan* was last fully updated in October, 2006, with minor revisions in 2009. Though the SSP did not exist at that time, all major energy suppliers in the state were given the draft and opportunity to comment. Also in 2009, Commerce received an American Recovery and Reinvestment Act (ARRA) grant from the US Department of Energy (USDOE), which required an update of the State's energy assurance plan. Commerce proposed, and USDOE approved, development of the SSP as an

addendum to the energy assurance plan to comply with the update requirement. All major energy companies in the state were provided the opportunity to join the ECC. The SSP was completed in November 2011.

A second addendum, an emergency fuel distribution implementation plan, is targeted for completion in the fall of 2013. Stakeholders will be provided an opportunity for input.

As of this writing, a new update of the entire energy assurance plan has not been scheduled.

On November 6, 2012, Commerce sent out a Storm Preparedness E-mail to all electric utilities in the state in preparation for the storm season. As of this writing, 53 of 59 electric utilities have provided updated emergency contact information.[18] Commerce is updating oil and natural gas company contacts through a separate process (integration of oil and natural gas supply disruption tracking into the Washington State Energy Supply Disruption Tracking System - WAESDTS).

The SSP itself, created by the ECC, and distributed to all major energy companies in the state at the end of 2011, is the initial communication to all the energy companies in Washington and the best possible articulation of the partnership that exists to identify and protect critical energy infrastructure.

After the major ice storm that hit Washington in January, 2012 (often referred to as Snowmageddon), Commerce participated with EMD to produce an After Action Report (AAR) with lessons learned. All electric utilities involved in the storm were surveyed and lessons learned articulated in the AAR. There were no major concerns raised with the ECC.

10. Biennial CIKR Report and SSP Updates

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. "

[18] Including BPA, which retails to Direct Service Industries, and two Idaho utilities that have Washington customers, there are 59 electric utilities serving the state of Washington.

Status

A 2013 Biennial CIKR Report has been produced (this document). No changes to the SSP have occurred as of the time of this Report. The next planned update of the SSP is scheduled for 2015/16.

Critical Infrastructure, Key Resources Survey

Energy supplies and services in Washington are provided by many different entities, including:

- Fifty-nine electric utilities, counting BPA, but not counting the Corps of Engineers and Bureau of Reclamation that operate hydroelectric facilities, and Independent Power Producers that own and operate other coal and natural gas fired and wind powered generating facilities;
- Five oil refiners, two major oil marketers, one crude oil pipeline, three petroleum product pipelines, 23 petroleum product terminals, plus dozens of gasoline, fuel oil and propane distributors and over two thousand gasoline station owners and operators;[19] and
- Two interstate natural gas transmission pipelines, a major underground natural gas storage facility, four investor-owned, and three municipal natural gas distribution utilities.

None of these companies, public utilities, or federal agencies are required to provide information about the criticality of their facilities, personnel, or systems to the State. The State has authority to acquire certain types of information as it relates to specific regulatory oversight, such as the WUTC regulation of pipeline safety. A lot of energy infrastructure is visible to the public, and its capacities and system functions well understood. So criticality is not completely unknown. Nevertheless, criticality is not always intuitive, and the State (and federal government) rely on voluntary information provided by energy owners and operators for a clear and complete understanding of CIKR issues.

Much of the information that is provided the State is not made public, nor is it widely shared amongst governments or even within the State itself. Not many have a need to know specific security information that is protected by state law. Which raises an important question – how can the public be confident that energy companies are taking reasonable steps to identify and protect their CIKR?

The ECC requirement that a CIKR Survey be conducted for biennial reports is, in large part, to strengthen public confidence in the energy sector's ability to manage risk and implement effective security, reliability, and recovery efforts – which is Goal 6 in the SSP.

[19] Actual station count is unknown. Statement is based on US average.

Survey Directive in the SSP

"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.

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."

The ECC approved CIKR Survey was initiated in September, 2012. It was sent to all electric utilities serving the state, oil refiners and petroleum product pipelines, and major natural gas transmission and distribution companies. Energy companies with only minor facilities (such as gasoline stations) were not included. A number of companies have been identified for inclusion in the next survey that were not included this time.[20]

- Companies that provided survey responses are listed in Appendix A.
- Survey questions and numeric answers are attached as Appendix B.
- A copy of the Survey Form is attached as Appendix C.

[20] These include oil terminals owned and operated by independent companies. Commerce has only recently begun to include them in discussions about emergency issues. Generally, Commerce communicates with oil companies whose supplies pass though the terminals. The terminal owners and operators do not own the product nor are they knowledgeable about or authorized to discuss its disposition. Regarding the facility, however, and its criticality, they are knowledgeable.

Survey Responses

Approximately 69 companies were asked to take the survey. Some companies have different types of infrastructure, e.g. electricity and natural gas, and operate different types of facilities, e.g. a refinery and a pipeline. It was left up to companies to decide to submit a company-wide response or separate responses for different types of infrastructure. In the end, 29 surveys were completed, nearly all company wide, representing 42 percent of companies asked to respond.

Twenty of 59 electric utilities (33.9%) responded. One other took the survey but its contents were not saved on the survey site. These 21 utilities together represent 87 percent of all electric customers in the state.

Four of five refiners (80%) and two of three petroleum product pipelines (66.7%) responded. The oil industry posted the best response rate of any energy sector.

Two of four surveyed natural gas utilities (50%) and the State's primary natural gas transmission company responded.[21] The two natural gas utilities together represent 78.8 percent of all natural gas customers in the state.

Key Findings

We find the overall response rate very good, considering it is primarily small and very small companies that did not respond. With a few exceptions, all major companies responded: those that provide major services and serve the vast majority of energy customers in the state.

While the energy sector in general, and electricity specifically, is considered high priority critical infrastructure by DHS, relatively few companies have facilities, personnel, and systems that can be considered critical to Washington and the United States. Only 13 of the companies responding to the survey claimed to have infrastructure meeting the NIPP criteria cited in survey question 4. Because we have the largest companies included in the survey, with the exception of just a few who did not take the survey, we can be sure that almost all the energy infrastructure critical to Washington and the United States is represented in this survey.[22] Expanding our second survey (in 2014) to include Independent Power Producers and independent terminal owners and operators will capture additional facilities, personnel and systems. However, by their very nature they are less likely to be critical by the NIPP definition. We lose individual power plants and storage facilities periodically without significant impacts to electricity service or fuel supply.

One issue of mainly administrative concern in the survey results is the discrepancy between CIKR identified as critical to the United States and to Washington. Only seven companies indicated they had CIKR critical to Washington, while nine indicated they had CIKR critical to

[21] The survey was not sent to the cities of Buckley, Enumclaw, or Ellensburg, which operate their own natural gas utilities and have less than 12,000 customers between them.
[22] The refiner and petroleum product pipeline company not included in the survey provided Commerce a written statement in lieu of taking the survey.

the United States. Generally, if it is important enough to garner federal attention, it is considered critical to the State.

A primary reason for the survey according to the SPP is so that the public can gain some confidence in the steps being taken by the State and energy companies to identify and protect CIKR. The following survey results are encouraging.

- Of the 13 companies reporting they have CIKR, they have all taken steps to identify and protect it.[23]
- With just a few exceptions, they all have completed at least one cycle of CIKR identification, risk assessment, prioritization, protective measure development, and protective measure implementation for their facilities, personnel, and systems. [24]
- Energy companies have been, and are, making extensive investments in identifying and protecting their CIKR. When asked about the amount of time it requires, the investment it requires, and the complexity of the work required, 12 of 13 companies (92.3%) indicated moderate to high in all categories, with most responses in the medium-high and high when taken together. While this survey was not able to develop a baseline upon which companies could rate their responses, nearly all the companies indicated that CIKR identification and protection represents an effort that is complex, takes significant time, and costs a lot.
- Most of the work that needs to be done to protect existing CIKR has been done.[25] Eight of the 13 companies (61.5%) agreed "Facilities and processes have been secured. We do not see the need for extensive, additional efforts." Four of the 13 (30.8%) said they were "80 percent of the way there." Only a single company thought the majority of their work was still ahead.
- Electric utilities are subject to FERC/NERC Transmission Reliability Standards that include robust Critical Infrastructure Protection (CIP) standards. Utilities must determine if they have infrastructure that meets the FERC/NERC criteria, and if so, comply with the standards. Non electric companies listed a number of other standards, requirements, and guidelines that they followed, including:
    - Security Vulnerability Assessments reported to the Coast Guard under the Maritime Transportation Security Act (MTSA), codified in 33CFR 105.

[23] A single company indicated its "no" answer was because of a technical reference to the NIPP. They also have taken steps to identify and protect their CIKR but under a different framework. So all 13 companies have done so.
[24] The few negative responses represent technicalities, as stated previously. The actions have been done but under different frameworks or processes.
[25] See Survey Question 8. This is about existing CIKR and initial efforts to identify and protect it. It does not address ongoing maintenance requirements, new infrastructure, and potential new threats. Efforts to address cyber security seem destined to expand. In the future, security measures will be included in planning and development processes, and therefore less often represent changes to existing facilities and processes. Retrofitting is usually more expensive and time consuming.

    - Reports to DHS on Chemical Facility Anti-Terrorism Standards (CFATS), Section 550 of the Homeland Security Appropriation Act of 2007.
- The FERC/NERC CIP standards include some dealing with Cyber Security. Nearly all the oil companies reported that their plans address six key cyber standards similar to the FERC/NERC requirements.[26]

[26] Different companies address security issues through different plans. Might be a business plan, a security plan or a COOP plan, for example. The survey did not ask them to specify actions to specific plans.

Appendix A: CIKR Survey Respondents

Electric Utilities

Avista Utilities
Big Bend Electric Cooperative
Bonneville Power Administration
City of Port Angeles
Clallam County PUD
Clark Public Utilities
Cowlitz County PUD
Franklin PUD
Grays Harbor PUD
Orcas Power and Light Co.
PacifiCorp
Parkland Light and Power
Public Utility District No. 1 of Chelan County
Public Utility District No. 2 of Pacific County
Puget Sound Energy
Richland Energy Services, City of Richland
Seattle City Light
Snohomish PUD
Tacoma Power
Vera Water and Power

Oil Companies

BP Cherry Point Refinery
Chevron U.S.A. and affiliated companies
ExxonMobil Pipeline Co.
Olympic Pipeline
Shell Puget Sound Refinery
Tesoro
US Oil and Refining Co.

Natural Gas Companies

Avista Utilities
Puget Sound Energy
Williams Northwest Pipeline

Appendix B: CIKR Survey Responses (Numeric)

Questions 1 – 4 were to be answered by all responders.

Q1 Please provide us with your contact information. Thank you!

Company	Name	Position	Phone Number	E-mail Address
29 [27]	29	29	29	29

Q2 This survey is required by the Washington State Sector Specific Plan (SSP) for Critical Energy Infrastructure, for the purpose of supporting a Biennial Report on Critical Energy Infrastructure in Washington. The SSP is an implementation plan for identifying and protecting energy infrastructure that is critical to the State and is a product of the State Energy Coordinating Council (ECC) - a private/public, industry/government body. Please select all that apply.

I have heard of the State ECC	I am familiar with the work of the ECC	I have heard of the SSP for Critical Energy Infrastructure	I am familiar with the contents of the SSP for Critical Energy Infrastructure
19	8	13	10

Q3 This survey asks questions about sensitive security issues. It does not, however, ask any questions about the purpose, priority, or vulnerability of any specific facilities, personnel, or systems, nor does it ask any questions about specific measures taken to protect them. In addition, survey answers will be reported in aggregate - we will not report the answers of individual companies. We will list the companies that participate in the survey. The information provided in your survey answers are protected by two different statutes.

- RCW 43.21F.060 requires the Department of Commerce to keep proprietary information confidential.
- RCW 42.56.420 provides an exemption from public disclosure for records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts.

At the end of the survey, we provide you the opportunity to indicate whether you have provided such information.

I have read and understand the protections described above.
28

Q4 According to the National infrastructure Protection Plan (NIPP), Critical Infrastructure and Key Resources (CIKR), "...includes systems and assets, whether physical or virtual, so vital

[27] Twenty-nine companies provided all requested contact information.

to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters." [NIPP, USDHS, 2009, p7] Some states and local jurisdictions have identified systems and assets critical to them, even if they do not rise to the level of national concern. For the purposes of this survey, all such systems and assets are deemed CIKR. Do you have facilities, personnel, or systems that are deemed CIKR by the following jurisdictions? Check all that apply. If none apply, select NA (Not Applicable) and go directly to Send Survey at the end of the survey form.

Governing Body / Regulator(s)	Cities or Counties	State of Washington	United States	NA
7	5	7	9	12

The survey assumes that responders selecting one or more of the jurisdictions in the previous question (Q4) are the only companies with CIKR, and are the only respondents required to complete the rest of the survey – Questions 5 through 23. Those companies number 14.

Q5 Have you taken steps to identify and protect CIKR?

Yes	No
13	0

Q6 The NIPP establishes an iterative Risk Management approach for addressing CIKR. After CIKR identification and the implementation of protective measures comes evaluation, which results in another cycle of goal setting, assessment, and protection. [NIPP, Pg. 4] Have you completed at least one cycle, annual or otherwise, of CIKR identification, risk assessment, prioritization, protective measure development, and protective measure implementation for each of the following?

Facilities		Personnel		Systems	
Yes	No	Yes	No	Yes	No
12	1 [28]	11	1	10	1

Q7 If you answered no for any item in question 6, please indicate the item(s) and date(s) by which you anticipate completing your first cycle from CIKR Identification through Measure Implementation. If you answered yes for all items in question 6, skip to question 8.

Open-Ended Response
2 [29]

[28] See question 7.

[29] Two companies explained their "no" and "blank" responses. Responses are technical, not indicative that facilities, personnel, and systems have not been addressed.

Q8 The US focus on CIKR is a relatively new initiative, with facilities to secure and procedures to tighten up. As security is more fully integrated into planning, there should be less need for corrective security projects and programs. How would you characterize your progress in addressing existing CIKR?

Facilities and processes have been secured. We do not see the need for extensive, additional efforts.	Eighty percent of the way there. We have a number of major efforts still underway.	Fifty/fifty. We identified work to be done and it is taking time and resources to do it.	Not very far along. Of the work we believe needs to be done the great part of it is still ahead.
8	4	0	1

Q9 Infrastructure and protective requirements vary among companies and industries. On a five point scale from Low to High, how would you characterize your efforts to identify and protect CIKR? You may provide more detail under "Additional Comments," if you would like.

Amount of time it requires				
Low	Medium Low	Moderate	Medium High	High
1	0	2	6	4
Level of investment/expenditures				
Low	Medium Low	Moderate	Medium High	High
1	0	4	5	3
Complexity of work				
Low	Medium Low	Moderate	Medium High	High
1	0	3	3	6

Q10 Does your Business Plan explicitly address CIKR? If you select YES, please briefly describe in the "Comments" field how CIKR is addressed. Select NA for "Not Applicable" if you do not have a Business Plan or equivalent.

Yes	No	NA
9	2	1

Q11 Electric utilities are required to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Indicate whether these and any other CIP programs apply to your company. Check all that apply.

Mandatory CIP Standards (such as the NERC CIP standards)	Voluntary CIP Standards	CIP Guidelines	None of the Above	Other (please specify) [30]
9	1	1	3	2

[30] Two companies listed alternatives.

Q12 Other than the NERC CIP standards, please identify by title, author, date and document number any other standards or guidelines you follow.

Open-Ended Response [31]
6

Q13 If you DO NOT face compliance with mandatory standards how do you ensure implementation of a quality CIKR protection program? Enter NA for "Not Applicable" if you DO face compliance requirements.

Open-Ended Response [32]	NA
2	9

Q14 This question applies to petroleum and natural gas companies only. Indicate whether your CIP plans address the following Cyber Security issues. Check all that apply.

Identification of Critical Cyber Assets	Physical Security of Critical Cyber Assets	Personnel Training in and Management for Critical Cyber Asset Security	Cyber Security of Critical Cyber Assets	Cyber Sabotage Reporting and Response Planning	Recovery Plans for Critical Cyber Assets
5	6	7	6	6	6

Q15 Traditional protective measures include options such as facility duplication, hardening, hiding, guarding and monitoring. Energy facilities and equipment are often located where such measures can be difficult to employ and expensive. Accordingly, the NIPP, and the Federal Energy Sector Specific Plan [USDOE, 2010], have made enhanced response and recovery a high priority. Indicate the degree to which you have chosen to implement enhanced response and recovery measures in addition to or in lieu of traditional measures to protect your CIKR.

Almost exclusively - we rely on response and recovery measures much more than traditional protective measures.	We do both, but the emphasis is clearly on response and recovery.	We do both, but the emphasis is clearly on traditional protective measures.	Almost Never - we have implemented or will implement traditional protective measures for all or nearly all, our CIKR and do not rely extensively on response and recovery measures in lieu of CIKR protection.
0	6	7	0

[31] Six companies listed alternatives.
[32] Two companies described their programs.

Q16 Please describe broadly actions you have taken since September 11, 2001, to enhance your response and recovery efforts, and more specifically actions you have taken in the past year (50-300 words).

Open-Ended Response
10 [33]

Q17 Do you have a Continuity of Operations Plan (COOP)? This is sometimes referred to as a Business Continuity Plan, Contingency Plan, or Emergency Response Plan.

Yes	No
13	0

Q18 How would you characterize your COOP? Select NA for "Not Applicable" if you do not have a COOP or equivalent.

Comprehensive and detailed, relies on human knowledge for specific purposes.	Outline and guidelines mainly, relies extensively on human knowledge.	Very limited in scope and detail, relies almost exclusively on human knowledge.	NA	Other (please specify) [34]
6	7	0	0	1

Q19 Does your COOP explicitly address CIKR? If you select YES, please briefly describe in the "Comments" field how CIKR is addressed. Select NA for "Not Applicable" if you do not have a COOP or equivalent.

Yes	No	NA
6	6	0 [35]

Q20 When is your COOP scheduled for the next update? Skip this question if you have no COOP or equivalent.

Open-Ended Response
11 [36]

[33] Ten companies described actions they have taken.
[34] One company described additional aspects of their COOP.
[35] Not all companies answered the question.
[36] Nine companies gave dates or described conditions, e.g. “as necessary.”

Q21 In Question 3, we described a number of protections for the information we are requesting. Please indicate whether you have provided information in this survey that is proprietary or restricted for security purposes.

Proprietary under 43.21F RCW	Security Sensitive under 42.56 RCW
6	7

Q22 The Washington State Sector Specific Plan for Critical Energy Infrastructure calls for this survey to be conducted every two years to inform a Biennial Report on Critical Energy Infrastructure. Future surveys will cover only the two-year period between reports. We value your input to improve the survey. If you have any comments or suggestions for us please provide them in the comment box. Thank you.

Open-Ended Response
0 [37]

Q23 If you would like to discuss this survey or infrastructure protection in general with an ECC Co-Chair, please select from the following options. You may choose to hear back from both individuals.

Mark Anderson, Co-Chair, Energy Coordinating Council, Washington State Department of Commerce	Mary Robinson, Co-Chair, Energy Coordinating Council, Puget Sound Energy	No thanks!
0	1	9

[37] No companies provided comments or suggestions.

Appendix C: CIKR Survey

Critical Infrastructure, Key Resources

1. Please provide us with your contact information. Thank you!

Company	
Name	
Position	
Phone Number	
E-mail Address	

2. This survey is required by the Washington State Sector Specific Plan (SSP) for Critical Energy Infrastructure, for the purpose of supporting a Biennial Report on Critical Energy Infrastructure in Washington. The SSP is an implementation plan for identifying and protecting energy infrastructure that is critical to the State and is a product of the State Energy Coordinating Council (ECC) - a private/public, industry/government body. Please select all that apply.

- ☐ I have heard of the State ECC
- ☐ I am familiar with the work of the ECC
- ☐ I have heard of the SSP for Critical Energy Infrastructure
- ☐ I am familiar with the contents of the SSP for Critical Energy Infrastructure

3. This survey asks questions about sensitive security issues. It does not, however, ask any questions about the purpose, priority, or vulnerability of any specific facilities, personnel or systems, nor does it ask any questions about specific measures taken to protect them. In addition, survey answers will be reported in aggregate - we will not report the answers of individual companies. We will list the companies that participate in the survey. The information provided in your survey answers are protected by two different statutes:

- RCW 43.21F.060 requires the Department of Commerce to keep proprietary information confidential.

- RCW 42.56.420 provides an exemption from public disclosure for records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts.

At the end of the survey we provide you the opportunity to indicate whether you have provided such information.

- ◯ I have read and understand the protections described above.

Critical Infrastructure, Key Resources

4. According to the National infrastructure Protection Plan (NIPP), Critical Infrastructure and Key Resources (CIKR), "...includes systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters." [NIPP, USDHS, 2009, pg 7] Some states and local jurisdictions have identified systems and assets critical to them, even if they do not rise to the level of national concern. For the purposes of this survey, all such systems and assets are deemed CIKR.
Do you have facilities, personnel, or systems that are deemed CIKR by the following jurisdictions? Check all that apply. If none apply, select NA (Not Applicable) and go directly to Send Survey at the end of the survey form.

- ☐ Governing Body / Regulator(s)
- ☐ Cities or Counties
- ☐ State of Washington
- ☐ United States
- ☐ NA

5. Have you taken steps to identify and protect CIKR?

- ◯ Yes
- ◯ No

6. The NIPP establishes an iterative Risk Management approach for addressing CIKR. After CIKR identification and the implementation of protective measures comes evaluation, which results in another cycle of goal setting, assessment and protection. [NIPP, Pg. 4] Have you completed at least one cycle, annual or otherwise, of CIKR identification, risk assessment, prioritization, protective measure development and protective measure implementation for each of the following?

	YES	NO
Facilities	◯	◯
Personnel	◯	◯
Systems	◯	◯

Critical Infrastructure, Key Resources

7. If you answered NO for any item in question 6, please indicate the item(s) and date(s) by which you anticipate completing your first cycle from CIKR Identification through Measure Implementation. If you answered yes for all items in question 6, skip to question 8.

8. The US focus on CIKR is a relatively new initiative, with facilities to secure and procedures to tighten up. As security is more fully integrated into planning, there should be less need for corrective security projects and programs. How would you characterize your progress in addressing existing CIKR?

- ◯ Facilities and processes have been secured. We do not see the need for extensive, additional efforts.
- ◯ Eighty percent of the way there. We have a number of major efforts still underway.
- ◯ Fifty/fifty. We identified work to be done and it is taking time and resources to do it.
- ◯ Not very far along. Of the work we believe needs to be done the great part of it is still ahead.

Other or Comments

9. Infrastructure and protective requirements vary among companies and industries. On a five point scale from Low to High, how would you characterize your efforts to identify and protect CIKR? You may provide more detail under "Additional Comments," if you would like.

	Low	Medium Low	Moderate	Medium High	High
Amount of time it requires.	◯	◯	◯	◯	◯
Level of investment/expenditures.	◯	◯	◯	◯	◯
Complexity of work.	◯	◯	◯	◯	◯

Additional Comments

Critical Infrastructure, Key Resources

10. Does your Business Plan explicitly address CIKR? If you select YES, please briefly describe in the "Comments" field how CIKR is addressed. Select NA for "Not Applicable" if you do not have a Business Plan or equivalent.

- ◯ YES
- ◯ NO
- ◯ NA

Comments

11. Electric utilities are required to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Indicate whether these and any other CIP programs apply to your company. Check all that apply.

- ☐ Mandatory CIP Standards (such as the NERC CIP standards)
- ☐ Voluntary CIP Standards
- ☐ CIP Guidelines
- ☐ None of the Above

Other (please specify)

12. Other than the NERC CIP standards, please identify by title, author, date and document number any other standards or guidelines you follow.

13. If you DO NOT face compliance with mandatory standards how do you ensure implementation of a quality CIKR protection program? Enter NA for "Not Applicable" if you DO face compliance requirements .

14. This question applies to petroleum and natural gas companies only. Indicate whether your CIP plans address the following Cyber Security issues. Check all that apply.

- ☐ Identification of Critical Cyber Assets
- ☐ Physical Security of Critical Cyber Assets
- ☐ Personnel Training in and Management for Critical Cyber Asset Security
- ☐ Cyber Security of Critical Cyber Assets
- ☐ Cyber Sabotage Reporting and Response Planning
- ☐ Recovery Plans for Critical Cyber Assets

15. Traditional protective measures include options such as facility duplication, hardening, hiding, guarding and monitoring. Energy facilities and equipment are often located where such measures can be difficult to employ and expensive. Accordingly, the NIPP, and the Federal Energy Sector Specific Plan [USDOE, 2010], have made enhanced response and recovery a high priority. Indicate the degree to which you have chosen to implement enhanced response and recovery measures in addition to or in lieu of traditional measures to protect your CIKR.

- ◯ Almost exclusively - we rely on response and recovery measures much more than traditional protective measures.
- ◯ We do both, but the emphasis is clearly on response and recovery.
- ◯ We do both, but the emphasis is clearly on traditional protective measures.
- ◯ Almost Never - we have implemented or will implement traditional protective measures for all, or nearly all, our CIKR and do not rely extensively on response and recovery measures in lieu of CIKR protection.

16. Please describe broadly actions you have taken since September 11, 2001, to enhance your response and recovery efforts, and more specifically actions you have taken in the past year (50-300 words).

17. Do you have a Continuity of Operations Plan (COOP)? This is sometimes referred to as a Business Continuity Plan, Contingency Plan or Emergency Response Plan.

- ◯ YES
- ◯ NO

Critical Infrastructure, Key Resources

18. How would you characterize your COOP? Select NA for "Not Applicable" if you do not have a COOP or equivalent.

- [ ] Comprehensive and detailed, relies on human knowledge for specific purposes.
- [ ] Outline and guidelines mainly, relies extensively on human knowledge.
- [ ] Very limited in scope and detail, relies almost exclusively on human knowledge.
- [ ] NA

Other (please specify)

19. Does your COOP explicitly address CIKR? If you select YES, please briefly describe in the "Comments" field how CIKR is addressed. Select NA for "Not Applicable" if you do not have a COOP or equivalent.

- ◯ YES
- ◯ NO
- ◯ NA

Comments

20. When is your COOP scheduled for the next update? Skip this question if you have no COOP or equivalent.

21. In Question 3, we described a number of protections for the information we are requesting. Please indicate whether you have provided information in this survey that is proprietary or restricted for security purposes.

- [ ] Proprietary under 43.21F RCW
- [ ] Security Sensitive under 42.56 RCW

Comments

Critical Infrastructure, Key Resources

22. The Washington State Sector Specific Plan for Critical Energy Infrastructure calls for this survey to be conducted every two years to inform a Biennial Report on Critical Energy Infrastructure. Future surveys will cover only the two year period between reports. We value your input to improve the survey. If you have any comments or suggestions for us please provide them in the comment box. Thank you.

23. If you would like to discuss this survey or infrastructure protection in general with an ECC Co-Chair, please select from the following options. You may choose to hear back from both individuals.

- [ ] Mark Anderson, Co-Chair, Energy Coordinating Council, Washington State Department of Commerce
- [ ] Mary Robinson, Co-Chair, Energy Coordinating Council, Puget Sound Energy
- [ ] No thanks!