Briefing Paper

The Role of State Public Utility Commissions in Protecting the National Utility Infrastructure:

Cost Recovery, Sensitive Information, and Security Guidelines

The National Regulatory Research Institute

March 2005

John Wilhelm
Senior Institute Engineer

Joe McGarvey
Graduate Research Associate

Raymond Lawton, Ph.D.
Director

EXECUTIVE SUMMARY

With financial support from the Mershon Center, the National Regulatory Research Institute conducted a research project focused on how to help state public utility commissions develop standards for regulating the country's critical energy and water infrastructure. One of the challenges for an era of heightened concern for the nation's vulnerability to domestic terrorism is that while security concerns have traditionally been addressed at the federal level, it is the states which have the expertise and responsibility to ensure the reliability of critical public utility services.

The NRRI convened a conference of national experts to bring federal and state government officials together with energy and water utility representatives to develop and frame the most important issues that state commissions need to address in order to ensure the security of the utility infrastructure. The NRRI served as a partner and advisor for the next phase of the project, in which the State of Oklahoma conducted a formal inquiry to develop policies to address the issues identified by the experts from the Mershon conference in preparation for issuing a formal rulemaking. The NRRI also conducted a survey of the state commissions to obtain information on their existing security efforts and the activity of their jurisdictional utilities.

This report presents the research results and the key issues identified by the survey, the national conference, and the Oklahoma inquiry, all three of which point to the same conclusion: *state commissions have a limited but important role in homeland security*. The state regulatory commission has the lead role in determining who pays for increased infrastructure security and the standards by which such security spending will be considered reasonable and appropriate. While the overall role is modest, it is notable for presenting a low level of state/federal jurisdictional conflict. State commissions are in a position to use existing cost recovery procedures to determine the funding for infrastructure security without requiring substantial federal funding. This distinction is unique as most state agencies often require federal funding in order to work with federal agencies.

This research was supported by a grant from the Mershon Center at The Ohio State University. The views and opinions of the authors do not necessarily express the views of the Mershon Center, the National Regulatory Research Institute, or any specific state regulatory commission.

TABLE OF CONTENTS

Page

Foreword v

Section

A. INTRODUCTION 1

B. PHASE I: MERSHON NATIONAL EXPERT GROUP 9

1. Workshop Proceedings 11
2. Results – Descriptors 11
3. Results – Alternative Scenarios 13

C. PHASE II: STATE-BASED TECHNICAL CONFERENCES 15

1. Key Homeland Security Issues Facing State Public Utility Commissions 16
   a. Protection of Sensitive Information 16
   b. Security Measures 19
   c. Cost Recovery 22

2. Technical Conferences in the State of Oklahoma 26
   a. Protection of Sensitive Information 26
   b. Security Measures 28
   c. Cost Recovery 31

3. Notice of Proposed Rulemaking in the State of Oklahoma 32

D. COST RECOVERY PROCEDURES AND MECHANISMS 34

1. Cost Recovery Procedures 35
2. Pre-Filing Activities and Administrative Procedure 37
3. Regulatory Procedures 38
4. Cost Recovery Mechanisms and Options 39
5. Cost Recovery Considerations 41
6. Other Implications 43

E. CONCLUSION 44

Appendices

A. List of Preliminary Descriptors Developed by the National Expert Group 46
B. List of Final Descriptors Developed by the National Expert Group 49
C. List of Descriptors, Alternative States (Outcomes), and *a priori* Probabilities of Occurrence used in Interactive Futures Simulation (IFS) 50
D. Descriptor Cross-Impact Analysis 52
E. Analysis of Driver and Driven Descriptors 55
F. IFS Generated Scenarios 57
G. Oklahoma Corporation Commission's Notice of Inquiry Into Critical Infrastructure Protection Guidelines 60
H. Oklahoma Corporation Commission's Proposed Electric Utility Rules 65
I. Oklahoma Corporation Commission's Proposed Gas Utility Rules 73
J. Oklahoma Corporation Commission's Proposed Telecommunications Service Rules 81

List of Figures and Tables

Figure

1. Interdependencies among critical infrastructures 3
2. Do states offer utilities protections from disclosure of security-related information? 18
3. Are there separate prudence guidelines for security costs? 23
4. Are utilities filing for security-related cost recovery? 24
5. Are utilities perceived to be reluctant to share security-related information with state commissions? 29
6. Who is driving security-related investments? 31
7. Map of state electricity markets 34
8. Detailed security-related cost recovery procedures process diagram 36

Table

1. Participants in Phase I: National Expert Group Session – Columbus 10
2. List of Descriptors Developed by National Expert Group 12
3. Participants in Phase II: State-based Technical Conferences 27

FOREWORD

September 11, 2001 revealed in the starkest manner that terrorists could use our transportation infrastructure to harm this country and the very people that the technology is intended to benefit. New awareness of the vulnerability of the infrastructure of our society raises a challenge to state public utility commissions. Commissions have been charged since their creation to ensure the safety and reliability of utility service, but this task has become even more vital since 9/11.

Thanks to the support of the Mershon Center, The National Association of Regulatory Utility Commissioners and the NRRI were able to bring together stakeholders to frame the issues facing state commissions and help determine what their role should be in the larger effort to achieve homeland security, and to advance those ideas in a particular state. Due to this work, we were also able to conduct a companion project for the Department of Energy to develop procedures for state commissions to use for allowing utilities to recovery appropriate critical infrastructure security costs.

The project described in this report will provide state commissions with a successful framework to consider when conducting their own efforts in this area.

Finally, I would like to gratefully acknowledge the state representatives who participated and in every respect contributed to this effort and with particular recognition to the Oklahoma Corporation Commission for its important contributions and willingness to take a leadership role in critical infrastructure protection.

The Honorable Connie O. Hughes, Chair
NARUC Ad Hoc Critical Infrastructure Committee
and
Commissioner, New Jersey Board of Public Utilities

A. INTRODUCTION

In his 2002 State of the Union Address, President Bush dramatically underscored the potential threat to our nation's public utilities when he revealed that "our discoveries in Afghanistan confirmed our worst fears, and showed us the true scope of the task ahead…We found diagrams of American nuclear power plants and public water facilities…." Ensuring adequate protection against terrorist threats to U.S. electric, gas, telecommunications and water utilities networks is an imperative for state and federal regulatory commissions. However, while commissions and jurisdictional utilities have a successful track record in restoring essential services after disasters, before 9/11 they had no equivalent experience preventing, responding to, or recovering from terrorist attacks. The objective of the project described in this report has been to identify the most salient issues facing state public utility commissions (PUCs) so that they may better succeed in their effort to secure utility service in the post-9/11 environment.

Since September 11, state regulators, utilities, and the federal government – especially the Department of Homeland Security and the Department of Energy -- have increased their attention toward the nation's utility sectors, with the goal of protecting electric, natural gas, telecommunications and water utility infrastructures from sabotage and attack from domestic and international sources. Our nation's utilities and their associated infrastructures support the stability and growth of our economy, promote confidence in all levels of government and markets, provide us with the basic ability to mobilize resources in times of crisis, offer us a high standard of living, and connect us individually to the larger society as a whole. Because of their importance, these utility sectors have been designated by the federal government as "critical infrastructures" [1] which "provide the essential services that underpin American society… [and] its incapacitation, exploitation, or

[1] As defined in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)) the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.[2]"

National security has traditionally been regarded as a federal issue, with states and private actors being only marginally involved. The impact of terrorism on American soil has resulted in the understanding that homeland security cannot be accomplished by the efforts of the federal government alone. As a consequence, a range of activities have been undertaken at various levels of government and among the private sector to identify and prevent threats and to assist in a rapid recovery in the event of a successful attack. A key security component is the protection of utility infrastructures. The utility sector is a 300 billion dollar component of the U.S. economy and provides a platform upon which all other industrial sectors are dependent.[3] The interconnected and interdependent nature of our nation's utility infrastructures increases the risks of cascading failures and may reduce our ability to respond during an event (see Figure 1). The electric, natural gas, and water infrastructures are highly dependent on telecommunications and information systems. The reliability of these systems in turn affects the natural gas, electric power, and water systems. The reliability of the electric power industry, in particular, affects nearly every other critical infrastructure. The August 14, 2003 blackout in the U.S. and Canada cost the U.S. between $4 and $10 billion, and resulted in the shutdown of water treatment and pumping facilities, the closing of gas stations and refineries, inoperable emergency dispatch systems, suspended air and ground transportation, and failure of cellular transmitting systems and some landline systems.[4]

Since the 1970s all of the utility sectors, with the exception of water, have been

[2] Homeland Security Presidential Directive 7 (Hspd-7), available at http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[3] Department of Commerce Bureau of Economic Analysis estimates utility sector gross output in 2003 at $331.8 billion, available at: http://www.bea.gov/bea/industry/gpotables/gpo_action.cfm?anon=2865&table_id=2927&format_type=0.

[4] See U.S – Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, available at https://reports.energy.gov; and General Accounting Office Report GAO-04-204, *Electricity Restructuring: 2003 Blackout Identifies Crises and Opportunity for the Electricity Sector*, November 2003, available at http://www.gao.gov/new.items/d04204.pdf.

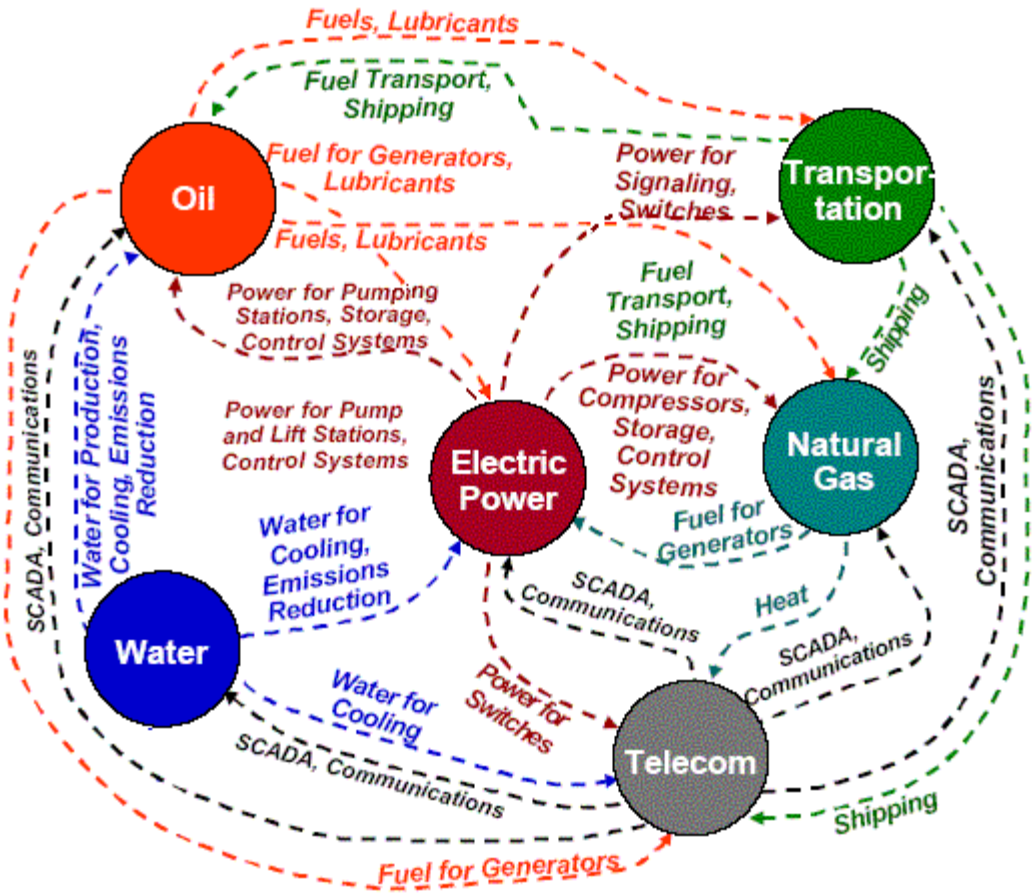


Figure 1: Interdependencies among critical infrastructures
(Source: U.S. Department of Energy, Office of Energy Assurance)

significantly restructured in ways that may make it much more difficult for homeland security and national security goals to be achieved. The ability of a state or federal regulatory commission to order utilities to make specified security investments has diminished as the utility sectors have been restructured and utility markets have increasingly opened up to competition. In this new operating environment "utilities" may now be regulated, partially regulated, or deregulated, and the term "network industries" is gaining popularity and hereafter used interchangeably.

The operating environment for network industries and the agencies that regulate them is conditioned by a complex array of laws, authorities, responsibilities,

market conditions, political forces, consumer needs and technologies. The current push for increased security requirements adds another layer of complexity to this already crowded landscape. State regulatory commissions have filled a vital role in this increasingly challenging arena for the past one hundred years. State PUCs have a statutory obligation to ensure the safe and reliable provisioning of affordable utility service to everyone in their state desiring utility service. With their reliability mandate, state commissions are the lead agency at the state level for promoting, monitoring and enforcing utility security measures. The significant vertical (inter-governmental) and horizontal (public-private) dimensions embedded in the issue further complicate the development and implementation of a coherent reliability and security policy for the nation, individual states and their jurisdictional utilities.

There is no one federal agency that is solely tasked or funded to carry out the mission of protecting our utility infrastructure. The Federal Energy Regulatory Commission, the Federal Communications Commission, the Nuclear Regulatory Commission, the U.S. Department of Energy, the U.S. Department of Homeland Security, and the U.S. Environmental Protection Agency all can play important parts in achieving national security goals. However, the largest portion of the major utility networks actually falls under the jurisdiction of state regulatory commissions. But, the state commissions do not have complete authority to achieve utility sector security goals and must cooperate with federal agencies and other state organizations. Federal agencies and commissions are preeminent regarding national security, inter-state utility flows, and the operation of nuclear plants. State commissions have preeminence over intra-state matters, including reliability and security. Achieving national security goals requires that the deliberations and decisions among the various governmental authorities (vertical, inter-governmental relations) be carried out in a cooperative, nonhierarchical manner.

The creation of the Department of Homeland Security (DHS) provides a unique opportunity to assess how the national security concerns of the federal

government will interact with state governments and private sector actors in achieving secure and reliable utility service. The DHS is empowered to define what constitutes homeland security, the national or public interest in utility provisioning of security measures, and the role utilities and state utility authorities play in achieving greater homeland security. Because state public utility commissions are responsible for the security and reliability of many utility services, they can and have provided the DHS with important insight and experience when designing and implementing policies and programs for achieving utility-sector security. In fact, state commissions have a history of being the glue that holds otherwise disparate coalitions of regulated and unregulated utility service providers together.[5]

The role of state commissions in national security is of increasing importance. The Homeland Security Act of 2002 requires the Department of Homeland Security to coordinate with state and local agencies in order to receive and share relevant critical infrastructure information, to recommend measures necessary to protect critical infrastructure, and to assess and advocate for the resources necessary for state and local agencies to implement the national strategy for combating terrorism. The Department of Homeland Security has joined the NARUC Ad Hoc Committee on Critical Infrastructure, which is responsible for developing recommended critical infrastructure practices for the state commissions.

Horizontal, non-governmental linkages involving the public and private sector are increasingly important in this environment. In the 1970s utilities were regulated monopolies and state and federal regulatory commissions could order that utilities take certain actions. The reason commissions could do this is because they could require "captive ratepayers" to pay higher rates. In the competitive markets that have developed since the 1970s commissions may no longer have the same authority, as many ratepayers are no longer captive. The design and implementation of a reliable and secure utility infrastructure has

[5] The DHS has worked directly with the National Association of Regulatory Utility Commissioners Ad Hoc Committee on Critical Infrastructure to promote and exchange of information among stakeholders.

evolved into a co-created interaction between the public and private sectors. Secretary of Homeland Security Ridge concurs with the belief that this facet of our current environment will be particularly challenging, noting "it's a political challenge because the government must act in partnership with the private sector, since most of the assets that are involved in this effort are owned by the private sector, which owns and operates the vast majority of America's critical infrastructure."[6] This horizontal, nonhierarchical dimension means that semi-voluntary agreements and compliance with state commission rules must be appropriately designed, implemented and monitored. State commissions may also need to develop innovative security procedures and standards that reflect the dynamics of partially competitive network industry markets. Crafting new and effective methods for cost recovery for prudent investments in security poses another new challenge for regulators. There is a growing tension between utilities and commissions in this area.

An important reason why state regulatory commissions will continue to play a major role with respect to achieving security objectives in this increasingly complex environment is due to the existence of a behavioral continuum on the part of utilities. When compliance to security mandates is voluntary, a powerful economic incentive may exist for an individual utility in a network industry to do as little as possible in order to minimize its costs and to maintain a competitive edge (i.e. to under-invest in the level of security that may be appropriate from a total social welfare perspective).[7] When compliance is mandatory, equally powerful incentives may exist to over-invest, in order to have the commission authorize higher rates to cover "excessive" investment in such things as plant,

[6] Department of Homeland Security, "Personnel Announcement by National Security Advisor Condoleezza Rice and Director of Homeland Security Thomas Ridge," October 9, 2001, available at http://www.dhs.gov/dhspublic/display?theme=76&content=315.

[7] See Martin Loeb and Wesley A. Magat, "A Decentralized Method for Utility Regulation," *Journal of Law and Economics*, Vol. 22 (1979), pp. 399-404, and David P. Baron and Roger B. Myerson, "Regulating a Monopolist with Unknown Costs," *Econometrica*, Vol. 50, No. 4 (July, 1982), p. 911-930, on the regulatory process as a principal-agent problem with asymmetric information.

property and equipment.[8] Public interest and national security goals are endangered when either of these two self-interested responses occurs. When utilities are fully regulated, these possible behaviors can be avoided.

The level of security investment reflects a tradeoff between risk and consequence. This tradeoff is informed by what is known about the threat environment in which the utility operates as well as what is deemed to be economically acceptable and sustainable given the strictures of the competitive market and limited government resources. Reaching a strategy for achieving acceptable levels of investment is necessary in ensuring that national security goals are met in an optimal fashion.

Commissions are positioned to play an essential role in facilitating communication among divergent industries and industry segments, and for security collaboration and cooperation. State regulatory commissions have recently had successful experiences using a number of Alternative Dispute Resolution mechanisms in harmonizing horizontal interests. Because state commissions are quasi-judicial they have more flexibility than what would occur in a court. Because they are quasi-legislative, they have the ability to promulgate rules that providers must follow. While there are several recent examples of the ability of state regulatory commissions to promote consensus among parties with widely divergent views, the successful Y2K effort stands out. With the right strategy, the even more complex national security mission can be achieved. The present NRRI project is intended to allow key utility sector stakeholders to critically examine alternative strategies for achieving national security goals.

Two weeks after the tragic events of September 11, the NRRI prepared and e-mailed a report outlining possible national security roles the state utility public utility commissions could undertake.[9] Based on the response to the report it was apparent that a serious need

[8] See Harvey Averch and Leland L. Johnson, "Behavior of the Firm under Regulatory Constraint," *American Economic Review* Vol. 52 (1962), pp. 1052-69.

[9] Bob Burns, Frank Darr, John Wilhelm, and Vivian Witkind-Davis, *National Security and State Public Utility Commission*, No. 01-15 (Columbus: NRRI, 2001).

exists for research that addresses the horizontal and vertical linkages noted above and to identify the best strategies for achieving national security goals.

From our perspective, one of the most important gaps following the initial crisis response after September 11 was the lack of a broader and more comprehensive framing and subsequent exploration of network industry security. We assembled an expert group comprised of utility executives, state public utility commissioners, emergency management personnel, security experts and academics to address this need. We used a modeling approach that has been designed to assist expert groups with framing complex problems and exploring the strategies that are most likely to produce desired outcomes.[10] The NRRI approach was supported by a computer program that unfolds at two levels. The first level is the development of the conceptual model of the problem. In this phase of the research project the experts describe the situation in terms of desired outcomes, significant drivers and processes, strategies available to decision makers and significant external agents. The second level allows the experts to "populate" a mathematical model generated by their conceptual framing of the problem. Through the use of cross impact matrixes, the group can further inform the model and explore the relationships between the different variables in the system and conduct sensitivity analyses on the outcomes. The result is a conceptual and mathematical representation of the operating environment that explicitly identifies the strategies that are most likely to produce desired outcomes.

The results generated by our endeavor provide a foundation from which state commissions can design and implement improved network industry security policies and procedures. Our effort addresses an important gap in the growing debate over how to best secure these critical infrastructures by convening a conference of national experts and representatives of the various affected parties and challenging them to identify their views of the threats to network infrastructures, as well as their

[10] Interactive Future Simulations (IFS™) is a software tool developed by Battelle Memorial Institute futurists to facilitate modeling future trends and their interactions. IFS allows users to consider varying alternative futures and run simulations.

proposals for securing reliable utility service. Our purpose has been to uncover the important issues facing PUCs in a new environment so that they can fulfill their responsibility to safeguard utility service and contribute to the nation's homeland security objectives.

The project was organized in two principle phases. The first phase involved convening a conference to bring federal and state government officials together with energy and water industry representatives to form a national expert group that could identify the most relevant issues facing state commissions in their effort to ensure the security of the utility infrastructure. In the second phase of the project, NRRI served as an advisor to the State of Oklahoma in its effort to develop policies to address the issues identified in the Mershon conference. The decisions reached in Oklahoma can serve as a model for other states as they work to craft rules to secure their own utility infrastructure.

B. PHASE I: MERSHON NATIONAL EXPERT GROUP

In order to examine the potential homeland security role of state public utility commissions, the first stage of the project involved assembling a group of experts who would use their judgment to frame the relevant issues. The expert working group consisted of 22 participants who met for a two-day workshop in Columbus, Ohio in June 2003 (see table 1). The participants were selected to represent three main groups: the federal government, state government agencies, and the utility industry. The federal government contingent included members from the National Communications System, the Office of the Secretary of Defense, and the Department of Homeland Security. The state government representatives included the Wisconsin and Ohio Emergency Management Agencies, the National Association of Regulatory Utility Commissioners, and the PUCs from the states of Oklahoma, Texas, and New Jersey. The utility industry was represented by the Electric Power

Research Institute, the American Gas Association, American Electric Power (the nation's largest electric utility), LG&E Energy (a gas and electric utility) and American States Water Company. Also attending were the directors of the Ohio State University Program for International and Homeland Security, the Mershon Center, and the Battelle Memorial Institute Office of Homeland Security.

Government	National	• Department of Homeland Security • Department of Defense • National Association of Regulatory Utility Commissioners • National Emergency Management Association • National Regulatory Research Institute
	State	• New Jersey Board of Public Utilities • Ohio Emergency Management Agency • Oklahoma Corporation Commission • Public Utility Commission of Ohio • Texas Public Utility Commission
Industry	National	• American Gas Association • Electric Power Research Institute • North American Electric Reliability Council
	Utilities	• American Electric Power • American States Water • Louisville Gas and Electric
Other		• Battelle Memorial Institute • The Mershon Center

Table 1: Participants in Phase I: National Expert Group Session – Columbus

The group was thus able to reflect the two underlying dimensions that public utility commissions operate in when trying to address homeland security questions: the vertical dimension of federal/state government and the horizontal dimension linking industry and regulator. The workshop was led by a facilitator, Steve Millet of the Battelle Memorial Institute, who specializes in guiding expert groups though their discussions. He also developed the group modeling software that was used in the workshop, Interactive Future Simulations. It is a modeling approach that has been designed to assist expert groups with framing complex problems and exploring the strategies that are most likely to produce desired outcomes.

1. Workshop Proceedings

The expert group was asked to consider the question of what will be the most likely role of the state public utility commissions (PUCs) in the context of homeland security by the year 2006. The 2006 timeline was selected to encourage the participants to think outside of their immediate frames of reference and to reflect the fact that as a practical matter it would likely take several years for both the state and federal governments to develop their responses to the new challenges of homeland security. The participants were asked to begin by referencing the extent to which they believed that electric, natural gas, water, and communications infrastructures would be vulnerable to attack; whether or not and to what extent PUCs will have responsibilities to protect that type of infrastructure; to what extent the Federal government will assume responsibility and funding for protecting U.S. infrastructure from attack; and the extent to which corporations will be required to defend their infrastructure assets.

2. Results – Descriptors

To help develop the conceptual model of the problem, the expert group developed a wide-ranging preliminary list of 40 items that they believed would be important descriptors (i.e., factors, trends, barriers, etc.) affecting the role of PUCs in homeland security over the following four years (see Appendix A)

Each participant was then asked to select eight ideas from the master list of 40

preliminary descriptors that he or she judged to be the most important and rank them from highest to lowest (see Appendix A). The final set of descriptors was derived by grouping together ideas from the preliminary list that were closely related or shared a common theme (see Appendix B). The final list of descriptors developed by the expert group is shown in Table 2.

Descriptors
1. Role of State Public Utility Commission
2. Allocation of Responsibility for Information Management
3. Allocation of Responsibility for Coordination and Communication
4. Allocation of Responsibility for Cost Recovery (Who Pays)
5. Public Perception of Threat/Vulnerability
6. Level of Terrorist Attacks on Utility Infrastructure
7. PUC Security Capabilities
8. PUC Role in Restoration Priorities
9. Information Sharing Protocols and Willingness to Share Information
10. Responsibility for Key Asset Protection and Mitigation
11. Standards for Utility Security

Table 2: List of Descriptors Developed by National Expert Group

The group subsequently developed alternative outcomes for each of the descriptors (e.g., public perception of threat as being "high," "medium," or "low"), and assigned rough estimates of the probabilities that each alternative outcome might take place (see Appendix C). Following this specification, a cross-

impact analysis was conducted using Battelle's proprietary software program Interactive Futures Simulations (IFS) (see Appendix D). This analysis examines what impact a given descriptor state would have on the probabilities of all other descriptor states occurring. The analysis draws upon the experts' evaluations of whether one descriptor has a direct effect on another, whether that effect is positive or negative, and how strong that effect might be on a three point scale. Appendix E lists which descriptors had the strongest effect on the others (i.e., the "drivers"), and which descriptors were most influenced by the others (i.e., the "drivens"). The information in the cross-impact analysis is used to establish posterior probabilities for each of the given alternative descriptor states (i.e., in light of how each descriptor is affected by the others, and the relative likelihoods of different combinations of descriptors).

3. Results – Alternative Scenarios

The IFS software arranged the different possible descriptor combinations into alternative scenarios and indicated the relative likelihood of each scenario given the expert opinions expressed during the course of the exercise. The scenario results are listed in Appendix F. Steve Millett, the facilitator of the workshop and creator of the IFS software used the information gathered during the workshop to generate the following four scenarios:

Scenario A: ***Limited Role in a Safer World***. The role of the state PUCs by 2006 will be characterized as "limited," meaning that it will have a relatively small role in Homeland Security. Many responsibilities for Homeland Security (such as information management, coordination and communication, and cost recovery for private investments) will largely be shared between the Federal and state governments, of which the PUC will be just one of several state authorities. The typical state PUC will likely have little or no security capabilities. Post-attack restoration priorities will fall largely to individual utilities rather than to the PUCs. Responsibilities for key asset protection and mitigation will be led by the Federal government. Standards for utility security will be in the low or medium range (meaning some Federal and state

guidelines and requirements, but much left to the states and to the utilities).

Scenario A represents a safer world in that the level of terrorist attacks on utility infrastructure in the U.S. will likely be low in number and low in consequences. Public perception of the terrorist threat, from either Islamic terrorists from the Middle East or domestic extremists like Timothy McVey, will likely be low. Scenario A is derived from the first two IFS scenarios listed in Appendix G. Participants scored it as the most likely scenario based on present inputs to the cross-impact model.

Scenario B: ***Medium Role in a Dangerous World***. The role of the state PUCs by 2006 will be characterized as "medium," reflecting a situation where states will play an increasingly important role in homeland security and with the PUCs having specified responsibilities within the context of state authority. The allocation of responsibilities for information management, coordination and communication, and cost recovery will fall largely upon states, locales, and the private sector. The burden of security investments by utilities will be born primarily by stockholders. With limited resources, the PUCs will have a struggle to fulfill their homeland security responsibilities.

Standards for utility security will be in the medium range, with the utilities having to make the investments to respond to security requirements originating from Washington and state capitals.

Scenario B occurs in a more dangerous world than in Scenario A. In this scenario, terrorist attacks on utility infrastructure will be low in number but high in consequences. The level of public perception of threat will be in the middle range (but higher than in Scenario A). This scenario is based on the third IFS scenario listed in Appendix G and participants gave it a relatively low likelihood of occurrence.

Scenario C: ***Stronger Role in a Dangerous World***. Scenarios B and C are very similar, except that in Scenario C the PUCs have a stronger role in homeland security than in Scenario B. In this scenario, most of the responsibilities for homeland security fall on state

governments; however, cost recovery will rest primarily on customers rather than on utility shareholders. The PUC will determine issues such as prudence (i.e., whether the critical infrastructure investment have been made) and allow many utility costs for security to be passed onto rate payers. PUCs will have better trained and qualified staff to support its homeland security role. The PUCs will play the primary role in restoration priorities, but will likely play a relatively weak role in information gathering, storing, and sharing. The responsibility for key asset protection will be born largely by the utilities and standards will fall into the low level.

Scenario C will occur in the same type of dangerous world occurring in Scenario B. Scenario C is based on the forth IFS scenario listed in Appendix G. It has the same likelihood of occurrence as Scenario B.

Scenario D: *Powerful Role in Homeland Security*. Scenario D is much like Scenarios B and C, except that the role of state PUCs will likely be broad. The allocation of responsibilities for information management, coordination and communication, and cost recovery will likely fall primarily to the states, locales, and the private sector. Among the state agencies, the PUCs play a very important role in homeland security. The PUC will be tasked with the lead role in restoration priorities. The responsibility for key asset protection and mitigation will be born primarily by the utilities with oversight by the PUC. The PUC state security capabilities will be characterized as skilled, robust, and sustainable.

Scenario D is likely to occur along with a lower number but high consequences attacks by terrorists and with a moderate level of threat perception by the public. Scenario D is based on the sixth IFS scenario listed in Appendix G; it is less likely to occur than either Scenario B or Scenario C.

C. PHASE II: STATE-BASED TECHNICAL CONFERENCES

The expert group concluded that the list of descriptors generated in the course of the workshop should serve as a basis for advancing a state-level exploration of the

question of what role PUCs should play in homeland security. Although the modeling exercise in the workshop helped to frame the most pressing issues in securing network industries, the workshop participants agreed that further modeling was not of interest to them and that the most appropriate step was to help PUCs gather evidence and issue rulemakings intended to ensure continuing utility service.

The Oklahoma Corporation Commission (OCC) volunteered to host and conduct the next phase of the work: to host a series of technical conferences bringing together commission officials with interested stakeholders in order to develop solutions to the issues framed in the Mershon workshop in preparation for issuing commission rules on critical infrastructure. The state of Oklahoma has had a special interest in domestic terrorism following the bombing of the Murrah Federal Building in Oklahoma City in 1995. The OCC is active on the NARCU Committee on Critical Infrastructure, and its efforts can serve as a guide for other state commissions when implementing their own rules on critical infrastructure protection.

The process and results of the Phase II Technical Conferences are described in greater detail in Section D of the paper. Immediately below is a discussion of the issues that were framed by the Mershon National Expert Group and taken up in the OCC's Technical Conferences, organized along the three general themes of:

- Protection of Sensitive Information
- Security Measures
- Cost Recovery

1. Key Homeland Security Issues Facing State Public Utility Commissions

a. Protection of Sensitive Information

Regulation of utilities is normally conducted in a transparent manner to provide the public with a clear understanding of the utilities' conduct. The companies are subject to regulation by a commission under the assumption that their services are critical to the public or that they operate from a monopolistic position and therefore thorough public examination of their

activity is appropriate. Mirroring developments such as the Freedom of Information Act, the trend in regulation has been to allow more information to be shared with the public. However, sensitive security information does not fall under normal assumptions about the desirability of public transparency. It would, for example, be self-defeating to publicize the specific security measures a utility has undertaken since this would inform would-be attackers about the specific obstacles they would face. Utilities might, therefore, be reluctant to share sensitive security information with a commission without a method to protect the confidentiality of the information.

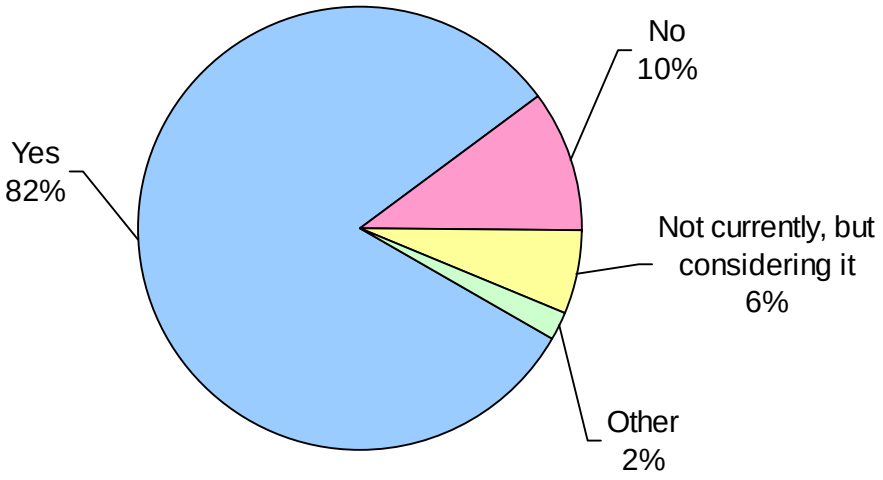
Commissions have responded to the need for greater protection for security sensitive information. A 2003 NRRI survey of the state commissions found that 82 percent of commissions offered protection against disclosure of sensitive security information under Freedom of Information Act or similar laws (see Figure 2), which marked a substantial increase from the 42 percent commissions who reported such protection in a related NRRI survey in the previous year.[11]

In 2003, the Federal Energy Regulatory Commission (FERC) issued Order No. 630 and Order No. 630-A, both of which address the protection of critical energy infrastructure information.[12] FERC defines critical energy infrastructure information to include information about existing and proposed critical infrastructure that is related to the production, transmission, or distribution of energy that could be useful to a person in preparing to attack; is exempt from mandatory disclosure under the Freedom of Information Act; and does not simply provide the location of the critical infrastructure. FERC will determine the applicability of FOIA requests on a case-by-case basis. The orders are limited to the protection of critical energy infrastructure information in FERC's possession, and nothing in the two orders prevents state commissions from seeking

[11] Joe McGarvey and John Wilhelm, *NARUC/NRRI 2003 Survey of Critical Infrastructure Security*, No. 04-01, (Columbus: NRRI, 2004).

[12] United States of America Federal Energy Regulatory Commission, 102 FERC ¶ 61,190 (Docket Nos. RM02-4-000, PL02-1-000; Order No. 630), issued February 21, 2003.

Figure 2: Do states offer utilities protections from disclosure of security-related information?



Yes - Most do. And this number has increased significantly since 2002.

Source: Authors' construct from McGarvey and Wilhelm (2003), n=49.

the information that they might need for their own purposes.

However, FERC's orders underscore the responsibility of commissions to protect confidentiality when appropriate and to have guidelines to employ protective orders when handling information that affects security. Some state legislatures have acted to ensure against the disclosure of security-sensitive documents under state and federal open meeting acts. Kansas has gone the furthest on this issue, passing acts to provide a confidential application and review process by the commission, wherein the amount of recovery requested, the amount allowed, and the method of cost recovery are kept confidential.[13] Other state legislatures have acted to include sensitive public

[13] See Kansas Statute Nos. 66-1233, 66-1234, 66-1235, and 66-1236.

utility information among the exceptions to its public access laws.[14]

b. Security Measures

In contrast to other expenditures where standards have been developed and refined over many years, state commissions do not have well-established precedents by which to evaluate the appropriateness of utilities' efforts to protect their critical infrastructure. Without pre-existing standards or guidelines, commissions would have to rely on witnesses in a proceeding in order to make a determination on cost recovery.

Both the gas and electric industries now operate under some level of security guidelines. In the electric industry, the North American Electric Reliability Council (NERC), an intra-industry organization, has compiled the most extensive set of guidelines for both physical and cyber security.[15] Originally developed in June 2002, the guidelines are arranged by security topic and are periodically updated with the understanding that the guidelines are intended to evolve along with the threats to the electric industry. The existence of the NERC physical security standards is beneficial, but they leave room for differences in protection.

The gas industry largely relies upon the Security Practices Guidelines developed by the Department of Transportation's Office of Pipeline Safety (OPS) and issued in September, 2002.[16] These guidelines were developed with the assistance of state pipeline agencies and pipeline industry representatives. The guidelines are not publicly available, but a review by the OCC found the guidelines to be methodical and

[14] See Arkansas Code Archive § 25-19-105 (2003); Connecticut General Statues § 1-210 (2003); 29 Delaware Code § 10002 (2004); Florida Statutes § 364.183, 366.093, 367.156, 368.108 (2003); Michigan Compiled Law § 460.10d (2003); Missouri Revised Statutes § 610.021 (municipal utilities only); Oregon Revised Statues § 469.530 (2003).

[15] North American Electric Reliability Council, *Security Guidelines for the Electricity Sector*, issued June 14, 2002, available at http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf; and North American Electric Reliability Council, *Urgent Action Standard 1200 – Cyber Security* issued August 13, 2003, available at ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf.

[16] Department of Transportation, Office of Pipeline Safety, *Pipeline Security Information Circular* and *Pipeline Security Contingency Planning Guidance*, , issued September 5, 2002; these documents are not publicly available.

comprehensive. In addition to on-site follow-up by OPS, compliance with the guidelines is subject to review by state pipeline agencies.[17]

Within the telecommunications sector, the Network Reliability & Interoperability Council (NRIC) is an intra-industry organization that has developed an extensive list of best practices for the telecommunication industry.[18] Although the telecommunication industry participants in the OCC's review supported the commission's use of the NRIC guidelines, NRIC states that the guidelines are not intended to be imposed as government regulations. More to the point, the nearly 800 highly technical items in the list would be impractical to adopt as regulations; in order to make use of the NRIC guidelines, it would be necessary for a commission to identify those best practices that were relevant for the companies under the commission's jurisdiction.

The Environmental Protection Agency (EPA) is the lead federal agency for the security of drinking water and waste water. In February 2004, the EPA's National Drinking Water Advisory Council formed the Water Security Working Group in order to establish and disseminate best practices for drinking water and wastewater utilities by 2005.[19] Under the Public Health Security and Bioterrorism Preparedness and Response Act, the EPA requires water operators serving populations larger than 3,300 people to certify to EPA that they have conducted a vulnerability assessment,

[17] In its guidelines, OPS notes that in addition to its *Pipeline Security Information Circular and Pipeline Security Contingency Planning Guidance* documents, it also relies on the industry consensus security guidance documents for purposes of evaluating the security plans of pipeline operators. Specifically, the American Petroleum Institute's *Guidelines for Developing and Implementing Security Plans for Petroleum Pipelines*, issued July 2002, are used in reference to hazardous liquid pipelines, and the American Gas Association and Interstate Natural Gas Association of America's *Security Guidelines: Natural Gas Industry, Transmission, and Distribution*, issued September 2002, are used to help evaluate natural gas transmission and distribution lines. The above documents are not publicly available.

[18] The Network Reliability and Interoperability Council, *NRIC Best Practices*, issued various years, available at http://www.bell-labs.com/cgi-user/krauscher/bestp.pl.

[19] See "National Drinking Water Advisory Council's Water Security Working Group Meeting Announcement," *Federal Register*, Vol. 69, No. 118, (June 21, 2004), p. 34351, available at http://frwebgate.access.gpo.gov/cgi-in/getdoc.cgi?dbname=2004_register&docid=fr21jn04-42.pdf.

and revise their emergency response plan accordingly.[20] EPA provides grants of up to $115,000 to defray the costs of assessments. Smaller water companies (i.e., those serving fewer than 3,300 people) are not required to conduct assessments partly out of concern that they could not recoup the relatively high costs, although grants and other assistance for voluntary assessments and low-cost security strategies are may be offered by state agencies. In addition, intra-industry organizations such as the American Water Works Association (AWWA) and the National Association of Water Companies (NAWC) support members with vulnerability assessments.

Commissions must decide whether to employ mandatory security standards or a set of official voluntary security guidelines. Mandatory standards make questions of cost recovery easier to resolve since the mandate would usually imply the prudence of the corresponding expenditure. Mandatory standards also offer greater assurance against companies under-investing in security. However, voluntary guidelines (possibly including a method of self-certification) would allow a commission greater flexibility in dealing with the cost burden on companies of different sizes and criticality and would allow companies more flexibility to develop security plans specific to their needs. Commissions must also resolve whether imposing equal standards on all companies would require openly publishing what those specific standards are, thereby serving notice to potential attackers.

Security expenses can be grouped into two categories:

1) the physical security of a utility's personnel, production plants, and distribution facilities, and

2) the protection of computer networks and digital control systems (such as SCADA) used in utility service, also known as "cyber security."

The technology of security may demand an expertise that is beyond the experience of existing commission staff and may require the commission to use an independent consultant to evaluate the efficacy of the proposed security costs.

[20] Public Law 107-188, 107th Congress, 2nd Session, (June 12, 2002), Sec. 401.

c. Cost Recovery

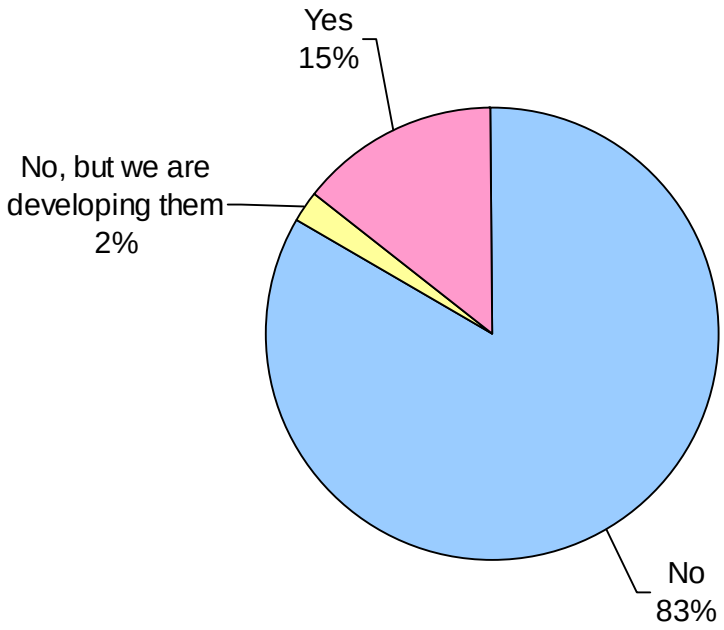
Regulated companies are allowed to recover costs that are both prudent and "used and useful." The commission is responsible for reviewing the costs and challenging those that were not prudently incurred and used and useful. While commissions want to ensure that utilities do not under invest in security, they must also guard against excessive or inappropriate spending. Commissions have extensive experience in judging other types of costs, but there is much less guidance for commissions on what should be considered reasonable security expenditures in the light of the vulnerabilities exposed in the wake of the 9/11 attacks.

An effective security program could include information management, vulnerability assessments, physical security, threat detection, event mitigation, and consequence management. Although some of the burden for these activities might be shared with state and federal government, utilities networks should expect recovery of appropriate security-related expenditures for their jurisdictional entities. Given that network utility industries frequently feature complicated corporate structures where expenses may be shared between jurisdictional and non-jurisdictional network entities, commissions must rely upon standard cost-allocation methods to ensure that only the costs of jurisdictional entities are recoverable.

Most states have not yet developed security-specific guidelines to help them evaluate cost recovery requests for security related investments. The 2003 NRRI survey of state commissions found that only 15% of commissions had specific prudency guidelines for security cost recovery, and 2% were developing them, despite the fact that 45% of states reported receiving filings for recovery of security expenses (see Figure 3). An additional 24% of states reported awareness of utilities' security investments, but had not received recovery requests (see Figure 4).

One of the challenges for a commission evaluating utility cost recovery requests is deciding what should qualify as critical infrastructure. FERC's definition of critical infrastructure (see

Figure 3: Are there separate prudence guidelines for security costs?

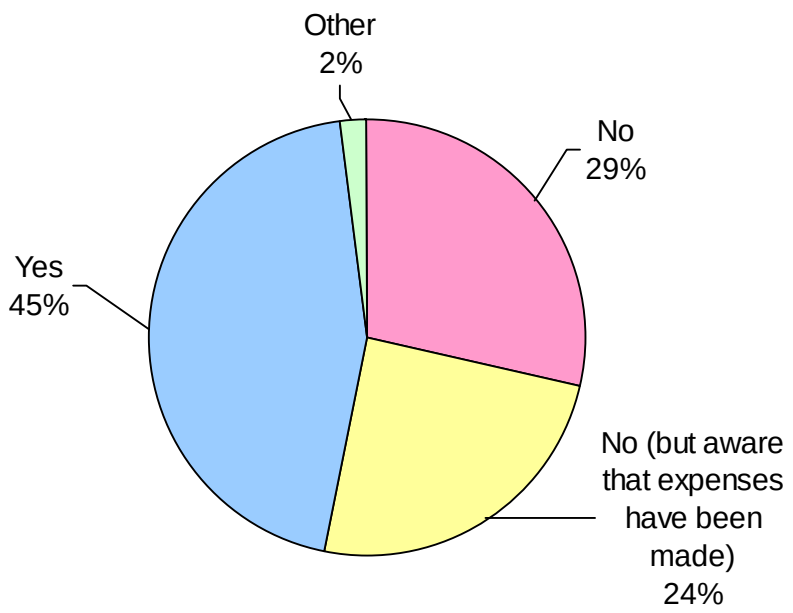


No – most states plan to use their existing prudence review process for handling security-related expenses. However, a few state commissions are developing them or have some modifications in place.

Source: Authors' construct from McGarvey and Wilhelm (2003), n=48.

accompanying box) differs somewhat from the definition used in the USA Patriot Act (see footnote 1). Though FERC offered its definition in the context of an order to protect critical energy infrastructure information in FERC's possession, FERC's definition of critical energy infrastructure could be a useful basis for creating a definition that states could use to help determine whether an existing system or asset should generally be considered to be critical energy infrastructure. However, some issues are raised if the broad definition is applied "as is" to cost recovery. The first issue is one of "existing" versus "proposed." The need to protect the sensitive information of a "proposed" critical infrastructure system or assets from unnecessary disclosure is easily understood. However, granting cost recovery for a "proposed" system or

Figure 4: Are utilities filing for security-related cost recovery?



Most states still have not had filings even though they are aware that security-related expenses have been made.

Source: Authors' construct from McGarvey and Wilhelm (2003), n=49.

asset investment is a larger question and requires more consideration. Under this definition, a commission would be asked to essentially grant pre-approval for "proposed" expenditures to be made in the future. Assuming a state commission wishes to grant approval of the proposed expenditure, it may take one of several approaches. Three common approaches would include the following. It could approve the proposed expenditure as submitted and say nothing further regarding the approval of future similar requests. The commission could approve the expenditure and in its order make clear that the approval was based solely on the merits of the individual rate case and was not precedent setting for future recovery requests of "proposed" systems or assets. Or the commission could approve the expenditure subject to a true-up of the actual recoverable amount following a decision on the type of expenditure in a commission generic

proceeding, or following the applicant's submission of actual expenditure records.

The FERC defines critical infrastructure as "existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters."[21]

Deciding an issue such as recovery of "proposed" systems or assets in a generic proceeding does offer a commission the opportunity to more broadly examine an issue. However, generic cases are generally very open and protracted proceedings. This may make generic proceedings unsuitable for some critical infrastructure issues. Furthermore, a conditional approval subject to a generic proceeding or future true-up may not provide adequate certainty to an applicant. At best it would provide a high degree of probability of some recovery, but would tell the applicant it may proceed, but should do so very cautiously.

The second issue with the FERC definition that a state commission must face is one of limiting the definition of what would "negatively affect security." Existing security and protection systems and assets whose loss would negatively affect security are clearly used and useful critical infrastructure. However, it might be possible to argue that a current or proposed system that does not directly enhance some aspect of security by its operation or addition, will actually have this effect when incapacitated or destroyed. For example, it might be possible for an applicant to argue that a new roof on its executive building, while not directly enhancing security would, if destroyed, negatively affect security. A commission must ask the question: Can a system or asset be considered used and useful or prudent if it does not directly enhance some aspect of security? In a network composed of many joint and common costs, this may be very difficult.

However, the definition raises an issue related to cost recovery. If commissions employ FERC's definition, they must still decide what assets would "negatively affect security" if harmed.

[21] United States of America Federal Energy Regulatory Commission, 102 FERC ¶ 61,190 (Docket Nos. RM02-4-000, PL02-1-000; Order No. 630), issued February 21, 2003, pp. 69-70.

Utilities might argue that an existing or proposed system that does not directly increase security when it is created (e.g., a new roof for an executive building), might still negatively affect security if it were destroyed. Commissions will face this question especially when dealing with network industries with many joint and common costs.

2. Technical Conferences in the State of Oklahoma

Following consultation with the NRRI on the results of the Phase I National Expert Group session, the OCC opened an inquiry to examine the role of PUCs in addressing the security of critical infrastructure in that state. The OCC began the process by issuing a Notice of Inquiry on October 17, 2003 soliciting comments from all interested parties on a list of items. Drawn up with the assistance of the NRRI, the list of items reflected the issues framed by the Mershon Expert Group (see Appendix G for a copy of the Notice containing the full list of the items for comment).

Following the collection of comments, the OCC held a series of eight technical conferences involving the commission and interested stakeholders, along with NRRI staff. The conferences took place in January and February, 2004 and were intended to facilitate discussion on the topics raised in the Notice of Inquiry. The parties attending the conferences included the NRRI, representatives from the electric, gas, telephone, and water companies, the FBI and the U.S. Secret Service (on behalf of the Department of Homeland Security), and the Oklahoma Attorney General's Office (see table 3 for a complete list of participants). The Oklahoma Office of Homeland Security also provided comments during the course of the conferences.

The results of the technical conferences are discussed below, and are grouped, as before, along the three general themes of protection of sensitive information, security measures, and cost recovery.

a. <u>Protection of Sensitive Information</u>

One clear finding of the Technical Conferences is that new legislation or commission rules are necessary if companies are to feel confident about

Table 3: Participants in Phase II: State-based Technical Conferences

Government	National	• Department of Homeland Security • National Regulatory Research Institute
	State	• Oklahoma Corporation Commission • Office of the Attorney General of the State of Oklahoma • Oklahoma Office of Homeland Security
Industry	Utilities	• American Electric Power / Public Service Company of Oklahoma • Center Point Energy • Oklahoma Gas and Electric • Oklahoma Natural Gas Company • Western Farmers Electric Cooperative

voluntarily sharing sensitive security information with the Oklahoma commission. Almost all of the utilities involved in the Technical Conferences expressed the belief that existing laws were not sufficient to protect against the disclosure of sensitive documents or discussions. The companies saw a need for broader use of *in camera* hearings and protective orders, as well as the development of new processes and protective forms created specifically to handle security information. They also suggested that the commission have one contact person with security clearance to receive sensitive information. The companies were also concerned that the security information they shared with the commission not be used in other courts of law and that it be properly handled by any other agencies that might receive it from the OCC. All the participants in the

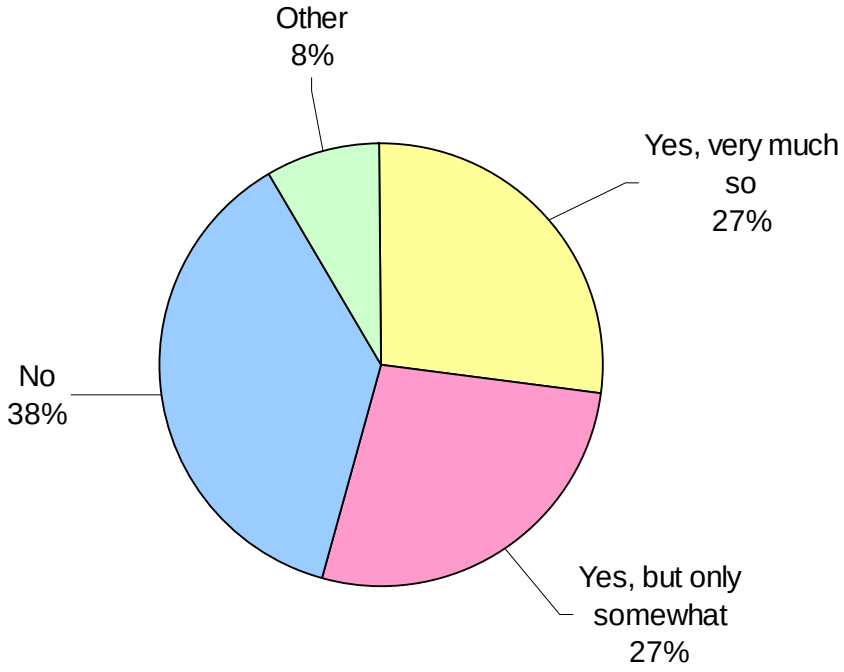
Technical Conferences agreed that security information should be protected from public disclosure and that further steps would be necessary to achieve that. Two options were considered for how to protect security information. The first option is to employ the commission's existing jurisdictional authority, an option that the chair of the OCC was inclined to choose. A second option would be to create new legislation to specify the protection. The OCC staff suggested that a statute could be created to protect critical infrastructure information, but that costs and other financial information be given a lower degree of protection so that consumers and third parties to cost recovery proceedings could review the costs that would be recovered though regulated rates, which consumers are responsible for paying. Under this arrangement, cost information would not be considered confidential automatically, but the commission could issue a protective order to that end. The OCC staff also recommended that a member of the Attorney General's office have access to all security information provided to the commission. The utility participants suggested that the companies might be less concerned with submitting security information to the commission if they were able to omit specifics, such as location, that could bring potential targets to the attention of terrorists.

The reluctance expressed by utilities in the Oklahoma proceedings is consistent with the results of a 2003 NRRI survey of the state utility commissions. The survey found that 54% of the responding states reported that utilities were either somewhat or very reluctant to share pertinent security information with the commission (see Figure 5). This was despite the fact that 82% of the responding commissions offered protection for security information from disclosure under the Freedom of Information Act (FOIA) or similar laws (see Figure 2 above).

b. Security Measures

The participants in the Technical Conferences agreed that whatever security standards or guidelines are used by the OCC should be consistent with other state and federal guidelines. The utilities argued that industry-group guidelines such as those issued by

Figure 5: Are utilities perceived to be reluctant to share security-related information with state commissions?



Yes - Most are. Over half of state public service commissions (PSCs) judged their jurisdictional utilities as being hesitant to share details of their security measures with the commissions.

Source: Authors' construct from McGarvey and Wilhelm (2003), n=48.

NERC, DOT, or NRIC were already in place and offered a sufficient measure. No consensus was reached as to whether the guidelines should be mandatory or voluntary. Mandatory guidelines offer certainty, but the regulated utilities expressed concern about the lack of flexibility they would have to tailor there own security plans for their own needs. A related concern is the differing effects of uniform sets of standards on large versus small companies; if all companies are forced to make the same expenditures, this could place a disproportionate burden on the small companies.

The 2003 NRRI survey of state commissions found that 57% of the commissions believed that most security investment had been driven by the

utilities themselves, while 32% of state commissions believed most investment had been driven by some combination of state or federal agencies (see Figure 6).

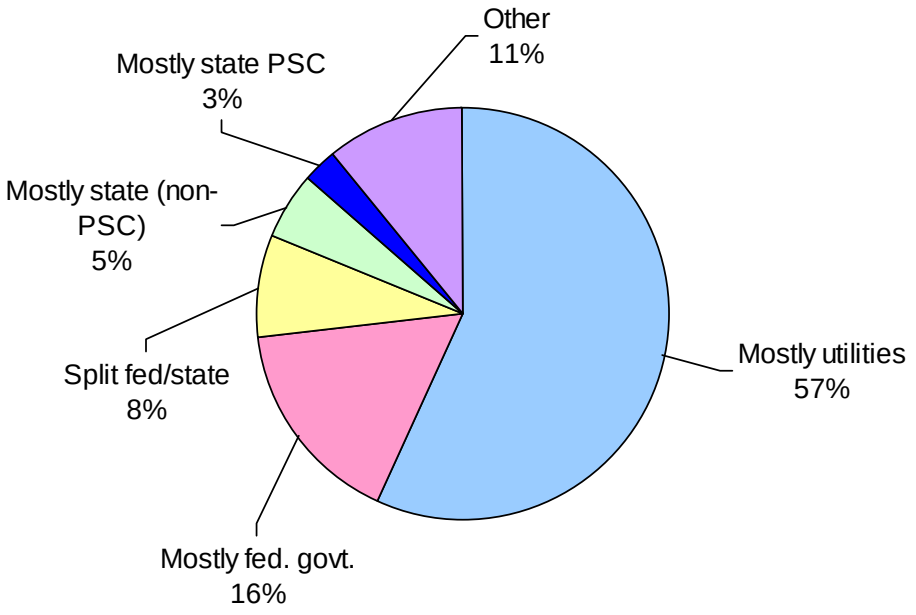
In addition, regulators can not simply assume that companies that are not subject to PUC regulation, such as electric cooperatives or independent power producers, will make the same expenditures on security as the regulated companies. A competitive business could be expected to only consider security costs to the extent that they will not be rendered uncompetitive. The PUC is interested in assuring that the public continues to receive service, yet at the same time is aware that utilities must have the opportunity for financial health if they are to be able to serve the public in the long term.

Utilities have the most direct interest in their own security, and ultimately the company is responsible for creating and enacting sufficient security plans. The OCC staff suggested that each company designate a high-level executive to review and certify the companies' compliance with the relevant guidelines and to develop and implement a security plan that would be subject to an annual assessment by the commission. The OCC staff suggested legislation might be appropriate to formalize what would define an acceptable security plan. Although some utilities objected to specifying the plan in a statue, the staff suggested the following elements be included in the definition:

1) Identification of critical infrastructure
2) Vulnerability assessment
3) Existence of a chain of command for operation decisions in the event of an emergency
4) Communications plan for vital public information
5) Continuity of operations provisions
6) Damage assessment procedures
7) Response and recovery procedures
8) Plans for interaction with state and federal emergency response officials

The participants agreed that, as it is impossible to plan for every possible form of terrorist attack, network industries should not be penalized for not foreseeing the unforeseeable. This concept is embedded in traditional regulation, which includes a proscription

Figure 6: Who is driving security-related investments?



According to state public utility commissions (PUCs) ─ It's mostly the utilities.

Source: Authors' construct from McGarvey and Wilhelm (2003), n=37 (10 other states reported no investments).

against hindsight when judging the prudence of an investment. In other words, while prudence is determined after an investment decision is made, regulators should not substitute an examination of the final outcome for standards of reasonableness at the time of the decision. Participants agreed that any legislation or commission rules should indicate that companies should not be held subject to private litigation based on the claim that either taking preventative or remedial action against terrorism makes the companies liable for failing to stop a terrorist attack.

c. Cost Recovery

The Technical Conference participants considered the use of legislation or PUC rules to explicitly allow the OCC to authorize the recovery of security costs. They suggested that provisions for such proceedings should be placed in commission rules rather than in legislation. Most of the regulated

utilities agreed that it is appropriate to consider security as any other ordinary cost of business, and therefore subject to normal regulatory accounting principles. Accordingly, the operating costs must be proven to be reasonably incurred, known, and measurable in order to be recoverable. The capital costs would also be subject to the "used and useful" test.[22]

The consensus among the participants was that most security costs could be handled in the course of a normal rate case. Telecommunications companies, which no longer undergo traditional rate cases, indicated that they would be unlikely to seek cost recovery unless new government mandates were put in place. However, utilities from all sectors also expressed support for having the option to pursue recovery outside of a normal rate case, especially if the security costs were the result of new government regulations.

The utilities underscored the potential for cost recovery proceedings to reveal both commercially sensitive and security sensitive information and were eager for special procedures to maintain the confidentiality of company information provided in the course of cost recovery proceedings. The Attorney General's Office expressed the belief that the current rules for protecting commercially sensitive information during proceedings would be sufficient, but that it might be beneficial to modify rules governing the issuance of protective orders, as long as any changes are uniformly applied and included specific guidelines to continue to allow the meaningful participation of, and discovery by, third parties to the proceedings.

3. Notice of Proposed Rulemaking in the State of Oklahoma

At the conclusion of the technical conferences the OCC released Notice of Proposed Rulemakings (NOPRs) on critical infrastructure protection for the electric, gas, and telecommunications sectors and issued final rules in December 2004 (see Appendices H, I, and J). The rules affirm the OCC's jurisdictional and supervisory authority to address the reasonableness and prudence of costs incurred by utilities for

[22] See Duquesne Light v. Barash, 488 U.S. 299 (1989).

homeland security and the protection of critical infrastructure from extraordinary events (natural and man-made). The rules encourage all electric, gas and telecommunications utilities to develop, implement, and maintain an annually updated Homeland Security and Critical Infrastructure Plan. Such a plan is required of any utility seeking cost recovery outside of a general rate review. Electric companies should follow the latest National Electric Reliability Council (NERC) 'Security Guidelines and Standards.' Security plans for gas companies should follow the most current U.S. Department of Transportation, Office of Pipeline Safety's 'Pipeline Security Information Circular' and 'Pipeline Security Contingency Plan Guidance' (DOT/OPS Guidelines). Telephone service providers would follow the most current Network Reliability and Interoperability Council (NRIC) 'Best Practices Security Guidelines and Standards' and the National Fire Protection Association's (NFPA) 'NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs.'[23]

The rules establish the restrictions on security cost recovery outside of a general rate case. The rules also detail confidentiality standards, set utility annual reporting requirements, and establish that only those Commission staff, state Attorney General personnel, and outside parties who have been authorized by the Commission may have access to a utility's plan.

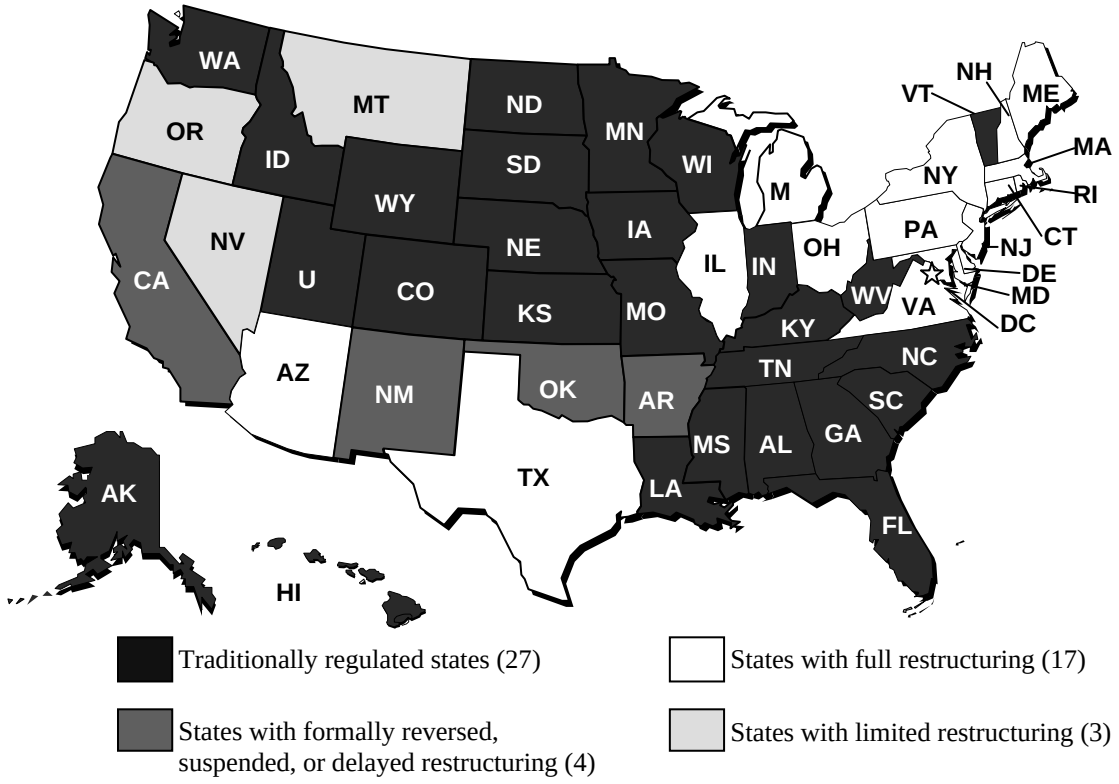
This is not the only route for other state commissions to take to address the challenges of securing critical infrastructure. The approach that a state commission might take is affected by whether the states have restructured their energy markets (19 states plus the District of Columbia) or traditionally regulated markets (31 states; see Figure 7).[24]

While restructured states no longer have the traditional general rate case (GRC) in which to interact with utilities and address security issues, commissions in those states generally have a significant degree of responsibility to ensure the

[23] NFPA standard available at http://www.nfpa.org/PDF/nfpa1600.pdf?src=nfpa

[24] Scott Potter, *After the Freeze: Issues Facing Some State Regulators as Electric Restructuring Transition Periods End*, No. 03-18 (Columbus: NRRI, 2003).

Figure 7: Map of state electricity markets



Source: Authors' construct from Potter (2003), updated to March 2005.

security and reliability of utility services (particularly at the distribution level). Some restructured states still allow utilities and regulators the option to pursue special regulatory treatments to resolve security cost recovery issues.[25]

D. COST RECOVERY PROCEDURES AND MECHANISMS

The national expert focus group and the state-based efforts in Oklahoma both revealed that one of the central concerns for utility industries and regulators alike

[25] For example, the Florida commission employed fuel adjustment clauses after it granted approval in a small number of cases in which utilities applied to recover cover increased security costs stemming from mandates by the Nuclear Regulatory Commission. The Iowa commission allowed changes to the base tariff rate in three cases. The New York Public Service Commission relies on existing rate processes to address cost recovery including consideration of settlements, forecast reconciliations, and deferral of carrying charges; utilities that are under-earning can file for deferral under Commission rules. The New Jersey commission started an ongoing informal dialogue by creating utility industry working groups to identify best practices, develop guidelines, and discuss security financing.

is the need for cost recovery of security-related expenditures. Utilities expect that state commissions will approve recovery of appropriate critical infrastructure protection expenses. Below we identify and discuss security cost recovery procedures that are appropriate for energy utilities in a variety of regulatory frameworks, in states with both restructured and traditionally regulated energy markets. We also review the existing cost recovery mechanisms successfully used by state commissions associated with each procedure.

Cost recovery procedures for critical infrastructure, like much of regulation, are about process.

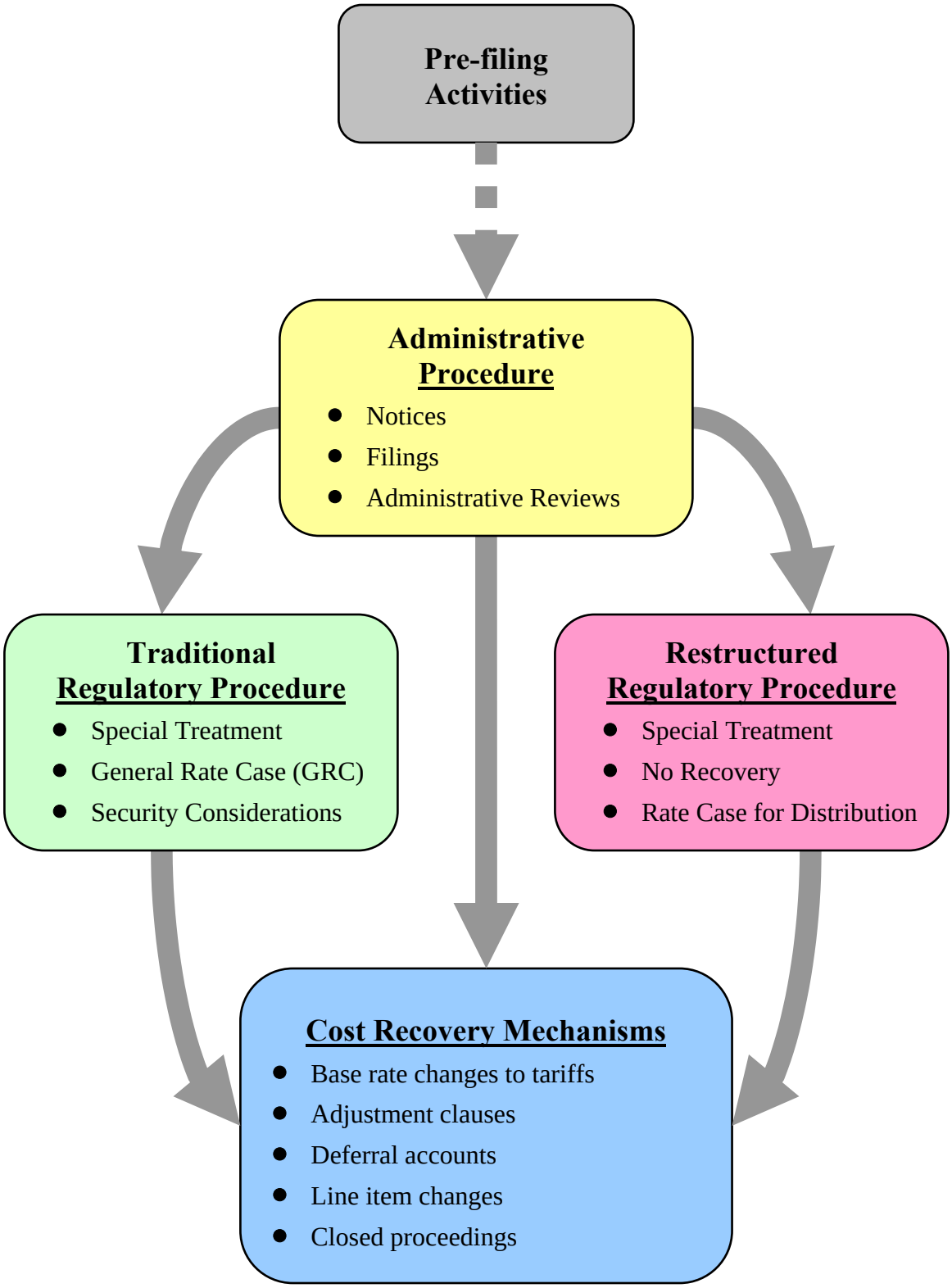
- A **cost recovery procedure** is the identifiable process that a commission uses to address a request by a utility in order to determine whether requested monies will be recovered.
- A **cost recovery mechanism** is the specific technique used for cost recovery. The procedure underlies the logic path for cost recovery for a rate regulated utility and the cost recovery mechanism, say, an adjustment clause, is how the commission authorizes the actual cost recovery.

The circumstances in different states may make one procedure more appropriate than another, but the actual cost recovery mechanisms — such as a deferral account — can be used in more than one procedure. In some states new legislation or regulatory proceedings were developed to deal with critical infrastructure cost recovery. In most cases existing regulatory cost recovery mechanisms were used. Nearly all of the procedures include a path to some form of a rate case proceeding.

1. Cost Recovery Procedures

Cost recovery procedures for critical infrastructure investment mirror the regulatory reforms that states have undertaken in the past decade. In the energy arena a mix of rate base regulated and competitive market regulatory frameworks exist, with cost recovery requests occurring only in the regulated portions of each sector. In addition to energy utilities, water utilities have made a significant number of recovery

Figure 8: Detailed security-related cost recovery procedure diagram



requests, all of which have been handled under a rate base regulatory process. Some form of price caps is the dominant type of regulation for telecommunications utilities. Accordingly, it is not unexpected that no security cost recovery requests were reported in our survey for telecommunications providers.

Figure 8 provides a general framework for the discussion of cost recovery procedures and identifies three procedures (administrative, traditional, and restructured) along with a set of cost recovery mechanisms.[26] While any state regulatory commission may have important variations, the protocols can be applied to different regulatory regimes and specific cost recovery situations. The cost recovery mechanisms available are the same for all three procedures, but there are differences in the underlying logic within each of the three procedures.

[26] Price caps generally have an exogenous adjustment factor that allows a utility to request cost recovery for extraordinary expenditures caused by circumstances outside the control of the utility. However, exogenous adjustments are unusual because all costs of a utility (those that have increased and those that have decreased) since base price caps were established would likely have to be examined. Incremental security cost increases, while significant, may not have reached the extraordinary cost threshold.

All states have administrative processes that occur on the front end of a cost recovery issue. Depending on the circumstances, this may lead directly to a cost recovery mechanism, or down one of the other procedural paths (traditional or restructured).

In a restructured environment, cost reimbursement requests are examined differently than in a traditionally regulated market. Regulatory standards such as used and useful, just and reasonable, and prudence tests are similarly applied in each procedure, except that a competitive market perspective is also employed in the restructured regulatory environment. In most states security investments have been initiated by utilities and not necessarily solely in response to governmental directives (see Figure 2). Interestingly, the utilities in most states have not filed for recovery security costs (see Figure 3).

2. Pre-Filing Activities and Administrative Procedure

Prior to the filing of a formal rate case, state rules may permit a utility to discuss issues with the state commission. Two

types of preliminary activities identified are pre-filing discussions and ongoing dialogues. While significant differences exist between states,

- Some state rules allow for discussions between utility and regulator prior to filing. This can serve to brief regulators about security cost considerations.
- Another activity is to promote an ongoing dialogue, such as New Jersey has done, that allows regulators and utilities to discuss infrastructure security issues, including cost recovery.

Commissions clearly have a well-formed set of administrative processes for addressing cost recovery issues. These processes serve as filters. The administrative procedure for security-related costs is applicable if and when a legislative act or commission rule specifies a particular cost recovery mechanism, such as Connecticut's Special Infrastructure Cost Recovery Hearing. This allows the commission to have a more focused cost recovery process, and not to have to rely on the traditional regulatory procedure.

3. Regulatory Procedures

Regulatory procedures guide the processes state commissions use to make cost recovery decisions. In states with vertically integrated, rate base regulated electric and natural gas utilities (see Figure 4), rate cases are the primary way that critical infrastructure costs are addressed. Iowa, for example, examined and allowed specifically identified critical infrastructure costs in several rate cases. In some other states, rate cases were pending but not resolved. Most states surveyed by NRRI indicated that they had not seen a specific critical infrastructure protection cost recovery request.

In states with restructured electricity markets, generally a base rate case exists that deals with cost recovery. The logic underlying a utility cost recovery request is that the increase in security costs was not known at the time of restructuring and that a filing to recover these costs is appropriate. In Connecticut, as noted above, and in Michigan the legislature acted to allow the regulator to consider cost recovery. In restructured markets

cost recovery is more risky than in traditionally regulated markets.

In each of the cost recovery procedures and cost recovery mechanisms, regulators consider all cost changes before determining what security costs are authorized for recovery, although cost recovery is not guaranteed, just allowed. A utility may present valid and well-documented critical infrastructure protection cost information, but not be allowed the opportunity for cost recovery because an equal offsetting cost savings has occurred. It may be that the cost-of-capital has decreased and these documented savings necessarily reduce some portion of the security costs allowed for recovery. Equally, significant cost offsets may not exist, or may be dealt with in a subsequent proceeding. These cost recovery considerations also apply to regulated water and telecommunications utilities.

4. Cost Recovery Mechanisms and Options

NRRI's survey of the states identified eight main cost recovery mechanisms that have been successfully implemented in various states. Utilities have been allowed the opportunity to recover their critical infrastructure protection costs in restructured as well as traditional regulatory environments.

a. Base Rate Changes to Tariffs

A rate case is the standard way regulated utilities recover costs through a change to the existing, or base, tariff. While all of the mechanisms listed in Table 1 serve distinct purposes, they all have a common origin in a rate case where utility requests to change tariffs are resolved. In a traditional regulatory environment procedure other types of cost recovery mechanisms are possible—most notably an adjustment clause—but each mechanism is either authorized in or reconciled to the rates previously approved in a rate case, although a significant time lag may exist. In a restructured environment procedure, commissions are able to consider rate changes for distribution rates, or retail customers, or standard offer customers, but these are generally tied to an initial rate case. NRRI found:

- States with pending utility rate case filings for critical infrastructure cost recovery, but as no action had been taken no trend lines can be drawn.
- States with rate cases filed, but which do not have specific security costs identified.
- Instances where utilities have indicated that they do not intend to file for cost recovery.
- Iowa's consideration and approval of security costs.

b. Adjustment Clauses

In many states adjustment clauses may be used to recover extraordinary costs that occur between rate cases. The Florida Public Service Commission used two different adjustment clauses to allow, in part, three Florida utilities to recover security costs due to compliance with a Nuclear Regulatory Commission order and for security actions taken that were consistent with Presidential Homeland Security directives and North American Electric Reliability Council actions.[27] Some of the costs authorized for recovery were costs that would normally be classified as capital items.

c. Closed Proceedings

Except for proprietary information, commission proceedings are generally open. Due to security concerns, the Kansas Legislature acted to provide a confidential proceeding where the amount of recovery requested, the amount allowed, and the method of cost recovery were kept confidential.[28] Its focus was on post-9/11 security costs and provides for a cost recovery period within half of the useable lifetime of the investment. The Act also allowed the Citizen's Utility Ratepayer Board access within a protective order.

d. Deferral (Balancing) Accounts

Deferral accounts allow a utility to accumulate critical infrastructure protection expenditures that may be recovered in a rate case or other proceeding. This may be the cost recovery mechanism most commonly

[27] See Florida Public Service Commission, Order No. PSC-02-1761-FOF-El and Florida Public Service Commission, Order No. PSC-01-2516-FOF-El.

[28] See 2003 Kansas HB 2374, codified as Kansas Statute Nos. 66-1234, 66-1235, and 66-1236.

used in conjunction with other cost recovery mechanisms. The Michigan legislature specifically authorized such an account so that costs could be accrued and deferred until rate caps are removed.[29]

e. Line Item Charges

In addition to general costs, a commission may allow a specific cost to be recovered and be separately identified on a consumer's bill. In Michigan, enhanced security costs can be recouped through a security recovery factor. In authorizing recovery the commission must determine if costs are reasonable and prudent and are jurisdictionally assigned to retail customers.

f. Notice of Inquiry

Rather than using a rate case, a commission may initiate a special proceeding or notice of inquiry (NOI) to establish a cost recovery framework (see Table 2). Cost recovery, confidentiality of data, and other critical infrastructure protection issues have been approached by Oklahoma through the NOI process.[30] Cost recovery was a central issue covered. Formal commission action is still pending, however.

g. Ongoing Dialogue

Both New Jersey and Ohio told NRRI that they had a dialogue with their utilities. In New Jersey dialogue occurred through the New Jersey Infrastructure Advisory Committee. In Ohio utilities are informally polled as they file rate cases.

h. Special Infrastructure Cost Recovery Proceeding

The Connecticut legislature acted to ensure ratemaking consideration of security costs. Connecticut regulators must examine the costs and find them reasonable. Connecticut has accepted some costs, but not others.

5. Cost Recovery Considerations

Subsequent to a determination that there is a need for recovery of costs, how

[29] Michigan Compiled Law, Chapter 460, Act 3 of 1939, Section 460.10d (17) (c).

[30] See Oklahoma Corporation Commission, Case No. PUD 200300624.

closely a state commission might want to exercise its prudence review should be influenced in part by the type of regulation to which the particular utility is subject. In other words, which procedural path is most appropriate?

If the anticipated expenditures on security are relatively small and the utility is over-earning, then a utility might be reluctant to bring a rate case to recover its additional cost. Some utilities might be uncertain about expending money or investing in security if they are subject to a price cap or a rate freeze. In such a situation, all other things being equal, there might be an incentive for the utility to under-invest in security measures. This can be particularly troublesome as many security-related expenditures have positive externalities and they might have the effect of making the utility network more secure. Equally, state commissioners are also sensitive to not creating an incentive for carte blanche expenditures on security, which in turn end up directly in higher rates. State and federal commissions have been sensitive to any possible incentive for a utility to cut expenditures to suboptimal levels under price cap or rate freezes, unless other mechanisms for cost recovery are created.

The policy implications are that:

- State commissions regulating utilities subject to either a price cap or rate freeze might mandate security measures (which would be difficult to the extent that asymmetry of information would tend to favor the utility having expertise over the commission).
- The commission might try to isolate prudently incurred security-related expenditures, or investments and provide for a special rate adjustment or rate supplement mechanism to allow these costs to be recovered.

At the federal level, as of June 2004, the FERC had approved at least five cost recovery surcharges.[31] And, as stated in the *FERC's FY 2005 Congressional Performance Budget Request*, the FERC plans to give its highest priority to processing any filing made for the recovery of extraordinary expenditures to

[31] Federal Energy Regulatory Commission, *FY 2005 Congressional Performance Budget Request*, February 2004, p. 34. Report is available at http://www.ferc.gov/about/strat-docs/FY05-Budg.pdf.

safeguard the reliability of our energy transportation systems and energy supply infrastructure. The FERC has set as its performance target of timely processing of such filings: within 30 days for gas and oil rate filings and within 60 days for electric filings.[32]

6. Other Implications

Other implications for states when considering critical infrastructure cost recovery requests include:

- **A need exists for critical infrastructure protection standards or guidelines** that regulators and utilities can use in ensuring that critical infrastructure is protected and that can be used in a cost recovery proceeding, which may be used in a pre-approval or other regulatory proceeding. State commissions can and have made cost recovery decisions without guidelines, but having guidelines is especially helpful for resolving prudence, reasonableness, and used and useful concerns.

- Commissions should **examine existing guidelines** issued by the North American Electric Reliability Council (NERC), the Network Reliability and Interoperability Council (NRIC), and the Department of Transportation's Office of Pipeline Safety (OPS) as a baseline for determining the guidelines or standards that they will use in their proceedings.

- Standards are more prescriptive than guidelines, but **standards may make cost recovery less problematic**. Guidelines, however, may offer greater flexibility that accounts for regional differences.

- **Critical infrastructure investments also need to be thought of as investments that increase shareholder value**. Both commissions and utilities have a common interest in ensuring continuity of service, but utility shareholders have the added interest in ensuring that net future revenue streams are not disrupted by terrorist attacks.

[32] Ibid., p. 85.

- Providers of utility services may be fully or partially regulated, or not regulated at all. Cost recovery for a vertically-integrated regulated utility raises a different set of issues than a partially-regulated utility in a price cap setting. **To date, all identified security cost recovery has occurred directly or indirectly in a rate case proceeding.**

- Whether or not standards or guidelines are used, **the state regulatory commission remains the final decision maker** (within constraints set by legislation and court decisions) regarding the timing, amount, and items eligible for cost recovery. A finding of prudence or reasonableness by a commission was a common part of all proceedings.

- **Pre-approval mechanisms exist,** but all identified have been eventually integrated in a larger rate case proceeding.

- **Utilities felt a strong need to have an informal dialogue with regulators** about their critical infrastructure plans. Procedures and rate cases may need to have this flexibility.

- **Insurance** may be difficult to acquire, but regulators may wish to see that insurance was considered as an option.

E. CONCLUSION

As the country's leaders confront the issue of how to protect against attacks on its critical infrastructure, state legislatures and public utility commissions have already begun to address the special role that the commissions will play. The NRRI has helped inform this process by using experts from across industries and levels of government to frame the relevant issues, in turn inspiring and assisting a state commission in taking the lead to establish, via a rulemaking, the capacity of public utility commissions to help ensure the security of the nation's critical infrastructure.

The state regulatory commission's role is a limited one in the larger scope of homeland security, but it is one in which state commissions have a unique authority: determining how to pay and who should pay for security costs. States are able to rely on existing regulatory procedures for carrying this authority, and can adapt these procedures to ensure the reliability and safety of the nation's critical utility infrastructure. This capability makes them somewhat unique in that they can be full partners with federal regulators without having to necessarily request federal funding.

Appendix A

List of Preliminary Descriptors Developed by the National Expert Group

The preliminary descriptors are the responses of the National Expert Group to the question "What will be the most important descriptors (trends, barriers, issues, factors, etc.) affecting the role of PUCs in Homeland Security by 2006?" Each participant was asked to select eight ideas from the master list of 40 that he or she judged to be the most important and to assign points to each ranging from eight, high, to one, low. The rank order of the descriptors is determined first by the sum of points received and second by the number of votes cast for a given descriptor.

Rank	Descriptor	Score	Number of Votes
1	Sorting out *who has responsibility* for what in Homeland Security – whose standards? – whose responsibilities to enforce?	65	9
2	Implementing or facilitating *cost recovery mechanisms* for the regulated utilities for their security investments – directly or indirectly – including issues of insurance and self-insuring	46	6
3	The *internal capabilities of the PUCs* – can they fulfill their duties? The availability of resources for PUCs.	43	10
4	*Resource allocation* in the event of a disruption in coordination with Federal government and others (state agencies, locales, etc.) – particularly electric load allocation and restoration priorities	43	7
5	Willingness of utilities to share *proprietary information* – intellectual property issues – business sensitive information – legal and privacy protection issues	36	10
6	Develop Homeland Security *information sharing protocols* – manage public release of information – protect business sensitive and classified information [also protect vulnerability information that could be used by terrorists]	33	7
7	*Terrorist attacks and threats*	33	6
8	PUC to be the manager and facilitator of *information between state emergency agencies and utilities* – an example is Oklahoma – alert network – ISAC	29	5
9	*Public priority of Homeland Security*	28	5
10	*Public perceptions of vulnerability* – public confidence	25	6
11	*Deteriorating, aging infrastructure*	23	7
12	*Sustainability of effort* Using *existing failure/accident plans and routines* to feed into larger disaster plans and routines	20	4

13	Regulation vs. deregulation vs. non-regulation [changing roles of the PUCs relative to deregulation of the utilities and how deregulation fits with the requirements of Homeland Security] – who follows the *non-regulated infrastructure*?	17	5
14	Regional/local public affairs agent – explanation and education [to and for the public relative to disasters] – *plans to communicate to the public in cases of disasters*	13	5
15	PUC will take lead role in facilitating *local and regional coordination of public and private exercises* – field and table-top exercises – simulations, plans, co ordinations, etc.	13	4
16a*	PUC commissioners to enable and incent increased "*shock absorbers*" [redundancy and surplus capabilities to withstand a terrorist attack or a natural disaster] in the infrastructure through new and innovative programs, technology creation, assessment, and technology transfer – consider impacts on policies and markets	13	2
16b*	Be prepared to identify *critical nodes of utility infrastructure* before and during orange alerts	13	2
16c*	Compliance officer role and [cost] *reasonableness review* – cost appropriate -- prudency	13	2
19a*	Credible, actionable, and timely *intelligence* [concerning terrorists threats and attacks]	12	3
19b*	PUCs facilitate *data and information sharing* by companies with each other – for example, pipeline companies with electric utilities – creation of a crisis response asset database	12	3
21a*	Assuming that resources (people, money, and authority) are available, analyzing and evaluating *sufficiency of vulnerability and risk assessments* conducted by utilities	11	2
21b*	Protecting utility security systems – time dynamic *forecasting of future needs* – predictive – strategic planning – first preventers	11	2
23	In coordination with public utility companies and other stakeholders, develop and selectively enforce *standards for the protection of public utilities* – multi-state level	10	3
24a*	*Technical advances*, like the self-healing grid	10	2
24b*	*Regulatory review and rationalization* relative to Homeland Security issues – review of regulatory models [in the light of new security requirement] – revision of models – the regulatory matrix – recognition of inter-dependencies of utilities	10	2

26	*System architecture for security* – will market-based economy support a secure architecture? System optimization.	9	3
27	*Determining appropriate redundancies*	9	2
28a*	*Updating and keeping current analysis and planning* – updating and revising contingency plans and emergency communications	7	2
28b*	Using *existing failure/accidents plans and routines* to feed into larger disaster plans and routines	7	2
28c*	Advocate for private utilities relative to other Federal and state agencies – *training, planning, and information*	7	2
31a*	Coordination and facilitation of all requests for critical *asset information* from Federal government, states, and locales	6	3
31b*	Consistency of *PUCs regulations* with each other [consistency of PUC regulations from state to state]	6	3
33	Siting of new and upgraded facilities	6	2
34	*Educating* people about the issues	4	1
35a*	*Integration of physical and cyber* [systems and security]	2	2
35b*	*Potential change of administration*	2	2
37	Coordinating with *independent and regional transmission systems operators* – RTOs and ISOs – sharing information with them	2	1
38a*	The aging workforce – issues of *training*	0	0
38b*	Growing U.S. *dependency on foreign manufacturing and software development*, etc.	0	0
38c*	Continued *capabilities of the U.S. military* – active duty, Reserves, and National Guards	0	0

Note: An asterisk (*) indicates descriptors that are tied with other items in both total score and number of votes received.

Appendix B

List of Final Descriptors Developed by the National Expert Group

Drawing from common themes in the list of preliminary descriptors (see appendix A), the National Expert Group developed a final list of 11 descriptors.

Descriptor	**Derived from preliminary descriptors, as listed in Appendix A**
1. Role of State Public Utility Commission	1,16c, 24b,
2. Allocation of Responsibility for Information Management	5, 8, 19b, 31a
3. Allocation of Responsibility for Coordination and Communication	9, 14, 15, 21b, 28c, 34, 37
4. Allocation of Responsibility for Cost Recovery (Who Pays)	2, 16a, 27
5. Public Perception of Threat/Vulnerability	10, 19a
6. Level of Terrorist Attacks on Utility Infrastructure	7, 19a
7. PUC Security Capabilities	3, 12, 21a, 28a
8. PUC Role in Restoration Priorities	4
9. Information Sharing Protocols and Willingness to Share Information	6, 8, 19b
10. Responsibility for Key Asset Protection and Mitigation	2, 9, 16a, 21a, 26, 27, 31a, 35a, 38c
11. Standards for Utility Security	1, 9, 23

Appendix C

List of Descriptors, Alternative States (Outcomes), and *a priori* Probabilities of Occurrence used in Interactive Futures Simulation (IFS™)

Descriptors	States	*A Priori* Probabilities
1. Role of State Public Utility Commissions		
	A. broad	0.15
	B. medium	0.55
	C. limited	0.30
2. Allocation of Responsibility for Information Management		
	A. strong Federal leadership, regulation, and direction	0.35
	B. mostly shared Fed and state roles	0.55
	C. mostly states, local, and utility initiatives	0.10
3. Allocation of Responsibility for Coordination and Communication		
	A. primarily Federal (top-down)	0.35
	B. primarily shared between Fed and state governments	0.55
	C. primarily driven by states, locales and private sector	0.10
4. Allocation of Responsibilities for Cost Recovery (Who Pays) (cost recovery for mitigation, strategies and implementation)		
	A. primarily tax payers (Fed, State, and local taxes)	0.20
	B. primarily rate payers/customers	0.50
	C. primarily shareholders	0.30
5. Public Perception of Threat/Vulnerability		
	A. high, engaged	0.20
	B. moderate	0.45
	C. low	0.35

Descriptors	States	*A Priori* Probabilities
6. Level of Terrorist Attacks on Utility Infrastructure		
	A. high number, high consequence	0.05
	B. low number, high consequence	0.25
	C. high number, low consequence	0.10
	D. low number, low consequence	0.45
	E. none	0.15
7. PUC Security Capabilities (in-house capabilities)		
	A. high: skilled, robust, sustainable	0.15
	B. medium: basically competent	0.40
	C. low: struggle	0.35
	D. none	0.10
8. PUC Role in Restoration Priorities		
	A. high, mostly responsible	0.30
	B. shared with Feds	0.20
	C. low (utility driven)	0.50
9. Information Sharing Protocols and Willingness to Share Information		
	A. protocols exist, high willingness/cooperation	0.10
	B. variable, developing	0.30
	C. low, poorly implemented	0.60
10. Responsibility for Key Asset Protection/Mitigation		
	A. mostly Federal	0.15
	B. mostly state and local	0.05
	C. mostly utilities	0.80
11. Standards for Utility Security (standards and enforcement)		
	A. high	0.20
	B. medium	0.60
	C. low	0.20

Note: *A priori* probabilities were developed during the National Expert Group by consensus and represent only the general estimate of the group.

Appendix D

Descriptor Cross-Impact Analysis

The National Expert Group related the effects of the descriptors on each other. This table indicates the consensus estimate of the group as to whether there is a direct effect of a given descriptor on another, whether the impact is positive (i.e., more likely to occur) or negative (i.e., less likely to occur), and whether the effect is strong (3), moderate (2), or weak (1). The result in any given cell represents the effect of the descriptor listed in the corresponding column heading (i.e., the "driver" descriptor) on the descriptor described in the relevant row heading (i.e., the "driven" descriptor).

Note: Descriptors are sometimes abbreviated; see Appendix C for a full list of the terms used below.

Descriptor (Driver)		1. Role of State PUC			2. Responsibility for Information Mgt.			3. Responsibility for Coordination / Communication			4. Responsibility for Cost Recovery			5. Public Perception of Threat			6. Level of Attacks					7. PUC Security Capability				8. PUC Role in Restoration Priorities			9. Information Sharing			10. Responsibility for Asset Protection			11. Standards for Utility Security				
Descriptor (Driven)	Alternative Descriptor States	0.15 A. broad	0.55 B. medium	0.30 C. limited	0.35 A. strong Fed	0.55 B. mostly shared	0.10 C. mostly state	0.35 A. federal	0.55 B. shared fed/st	0.10 C. state/local/priv	0.20 A. tax payers	0.50 B. shareholders	0.30 C. customers	0.20 A. high, engaged	0.45 B. moderate	0.35 C. low	0.05 A. high #, hi cons	0.25 B. low #, hi cons	0.10 C. high #, lo cons	0.45 D. low #, lo cons	0.15 E. none	0.15 A. high: skilled	0.40 B. medium	0.35 C. low: struggle	0.10 D. none	0.30 A. high	0.20 B. shared feds	0.50 C. low (utility)	0.10 A. high	0.30 B. variable	0.60 C. low	0.15 A. mostly Fed	0.05 B. mostly state	0.80 C. mostly utility	0.20 A. high	0.60 B. medium	0.20 C. low	Sum of Values	Non-Zero Entries
1. Role of State PUC	0.15 A. broad	*	*	*	-2	0	2	-3	-1	3	0	0	0	0	0	0	1	0	0	0	-1	3	1	-1	-3	3	1	-3	2	0	-2	-2	0	2	2	0	-2	0	20
	0.55 B. medium	*	*	*	-1	1	1	-1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	-1	-1	1	1	-1	1	1	-1	-1	1	1	1	1	-1	6	22
	0.30 C. limited	*	*	*	2	0	-2	3	1	-3	0	0	0	0	0	0	-1	0	0	0	1	-3	-1	1	3	-3	-1	3	-2	0	2	2	0	-2	-2	0	2	0	20
2. Responsibility for Information Management	0.35 A. strong Fed	-2	0	2	*	*	*	3	1	-3	3	1	-3	3	1	-3	3	1	0	-1	-3	0	0	0	0	0	0	0	2	0	-2	3	1	-3	0	0	0	4	20
	0.55 B. mostly shared	-1	1	1	*	*	*	1	1	-1	1	1	-1	1	1	-1	1	1	0	-1	-1	0	0	0	0	0	0	0	1	1	-1	1	1	-1	0	0	0	6	22
	0.10 C. mostly states	2	0	-2	*	*	*	-3	-1	3	-3	-1	3	-3	-1	3	-3	-1	0	1	3	0	0	0	0	0	0	0	-2	0	2	-3	-1	3	0	0	0	-4	20
3. Responsibility for Coordination, Communication	0.35 A. federal	0	0	0	3	1	-3	*	*	*	2	0	-2	3	1	-3	3	1	0	-1	-3	-1	0	0	1	-1	0	1	2	0	-2	3	1	-3	0	0	0	3	21
	0.55 B. shared fed/state	0	0	0	1	1	-1	*	*	*	1	1	-1	1	1	-1	1	1	0	-1	-1	0	0	0	0	0	0	0	1	1	-1	1	1	-1	0	0	0	5	19
	0.10 C. state/local/private	0	0	0	-3	-1	3	*	*	*	-2	0	2	-3	-1	3	-3	-1	0	1	3	1	0	0	-1	1	0	-1	-2	0	2	-3	-1	3	0	0	0	-3	21

Descriptor (Driven)	Alternative Descriptor States	1. Role of State PUC				2. Responsibility for Information Mgt.				3. Responsibility for Coordination / Communication				4. Responsibility for Cost Recovery				5. Public Perception of Threat				6. Level of Attacks						7. PUC Security Capability					8. PUC Role in Restoration Priorities				9. Information Sharing				10. Responsibility for Asset Protection				11. Standards for Utility Security					
	Descriptor (Driver)	0.15 A. broad	0.55 B. medium	0.30 C. limited		0.35 A. strong Fed	0.55 B. mostly shared	0.10 C. mostly state		0.35 A. federal	0.55 B. shared fed/st	0.10 C. state/local/priv		0.20 A. tax payers	0.50 B. shareholders	0.30 C. customers		0.20 A. high, engaged	0.45 B. moderate	0.35 C. low		0.05 A. high #, hi cons	0.25 B. low #, hi cons	0.10 C. high #, lo cons	0.45 D. low #, lo cons	0.15 E. none		0.15 A. high: skilled	0.40 B. medium	0.35 C. low: struggle	0.10 D. none		0.30 A. high	0.20 B. shared feds	0.50 C. low (utility)		0.10 A. high	0.30 B. variable	0.60 C. low		0.15 A. mostly Fed	0.05 B. mostly state	0.80 C. mostly utility		0.20 A. high	0.60 B. medium	0.20 C. low		Sum of Values	Non-Zero Entries
4. Responsibility for Cost Recovery	0.20 A. primarily tax payers	0	0	0		0	0	0		0	0	0		*	*	*		1	0	-1		2	0	0	0	-2		0	0	0	0		0	0	0		0	0	0		2	0	-2		-2	0	2		0	8
	0.50 B. primarily customers	0	0	0		0	0	0		0	0	0		*	*	*		0	0	0		1	0	0	0	-1		0	0	0	0		0	0	0		0	0	0		1	1	-1		-1	1	1		2	8
	0.30 C. primarily shareholders	0	0	0		0	0	0		0	0	0		*	*	*		-1	0	1		-2	0	0	0	2		0	0	0	0		0	0	0		0	0	0		-2	0	2		2	0	-2		0	8
5. Public Perception of Threat	0.20 A. high, engaged	0	0	0		0	0	0		-1	0	1		0	0	0		*	*	*		3	1	0	-1	-3		0	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		0	6
	0.45 B. moderate	0	0	0		0	0	0		0	0	0		0	0	0		*	*	*		1	1	0	-1	-1		0	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		0	4
	0.35 C. low	0	0	0		0	0	0		1	0	-1		0	0	0		*	*	*		-3	-1	0	1	3		0	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		0	6
6. Level of Attacks on Infrastructure	0.05 A. high number, high consequence	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		*	*	*	*	*		0	0	0	0		0	0	0		-1	0	1		-2	0	2		-2	0	2		0	6
	0.25 B. low number, high consequence	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		*	*	*	*	*		0	0	0	0		0	0	0		0	0	0		-1	0	1		-1	0	1		0	4
	0.10 C. high number, low consequence	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		*	*	*	*	*		0	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		0	0
	0.45 D. low number, low consequence	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		*	*	*	*	*		0	0	0	0		0	0	0		0	0	0		1	0	-1		1	0	-1		0	4
	0.15 E. none	0	0	0		0	0	0		0	0	0		0	0	0		0	0	0		*	*	*	*	*		0	0	0	0		0	0	0		1	0	-1		2	0	-2		2	0	-2		0	6
7. PUC Security Capability	0.15 A. high: skilled	3	1	-3		-1	0	1		-1	0	1		0	0	0		0	0	0		1	0	0	0	-1		*	*	*	*		2	0	-2		2	0	-2		0	0	0		1	0	-1		1	15
	0.40 B. medium: competent	1	1	-1		0	0	0		0	0	0		0	0	0		0	0	0		0	0	0	0	0		*	*	*	*		1	0	-1		1	0	-1		0	0	0		0	0	0		1	7
	0.35 C. low: struggle	-1	-1	1		0	0	0		0	0	0		0	0	0		0	0	0		0	0	0	0	0		*	*	*	*		-1	0	1		-1	0	1		0	0	0		0	0	0		-1	7
	0.10 D. none	-3	-1	3		1	0	-1		1	0	-1		0	0	0		0	0	0		-1	0	0	0	1		*	*	*	*		-2	0	2		-2	0	2		0	0	0		-1	0	1		-1	15

Descriptor (Driven)	Alternative Descriptor States	1. Role of State PUC				2. Responsibility for Information Mgt.				3. Responsibility for Coordination / Communication				4. Responsibility for Cost Recovery				5. Public Perception of Threat				6. Level of Attacks						7. PUC Security Capability					8. PUC Role in Restoration Priorities				9. Information Sharing				10. Responsibility for Asset Protection				11. Standards for Utility Security					
	Descriptor (Driver)	0.15 A. broad	0.55 B. medium	0.30 C. limited		0.35 A. strong Fed	0.55 B. mostly shared	0.10 C. mostly state		0.35 A. federal	0.55 B. shared fed/st	0.10 C. state/local/priv		0.20 A. tax payers	0.50 B. shareholders	0.30 C. customers		0.20 A. high, engaged	0.45 B. moderate	0.35 C. low		0.05 A. high #, hi cons	0.25 B. low #, hi cons	0.10 C. high #, lo cons	0.45 D. low #, lo cons	0.15 E. none		0.15 A. high: skilled	0.40 B. medium	0.35 C. low: struggle	0.10 D. none		0.30 A. high	0.20 B. shared feds	0.50 C. low (utility)		0.10 A. high	0.30 B. variable	0.60 C. low		0.15 A. mostly Fed	0.05 B. mostly state	0.80 C. mostly utility		0.20 A. high	0.60 B. medium	0.20 C. low		Sum of Values	Non-Zero Entries
8. PUC Role in Restoration Priorities	0.30 A. high	2	0	-2		-1	0	1		0	0	0		0	0	0		0	0	0		-1	0	0	0	1		3	1	-1	-3		*	*	*		1	0	-1		0	0	0		0	0	0		0	12
	0.20 B. shared with feds	1	1	-1		0	0	0		0	0	0		0	0	0		0	0	0		0	0	0	0	0		1	1	-1	-1		*	*	*		0	0	0		0	0	0		0	0	0		1	7
	0.50 C. low (utility driven)	-2	0	2		1	0	-1		0	0	0		0	0	0		0	0	0		1	0	0	0	-1		-3	-1	1	3		*	*	*		-1	0	1		0	0	0		0	0	0		0	12
9. Information Sharing	0.10 A. high cooperation	0	0	0		3	1	-3		2	0	-2		0	0	0		2	0	-2		3	1	0	-1	-3		2	0	0	-2		1	0	-1		*	*	*		2	0	-2		1	0	-1		1	19
	0.30 B. variable, developing	0	0	0		1	1	-1		1	1	-1		0	0	0		1	1	-1		1	1	0	-1	-1		1	0	0	-1		0	0	0		*	*	*		1	1	-1		0	0	0		4	18
	0.60 C. low, not implemented	0	0	0		-3	-1	3		-2	0	2		0	0	0		-2	0	2		-3	-1	0	1	3		-2	0	0	2		-1	0	1		*	*	*		-2	0	2		-1	0	1		-1	19
10. Responsibility for Asset Protection	0.15 A. mostly Fed	-2	0	2		2	0	-2		0	0	0		2	0	-2		2	0	-2		2	0	0	0	-2		-1	0	0	1		0	0	0		0	0	0		*	*	*		1	0	-1		0	14
	0.05 B. mostly state/local	-1	1	1		1	1	-1		0	0	0		1	1	-1		1	1	-1		1	0	0	0	-1		0	0	0	0		0	0	0		0	0	0		*	*	*		0	0	0		4	14
	0.80 C. mostly utility	2	0	-2		-2	0	2		0	0	0		-2	0	2		-2	0	2		-2	0	0	0	2		1	0	0	-1		0	0	0		0	0	0		*	*	*		-1	0	1		0	14
11. Standards for Utility Security	0.20 A. high	3	1	-3		2	0	-2		2	0	-2		2	0	-2		2	0	-2		3	1	0	-1	-3		3	1	-1	-3		0	0	0		3	1	-3		3	1	-3		*	*	*		3	25
	0.60 B. medium	1	1	-1		1	1	-1		1	1	-1		1	1	-1		1	1	-1		1	1	0	-1	-1		1	1	-1	-1		0	0	0		1	1	-1		1	1	-1		*	*	*		7	29
	0.20 C. low	-3	-1	3		-2	0	2		-2	0	2		-2	0	2		-2	0	2		-3	-1	0	1	3		-3	-1	1	3		0	0	0		-3	-1	3		-3	-1	3		*	*	*		-3	25
	Sum of Values	0	4	0		3	5	-3		2	4	-2		4	4	-4		5	5	-5		7	5	0	-5	-7		4	3	-3	-4		1	1	-1		4	4	-4		4	6	-4		0	2	0			
	Non-Zero Entries	16	10	16		19	9	19		16	8	16		12	6	12		17	9	17		27	15	0	15	27		16	9	9	16		11	3	11		20	6	20		22	12	22		16	2	16			

Appendix E

Analysis of "Driver" and "Driven" Descriptors

The tables below describe the overall impact of descriptors on each other according to the results presented in Appendix D. A descriptor that ranks highly on the list of "drivers" has a strong effect on the other descriptors. Similarly, a descriptor that ranks highly on the list of "drivens" is strongly affected by the other descriptors.

The rankings in these tables are the result of two scores compiled from the descriptor cross-impact matrix in Appendix D. The average interaction score is a measure of the number of non-zero entries in the matrix, summed for each state of a given descriptor, then averaged across the alternate states of that descriptor. The average intensity score is the absolute value of the entries in the matrix, summed for each state of a given descriptor and then averaged across the alternate states of that descriptor.

Driver Descriptors	Average Interaction	Average Intensity
1. Responsibility for Key Asset Protection/Mitigation	19	32
2. Level of Terrorist Attacks on Utility Infrastructure	17	26
3. Allocation of Responsibility for Information Management	16	25
4. Information Sharing Protocols and Willingness to Share Information	15	23
5. Role of State Public Utility Commissions	14	23
6. Public Perception of Threat/Vulnerability	14	24
7. Allocation of Responsibility for Coordination and Communication	13	21
8. PUC Security Capabilities	13	20
9. Standards for Utility Security	11	15
10. Allocation of Responsibilities for Cost Recovery (Who Pays)	10	17
11. PUC Role in Restoration Priorities	8	12

Driven Descriptors	Average Interaction	Average Intensity
1. Standards for Utility Security	26	45
2. Allocation of Responsibility for Information Management	21	37
3. Role of State Public Utility Commissions	21	34
4. Allocation of Responsibility for Coordination and Communication	20	34
5. Information Sharing Protocols and Willingness to Share Information	19	29
6. Responsibility for Key Asset Protection/Mitigation	14	21
7. PUC Security Capabilities	11	15
8. PUC Role in Restoration Priorities	10	14
9. Allocation of Responsibilities for Cost Recovery (Who Pays)	8	12
10. Public Perception of Threat/Vulnerability	5	8
11. Level of Terrorist Attacks on Utility	4	6

Appendix F

IFS Generated Scenarios

Battelle Memorial Institute's proprietary IFS™ software adjusts all *a priori* probabilities up and down to 1.0 (occurs) or 0 (does not occur) to create posterior probabilities, and it then groups all occurring descriptor states into scenario groups. The larger the grouping of scenarios, the more likely is that type of scenario to take place.

Scenario Type	1	2	3	4	5	6	7	8	9	10	11	*A Priori* Probability	Total Occur-rences	Posterior Probability
Frequency	**12**	**11**	**3**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**			
1. Role of State PUCs														
A. broad	0	0	0	0	0	1	0	0	0	0	0	0.15	6	0.08
B. medium	0	0	1	1	0	0	0	0	0	1	1	0.55	17	0.24
C. limited	1	1	0	0	1	0	1	1	1	0	0	0.30	49	0.68
2. Allocation of Responsibility for Information Management														
A. strong Federal leadership, regulation, and direction	0	0	0	0	0	0	0	1	0	0	0	0.35	6	0.08
B. mostly shared Fed and state roles	1	1	0	0	1	0	1	0	1	0	0	0.55	41	0.57
C. mostly states, local, and utility initiatives	0	0	1	1	0	1	0	0	0	1	1	0.10	25	0.35
3. Allocation of Responsibility for Coordination and Communication														
A. primarily Federal (top-down)	0	0	0	0	0	0	1	0	0	0	0	0.35	6	0.08
B. primarily shared between Fed and state governments	1	1	0	0	1	0	0	1	1	0	0	0.55	40	0.56
C. primarily driven by states, locales and private sector	0	0	1	1	0	1	0	0	0	1	1	0.10	26	0.36
4. Allocation of Responsibility for Cost Recovery (Who pays)														
A. primarily tax payers (Fed, State, and local taxes)	0	0	0	0	0	0	0	0	0	0	0	0.20	5	0.07
B. primarily rate payers/customers	1	1	0	1	1	0	1	1	1	1	1	0.50	55	0.76
C. primarily shareholders	0	0	1	0	0	1	0	0	0	0	0	0.30	12	0.17

Scenario Type	1	2	3	4	5	6	7	8	9	10	11	*A Priori* Probability	Total Occur-rences	Posterior Probability
Frequency	**12**	**11**	**3**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**			
5. Public Perception of Threat/Vulnerability														
A. high, engaged	0	0	0	0	0	0	0	0	0	0	0	0.20	3	0.04
B. moderate	0	0	1	1	1	1	0	0	0	0	1	0.45	31	0.43
C. low	1	1	0	0	0	0	1	1	1	1	0	0.35	38	0.53
6. Level of Terrorist Attacks on Infrastructure														
A. high number, high consequence	0	0	0	0	0	0	0	0	0	0	0	0.05	5	0.07
B. low number, high consequence	0	0	1	1	1	1	0	0	0	0	1	0.25	24	0.33
C. high number, low consequence	0	0	0	0	0	0	0	0	0	0	0	0.10	1	0.01
D. low number, low consequence	1	1	0	0	0	0	1	1	1	1	0	0.45	41	0.57
E. none	0	0	0	0	0	0	0	0	0	0	0	0.15	1	0.01
7. PUC Security Capabilities														
A. high: skilled, robust, sustainable	0	0	0	0	0	1	0	0	0	0	0	0.15	6	0.08
B. medium: basically competent	0	0	0	1	0	0	0	0	0	0	0	0.40	5	0.07
C. low: struggle	0	0	1	0	0	0	0	0	0	0	0	0.35	11	0.15
D. none	1	1	0	0	1	0	1	1	1	1	1	0.10	50	0.69
8. PUC Role in Restoration														
A. high, mostly responsible	0	0	0	1	0	1	0	0	0	0	0	0.30	12	0.17
B. shared with Feds	0	0	0	0	0	0	0	0	0	0	0	0.20	1	0.01
C. low (utility driven)	1	1	1	0	1	0	1	1	1	1	1	0.50	59	0.82
9. Information Sharing Protocols and Willingness to Share Information														
A. protocols exist, high willingness/cooperation	0	0	0	0	0	0	0	0	0	0	0	0.10	3	0.04
B. variable, developing	0	0	0	0	0	0	0	0	0	0	0	0.30	3	0.04
C. low, poorly implemented	1	1	1	1	1	1	1	1	1	1	1	0.60	66	0.92
10. Responsibility for Key Asset Protection/Mitigation														
A. mostly Federal	1	1	0	0	0	0	1	1	0	0	0	0.15	38	0.53
B. mostly state and local	0	0	0	0	0	0	0	0	0	0	0	0.05	1	0.01
C. mostly utilities	0	0	1	1	1	1	0	0	1	1	1	0.80	33	0.46

Scenario Type	1	2	3	4	5	6	7	8	9	10	11	*A Priori* Probability	Total Occur-rences	Posterior Probability
Frequency	**12**	**11**	**3**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**			
11. Standards for Utility Security														
A. high	0	0	0	0	0	0	0	0	0	0	0	0.20	2	0.03
B. medium	1	0	1	0	0	1	1	1	0	0	0	0.60	32	0.44
C. low	0	1	0	1	1	0	0	0	1	1	1	0.20	38	0.53

Appendix G

Oklahoma Corporation Commission's Notice of Inquiry into Critical Infrastructure Protection Guidelines

BEFORE THE CORPORATION COMMISSION OF THE STATE OF OKLAHOMA

IN RE: INQUIRY OF THE OKLAHOMA CORPORATION COMMISSION INTO GUIDELINES FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE AND KEY ASSETS	)))))	CAUSE NO. PUD 200300624

1) NOTICE OF INQUIRY

Article II. INTRODUCTION

Since September 11, 2001, the role of public utility commissions in protecting critical infrastructure and key assets has undergone reevaluation. During the same time period, public service companies have reexamined their need to enhance existing security precautions and incur additional costs for security purposes. The purpose of this Notice of Inquiry (NOI) by the Oklahoma Corporation Commission (the "Commission") is to consider the issues related to the role of public utility commissions and regulated companies in addressing the security of critical infrastructure.

Article III. ISSUES PROPOSED FOR COMMENT

The Commission requests that interested parties provide comments on the following topics, and include a discussion explaining their response:

a) Confidentiality

1) Please comment on whether the Oklahoma statutes are sufficient to offer protection from disclosure for security-sensitive documents and discussions under state and federal disclosure and open meetings acts.

2) If the statutes are sufficient, are there additional rules that the Commission should adopt to provide adequate protection for security-sensitive documents and discussions?

3) If the statutes are insufficient, please provide proposed legislative language that would adequately protect security-sensitive documents and discussions.

4) Please comment on any allocation of responsibility for information management relevant to protecting critical infrastructure.

5) Please comment on any allocation of responsibility for coordination and communication relevant to protecting critical infrastructure.

6) Please comment on any public utility commission security capabilities.

7) Please comment on information sharing protocols and willingness to share information.

b) Cost Recovery Proceedings

1) Please comment on whether the Commission rules of practice are adequate to address security concerns in the context of protective orders.

2) Please comment on whether the Commission rules of practice are adequate to address security concerns in the context of intervention by third parties.

3) Please comment on whether the Commission rules of practice are adequate to address security concerns in the context of discovery by the parties in a cause.

4) Please comment on whether the Commission rules of practice regarding notice and hearings are adequate for cost recovery proceedings.

c) Security Measures

1) Please discuss the advisability of adopting specific standards (i.e. uniform requirements based on widely used practices) as opposed to guidelines (outlines of policies or conduct) designed to achieve security objectives. An example of "specific standards" could be rules in the nature of pipeline safety regulations (49 CFR §192, et seq.), while an example of "guidelines" could be more like the NERC physical security guidelines.

2) If specific standards are advisable, please comment on the specific standards that should be adopted to protect critical infrastructure (standards for utility security, both physical and cyber).

3) If guidelines are advisable, please comment on the guidelines that should be adopted to protect critical infrastructure.

4) Please comment on the advisability of requiring jurisdictional companies to conduct vulnerability assessments.

5) Please comment on the advisability of requiring jurisdictional companies to have a written security plan.

6) Please comment on whether the Commission should have full access to the results of vulnerability assessments. If the Commission should not have full access, please explain how the Commission should determine whether proposed security expenditures would be prudent.

7) Please comment on whether the Commission should have "security clearance" prior to having access to certain confidential data.

8) Please comment on methods for Commission staff to obtain the services of qualified security consultants and methods to pay for their services.

9) Please comment on any public utility commission role in restoration priorities.

10) Please comment on responsibility for key asset protection and mitigation.

11) Please comment on the cost impact of the Department of Homeland Security's color-based threat advisories or any required or voluntary actions made in response to a federal agency.

12) Please comment on the advisability of the Commission having a written security oversight plan.

d) Reasonableness of Costs

1) Please comment on any guidelines, indices, or other readily available authorities that the Commission should consider in determining the reasonableness of proposed security costs.

2) Please comment on the advisability of requiring utilities to use a bidding process for obtaining materials and services for security projects.

3) Please comment on any concerns related to inspections of facilities and audits of security costs.

4) Please comment on any cost recovery distinction between security measures undertaken by virtue of your fiduciary responsibilities and those taken in response to governmental mandates.

(ii) Collection of Security Costs

1) Please comment on recommended collection and reporting methods for security costs.

2) Please comment on any rate design issues unique to the recovery of security costs.

3) Please comment on the accounting treatment of specific security costs.

Commission Monitoring of Security

1) Please comment on whether the Commission should monitor the physical and cyber security of jurisdictional utilities.

2) Please comment on any procedural steps the Commission should employ to monitor the security arrangements of jurisdictional utilities.

3) Please comment on the types and timing of technical analysis the Commission should perform and/or data the Commission should collect regarding the physical and cyber security of jurisdictional companies.

Furthermore, the Commission requests that all interested parties provide input on any other pertinent concerns related to the hedging issues being considered in this Notice of Inquiry.

Article IV. TECHNICAL CONFERENCES AND COMMENTS

The Commission Staff will conduct informal technical conferences in Commission Courtroom 301, from 9:30 a.m. to 12:30 p.m. as per the following tentative schedule:

Nov.14, 2003	Electric Companies	Comments due
Nov.21, 2003	Gas Companies	Comments due
Dec. 5, 2003	Telephone Companies	Comments due
Dec.12, 2003	Water Companies	Comments due
Jan. 8, 2004	Electric Companies	1st Tech Conference
Jan. 15, 2004	Gas Companies	1st Tech Conference
Jan. 22, 2004	Telephone Companies	1st Tech Conference
Jan. 29, 2004	Water Companies	1st Tech Conference
Feb. 5, 2004	Electric Companies	2nd Tech Conference
Feb. 12, 2004	Gas Companies	2nd Tech Conference
Feb. 19, 2004	Telephone Companies	2nd Tech Conference
Feb. 26, 2004	Water Companies	2nd Tech Conference
Mar. 4, 2004	Deliberations by Commission	

Interested persons are invited to submit written comments and to attend the technical conferences to the fullest extent possible. The purpose of the technical conferences will be to receive pertinent training and to discuss issues and reply comments received by the Commission in response to this Notice of Inquiry.

For further information, contact Ken Zimmerman, 500 Jim Thorpe Building, 2101 North Lincoln Boulevard, Oklahoma City, OK 73105, (405) 522-3364 or Michele Craig, Assistant General Counsel, 400 Jim Thorpe Building, 2101 North Lincoln Boulevard, Oklahoma City, OK 73105, (405) 521-2259.

(a) OKLAHOMA CORPORATION COMMISSION

_____
DENISE A. BODE, Chairman

_____
BOB ANTHONY, Vice Chairman

_____
JEFF CLOUD, Commissioner

DONE AND PERFORMED this _____ day of October, 2003.
BY ORDER OF THE COMMISSION:

_____
PEGGY MITCHELL, Secretary

Appendix H

Oklahoma Corporation Commission's Proposed Electric Utility Rules

BEFORE THE CORPORATION COMMISSION OF THE STATE OF OKLAHOMA

IN THE MATTER OF A RULEMAKING OF THE OKLAHOMA CORPORATION COMMISSION AMENDING OAC 165:35, ELECTRIC UTILITY RULES	))))	CAUSE NO. RM 200400011

CHAPTER 35. ELECTRIC UTILITY RULES
(Critical Infrastructure Security Rules)

SUBCHAPTER 33

FINAL PROPOSED RULE

December 9, 2004

SUBCHAPTER 33. HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE

Section
165:35-33-1. Purpose and Scope
165:35-33-2. [RESERVED]
165:35-33-3. Definitions
165:35-33-4. [RESERVED]
165:35-33-5. Utility Security Plan
165:35-33-6. [RESERVED]
165:35-33-7. Reporting Requirements
165:35-33-8. [RESERVED]
165:35-33-9. Cost Recovery
165:35-33-10. Commission Authorized Participation
165:35-33-11. Confidentiality

165:35-33-1. Purpose and Scope

(a) The purpose of this Subchapter is to encourage utilities to take all reasonable measures necessary to protect their critical infrastructures from extended interruption of service from all extraordinary events, natural and man-made.

(b) The Corporation Commission encourages electric utilities to develop, implement, and maintain Homeland Security and Critical Infrastructure Plans according to the industry standards enumerated in sub-section (d) below.

(c) To the extent that a utility seeks to recover costs for security measures outside of a general rate review for the implementation of Homeland Security and/or Critical Infrastructure protections, the utility shall comply with all provisions of this Subchapter.

(d) Each electric utility serving Oklahoma jurisdictional ratepayers is encouraged to follow the most current North American Electric Reliability Council's (NERC's) Security Guidelines and Standards, as may be amended from time to time, for use as guidelines for protecting the utility's Critical Infrastructure from extended service interruption.

(e) Each electric utility seeking to recover costs for security measures from Oklahoma jurisdictional ratepayers outside of a general rate review shall develop, implement, and maintain a Critical Infrastructure and Security Plan as further set forth within this Subchapter.

(f) If the utility has implemented a Security Plan or process in accordance with the applicable industry guidelines but is not seeking or receiving cost recovery for security-related costs, the utility shall submit the Certification Letter required by OAC 165:35-33-7(f) and the Plan shall be subject to review pursuant to the Authorized Participation and Confidentiality provisions of OAC 165:35-33-10 and OAC 165:35-33-11. The utility is not otherwise required to comply with the provisions of this Subchapter.

(g) The Commission retains its jurisdictional and supervisory authority to address the reasonableness and/or prudence of any proposed security cost recovery.

(h) Nothing in this subchapter shall relieve any utility from any duty otherwise prescribed by the laws of the State of Oklahoma or this Commission's rules.

(i) Nothing in this Subchapter is intended to divest the utility of its right to object to any discovery requests from intervenors seeking access to "Highly Sensitive Confidential" materials.
(j) If any provision of this Subchapter is held invalid, such invalidity shall not affect other provisions or applications of this Subchapter which can be given effect without the invalid provision or application, and to this end, the provisions of this Subchapter are declared to be severable.

165:35-33-2. [RESERVED]

165:35-33-3. Definitions
The following words and terms, when used in this Subchapter 33, shall have the following meaning, unless the context clearly indicates otherwise:

"Annual Report" means the Annual Report submitted by Commission Staff to the Commission beginning December 30, 2005 and by July 1 of each year thereafter, summarizing the results of Staff's review of each utility's Security Plan (and any Plan Update Reports), along with any recommendations that Staff may have regarding such Plan(s).

"Authorized Participant" means those persons authorized by the utility or as may otherwise be authorized by law and/or ordered by the Commission, to view highly sensitive confidential information. Such authorization shall be granted on a case-by-case basis and may extend to the utility, state government officials, persons having been granted intervenor status by the Commission and Commission authorized designees of the parties.

"Certification Letter" means the written certification to the Director of the Public Utility Division made by August 1, 2005 and on March 1 of each subsequent year thereafter, indicating that as of the date of the Certification Letter, the utility has a Plan or that it has updated the Plan and/or previous Plan Update Reports, has a Plan but is not seeking cost recovery or has no Plan in place.

"Critical Infrastructure" means the property of a utility located in the State of Oklahoma, comprised of either physical assets or computer software which, if severely damaged or destroyed, would have a significant impact on the ability of the utility to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

"Highly Sensitive Confidential" means that the information is of such a sensitive nature that its public disclosure could be harmful to the security of a utility's critical infrastructure and as such it may only be viewed by those persons authorized by the utility or as may otherwise be ordered by the Commission.

"NERC" means the North American Electric Reliability Council.

"Plan" means a Homeland Security and Critical Infrastructure Plan including any subsequent Plan Update Reports that have been prepared with reference to the NERC

GUIDELINES.

"Plan Update Report" means the written redlined changes made by the utility updating the Plan and/or previous Plan Update Reports. At the utility's option, changes will either be redlined or a history of changes may be maintained.

"Security Cost Rider" means the per billing unit rate mechanism whereby a utility may, upon approval and Order of this Commission, recover the costs of providing security for its Critical Infrastructure as defined under this Subchapter 33.

165:35-33-4. [RESERVED]

165:35-33-5. Utility Security Plan

(a) Each electric utility is encouraged to prepare and make available for inspection, a "Homeland Security and Critical Infrastructure Plan" ("Plan") that has been prepared with reference to the NERC Security Guidelines and Standards.

(b) The Plan shall be marked as "Highly Sensitive Confidential" and designate those facilities that the utility considers to be Critical Infrastructure (physical assets and computer software as defined in OAC 165:35-33-3 above), and shall set forth the utility's measures to secure such facilities from extended service interruption. The Plan shall also include an estimate of the costs necessary to achieve such measures.

(c) The Plan shall remain on site at the utility's business office in accordance with OAC 165:35-33-7(g) below and shall have the most current version of the redlined Plan Update Report attached to the clean version of the utility's latest Plan. At the utility's option, changes will either be redlined or a history of changes may be maintained.

(d) The Plan shall list all locations deemed by the utility to be critical, as well as identification of any subsequently increased security measures. All locations and security measures shall be identified by code known only to the utility and designated state government officials and their designees.

(e) Any subsequent security measures identified in the Plan shall contain an estimate of the cost necessary to implement such measures, a description of the measures necessary to adequately secure each specific location and an estimated schedule for completion of each measure.

(f) All locations identified by the Plan that require additional security measures shall be prioritized by the utility.

(g) Beginning December 30, 2005 and on July 1 of each year thereafter, Commission Staff shall submit an Annual Report marked as "Highly Sensitive Confidential" to the Commission, summarizing the results of Staff's review of a utility's Plan (and any Plan Update Reports), along with any recommendations that Staff may have regarding such Plan(s).

(h) Beginning December 30, 2005, where the Attorney General elects to submit recommendations to the Commission regarding a utility's Plan, such recommendations shall be marked as "Highly Sensitive Confidential" and shall also be due by July 1 of each subsequent year thereafter.

165:35-33-6. [RESERVED]

165:35-33-7. Reporting requirements

(a) Subsequent to the preparation of the initial Plan prepared under OAC 165:35-33-5(a), each utility shall prepare a Plan Update Report by March 1 of each succeeding year, following the same format as the initial Plan with redlines of all new changes, marked "Highly Sensitive Confidential" and kept on site at the utility's business office.

(b) Each subsequent Plan Update Report shall update the previous year's report by indicating for each specific coded location, all costs and completion dates (actual and projected) for all current and prior additional security measures claimed under this Subchapter.

(c) For those security measures previously reported that have not yet been completed, revised estimated costs and estimated completion dates shall be provided.

(d) The Plan Update Report shall also include (by specific coded location) a description of each proposed security measure that has not been previously reported, the estimated costs for each, as well as the estimated completion date for each measure.

(e) Costs reflected in the initial Plan and in subsequent Plan Update Reports, whether estimated or actual, shall be identified as either capital or expense costs.

(f) Beginning August 1, 2005 and by March 1 of every year thereafter, each utility shall submit a Certification Letter to the Director of the Public Utility Division, marked as "Highly Sensitive Confidential" and certifying that as of the date of the Certification Letter:

(1) The utility does not have a Homeland Security and Critical Infrastructure Plan as contemplated and defined by this Subchapter;

(2) The utility does not have a Homeland Security and Critical Infrastructure Plan as contemplated or defined by this Subchapter but has otherwise taken steps to secure Critical Infrastructure and is not seeking cost recovery under this Subchapter;

(3) The utility does have a Plan but is not seeking cost recovery; or

(4) The utility has a Plan and/or has prepared its Plan Update Report updating the Plan and/or previous year's Plan Update Report;

(A) The redlines contained within the current Plan Update Report encompass in the entirety, all of the changes made to the utility's Plan since the Plan's inception or the previous year's certification; and

(B) The Plan is available for Commission and/or Attorney General review at the utility's local place of business.

(g) A utility shall not be required to file its initial Plan or any of its subsequent Plan Update Reports with the Commission. Each utility shall instead, secure and maintain on site, at the utility's local place of business, its initial Plan and all subsequent Plan Update Reports.

165:35-33-8. [RESERVED]

165:35-33-9. Cost recovery

(a) Each utility seeking cost recovery of expenditures outside of a general rate review related to securing its Critical Infrastructure shall prepare and make available for inspection, its Plan and any subsequent Plan Update Reports in accordance with this Subchapter.

(b) A utility shall file an application with the Commission for cost recovery as provided for within this Subchapter. Such cost recovery shall only occur to the extent the utility has incurred all or a portion of its actual security-related costs.

(c) Unless otherwise ordered by the Commission, the utility shall have the burden of proving compliance with all of the provisions of this Subchapter prior to obtaining any cost recovery for security related measures.

(d) Upon approval and Order of the Commission, a utility shall be allowed to recover a return based on its weighted cost of long-term debt and equity on all capital expenditures made for security measures. The utility shall also be allowed to recover related depreciation expense and ad valorem taxes. Such recoveries shall be based upon similar ratemaking treatment for corresponding cost elements from the utility's most recent general rate case.

(e) Upon approval and Order of the Commission, a utility shall be allowed to recover expenses typically classified as operations and maintenance expenses for ratemaking purposes. The utility may request inclusion of any such similar costs incurred as long as these costs are directly associated with the security measures taken.

(f) The total costs incurred under this Subchapter shall be combined for recovery purposes, for consideration by the Commission.

(g) All costs approved by the Commission for recovery, shall be recovered from the utility's customers through a "Security Cost Rider" based on the projected annual billing units for the utility and shall be subject to annual true-up.

(h) Unless otherwise ordered by the Commission, a utility shall immediately discontinue recovery of the "Security Cost Rider" when the earlier of the following occurs: natural expiration due to the full recovery provided for in a Rider granted under this Subchapter or forced expiration required pursuant to OAC 165:35-33-9(i) and/or OAC 165:35-33-9(j). Under no circumstances, shall the utility be permitted to double recover Homeland Security and Critical Infrastructure related costs.

(i) Unless otherwise ordered by the Commission, any utility with a "Security Cost Rider" currently in effect, that files for a general rate change, shall include in the rate case, all security-related costs and those costs shall be accorded standard ratemaking treatment. A utility shall discontinue its "Security Cost Rider" when the change in rates becomes effective upon Final Order in the rate case.

(j) Unless otherwise ordered by the Commission, all "Security Cost Riders" approved by the Commission, shall expire five years from the initial date of the "Security Cost Rider's" implementation.

(k) Upon the filing of a cost recovery request by a utility, Commission Staff, the state Attorney General's office (based upon that entity's statutory authority) and all other Authorized Participants shall review the cost recovery proposal submitted by the utility and file testimony in accordance with:

(1) Any applicable protective orders issued by the Commission in the security-related cost recovery cause;

(2) OAC 165:35-33-11 (below);
(3) The Commission's Rules of Practice (OAC 165:5); and
(4) Any other protective measures or requirements prescribed by law or the Commission.

(l) Testimony of Commission Staff, the state Attorney General and all other Authorized Participants, shall detail each of the parties' respective recommendations and any objections to the utility's Plan and the utility's request for cost recovery related to the Plan. Also in accordance with the Commission's Rules of Practice, Commission Staff, the state Attorney General and all other Authorized Participants shall provide copies of their respective individual testimonies to one another, with redacted versions of each individual testimony filed with the Court Clerk at the Commission.

(m) Upon notice and hearing, the Commission shall issue an Order regarding any requests for security-related cost recovery.

165:35-33-10. Commission Authorized Participation

(a) **Commission Staff.** Only those Commission Staff and Staff's designees authorized by the Commission shall participate in a cause before the Commission regarding a utility's Plan and then, shall do so only after meeting all applicable requirements for Commission authorization, which shall be determined on a case-by-case basis. All Commission Staff and Staff's designees authorized to participate in a security cause shall comply with the requirements for protecting information obtained under the "Highly Sensitive Confidential" designation.

(b) **Attorney General.** Only those Attorney General personnel who have formally entered an appearance pursuant to Oklahoma Statute and the Commission's Rules of Practice and that entity's Commission authorized designees shall be granted review of a utility's Plan and/or Plan Update Reports. All Attorney General personnel and their designees authorized to participate in a security cause shall meet all applicable requirements for Commission authorization, to be determined on a case-by-case basis, and shall comply with the protections afforded information obtained under the "Highly Sensitive Confidential" designation.

(c) **Intervenors.**

(1) For the purposes of this Subchapter, all intervenors, including but not limited to counsel and experts for intervenors, shall be deemed "Authorized Participants" in accordance with OAC 165:35-33-3 above. All Authorized Participants wishing to participate in a security-related cause before the Commission shall meet all applicable requirements for Commission authorization, which shall be determined on a case-by-case basis, and shall comply with the protections afforded information obtained under the "Highly Sensitive Confidential" designation.

(2) In addition to acquiring "Authorized Participant" status from the Commission, each intervenor and its designees desiring to participate in a cause before the Commission regarding a utility's Plan shall post a bond or other security acceptable to the Commission, in an amount to be determined by the Commission, to protect the utility from harm in the event the Authorized Participant breaches the confidentiality terms established under this Subchapter or as may otherwise be

established by the Commission. A copy of such bond or other security shall be filed with the Commission's Court Clerk. This subsection shall not apply to the Attorney General of the State of Oklahoma or the Oklahoma Corporation Commission Commissioners and Staff.
(3) Any Authorized Participant found in violation of a Commission issued Protective Order and Proprietary Agreement, shall be liable for contempt penalties pursuant to the penalty provisions found in Article IX, § 19 of the Oklahoma Constitution, Title 17 of the Oklahoma Statutes and the Commission's Rules of Practice at OAC 165:5. This subsection shall not apply to the Attorney General of the State of Oklahoma or the Oklahoma Corporation Commission Commissioners and Staff.
(4) In addition to the above protections, all Authorized Participants may be required by the Commission to enter into a separate non-disclosure agreement as a pre-requisite to being granted intervention and "Authorized Participant" status.

165:35-33-11. Confidentiality

(a) Pursuant to the Commission's jurisdiction granted under Article IX, Section 18 of the Oklahoma Constitution, 51 O.S. (2001) §24A.22 of the Oklahoma Statutes and OAC 165:5, the Commission's Rules of Practice; all un-redacted documents related to a utility's Homeland Security and Critical Infrastructure Plan shall be considered "Highly Sensitive and Confidential" and shall only be admitted into evidence in en camera proceedings.
(b) "Highly Sensitive Confidential" designation and protection shall extend but not be limited to the following: initial Plans (including underlying documents), Plan Update Reports, Certification Letters, Annual Reports made by Commission Staff, recommendations submitted by the Attorney General of the State of Oklahoma and un-redacted documents used in cost recovery proceedings. For all other documents, the "Highly Sensitive Confidential" designation may be granted upon hearing and Final Order of the Commission.
(c) Each utility's Plan and/or Plan Update Report prepared in accordance with this Subchapter, shall be marked "Highly Sensitive Confidential" and shall be kept and maintained on site at the utility's business office in accordance with OAC 165:35-33-7(g), above. Only those individuals on the Staff of the Corporation Commission and in the State Attorney General's office and their respective experts who have been authorized by the Commission, shall have access to the Plan and Plan Update Reports prepared by each utility and any related or supporting documentation thereto. All other parties granted authorized intervenor status to a security cause pursuant to OAC 165:35-33-10(c) may also have access to the Plan, Plan Update Reports and supporting documentation after notice and hearing.

Appendix I

Oklahoma Corporation Commission's Proposed Gas Utility Rules

BEFORE THE CORPORATION COMMISSION OF THE STATE OF OKLAHOMA

IN THE MATTER OF A RULEMAKING OF THE OKLAHOMA CORPORATION COMMISSION AMENDING OAC 165:45, GAS UTILITY RULES	))))	CAUSE NO. RM 200400012

CHAPTER 45. GAS SERVICE UTILITY RULES

(Critical Infrastructure Security Rules)

SUBCHAPTER 21

FINAL PROPOSED RULE

December 9, 2004

SUBCHAPTER 21. HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE

Section
165:45-21-1. Purpose and Scope
165:45-21-2. [RESERVED]
165:45-21-3. Definitions
165:45-21-4. [RESERVED]
165:45-21-5. Utility Security Plan
165:45-21-6. [RESERVED]
165:45-21-7. Reporting Requirements
165:45-21-8. [RESERVED]
165:45-21-9. Cost Recovery
165:45-21-10. Commission Authorized Participation
165:45-21-11. Confidentiality

165:45-21-1. Purpose and Scope

(a) The purpose of this Subchapter is to encourage utilities to take all reasonable measures necessary to protect their critical infrastructures from extended interruption of service from all extraordinary events, natural and man-made.

(b) The Corporation Commission encourages electric utilities to develop, implement, and maintain Homeland Security and Critical Infrastructure Plans according to the industry standards enumerated in sub-section (d) below.

(c) To the extent that a utility seeks to recover costs for security measures outside of a general rate review for the implementation of Homeland Security and/or Critical Infrastructure protections, the utility shall comply with all provisions of this Subchapter.

(d) Each electric utility serving Oklahoma jurisdictional ratepayers is encouraged to follow the most current North American Electric Reliability Council's (NERC's) Security Guidelines and Standards, as may be amended from time to time, for use as guidelines for protecting the utility's Critical Infrastructure from extended service interruption.

(e) Each electric utility seeking to recover costs for security measures from Oklahoma jurisdictional ratepayers outside of a general rate review shall develop, implement, and maintain a Critical Infrastructure and Security Plan as further set forth within this Subchapter.

(f) If the utility has implemented a Security Plan or process in accordance with the applicable industry guidelines but is not seeking or receiving cost recovery for security-related costs, the utility shall submit the Certification Letter required by OAC 165:35-33-7(f) and the Plan shall be subject to review pursuant to the Authorized Participation and Confidentiality provisions of OAC 165:35-33-10 and OAC 165:35-33-11. The utility is not otherwise required to comply with the provisions of this Subchapter.

(g) The Commission retains its jurisdictional and supervisory authority to address the reasonableness and/or prudence of any proposed security cost recovery.

(h) Nothing in this subchapter shall relieve any utility from any duty otherwise prescribed

by the laws of the State of Oklahoma or this Commission's rules.
(i) Nothing in this Subchapter is intended to divest the utility of its right to object to any discovery requests from intervenors seeking access to "Highly Sensitive Confidential" materials.
(j) If any provision of this Subchapter is held invalid, such invalidity shall not affect other provisions or applications of this Subchapter which can be given effect without the invalid provision or application, and to this end, the provisions of this Subchapter are declared to be severable.

165:35-33-2. [RESERVED]

165:35-33-3. Definitions
The following words and terms, when used in this Subchapter 33, shall have the following meaning, unless the context clearly indicates otherwise:

"Annual Report" means the Annual Report submitted by Commission Staff to the Commission beginning December 30, 2005 and by July 1 of each year thereafter, summarizing the results of Staff's review of each utility's Security Plan (and any Plan Update Reports), along with any recommendations that Staff may have regarding such Plan(s).

"Authorized Participant" means those persons authorized by the utility or as may otherwise be authorized by law and/or ordered by the Commission, to view highly sensitive confidential information. Such authorization shall be granted on a case-by-case basis and may extend to the utility, state government officials, persons having been granted intervenor status by the Commission and Commission authorized designees of the parties.

"Certification Letter" means the written certification to the Director of the Public Utility Division made by August 1, 2005 and on March 1 of each subsequent year thereafter, indicating that as of the date of the Certification Letter, the utility has a Plan or that it has updated the Plan and/or previous Plan Update Reports, has a Plan but is not seeking cost recovery or has no Plan in place.

"Critical Infrastructure" means the property of a utility located in the State of Oklahoma, comprised of either physical assets or computer software which, if severely damaged or destroyed, would have a significant impact on the ability of the utility to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

"Highly Sensitive Confidential" means that the information is of such a sensitive nature that its public disclosure could be harmful to the security of a utility's critical infrastructure and as such it may only be viewed by those persons authorized by the utility or as may otherwise be ordered by the Commission.

"NERC" means the North American Electric Reliability Council.

"Plan" means a Homeland Security and Critical Infrastructure Plan including any

subsequent Plan Update Reports that have been prepared with reference to the NERC GUIDELINES.

"Plan Update Report" means the written redlined changes made by the utility updating the Plan and/or previous Plan Update Reports. At the utility's option, changes will either be redlined or a history of changes may be maintained.

"Security Cost Rider" means the per billing unit rate mechanism whereby a utility may, upon approval and Order of this Commission, recover the costs of providing security for its Critical Infrastructure as defined under this Subchapter 33.

165:35-33-4. [RESERVED]

165:35-33-5. Utility Security Plan

(a) Each electric utility is encouraged to prepare and make available for inspection, a "Homeland Security and Critical Infrastructure Plan" ("Plan") that has been prepared with reference to the NERC Security Guidelines and Standards.

(b) The Plan shall be marked as "Highly Sensitive Confidential" and designate those facilities that the utility considers to be Critical Infrastructure (physical assets and computer software as defined in OAC 165:35-33-3 above), and shall set forth the utility's measures to secure such facilities from extended service interruption. The Plan shall also include an estimate of the costs necessary to achieve such measures.

(c) The Plan shall remain on site at the utility's business office in accordance with OAC 165:35-33-7(g) below and shall have the most current version of the redlined Plan Update Report attached to the clean version of the utility's latest Plan. At the utility's option, changes will either be redlined or a history of changes may be maintained.

(d) The Plan shall list all locations deemed by the utility to be critical, as well as identification of any subsequently increased security measures. All locations and security measures shall be identified by code known only to the utility and designated state government officials and their designees.

(e) Any subsequent security measures identified in the Plan shall contain an estimate of the cost necessary to implement such measures, a description of the measures necessary to adequately secure each specific location and an estimated schedule for completion of each measure.

(f) All locations identified by the Plan that require additional security measures shall be prioritized by the utility.

(g) Beginning December 30, 2005 and on July 1 of each year thereafter, Commission Staff shall submit an Annual Report marked as "Highly Sensitive Confidential" to the Commission, summarizing the results of Staff's review of a utility's Plan (and any Plan Update Reports), along with any recommendations that Staff may have regarding such Plan(s).

(h) Beginning December 30, 2005, where the Attorney General elects to submit recommendations to the Commission regarding a utility's Plan, such recommendations shall be marked as "Highly Sensitive Confidential" and shall also be due by July 1 of

each subsequent year thereafter.

165:35-33-6. [RESERVED]

165:35-33-7. Reporting requirements

(a) Subsequent to the preparation of the initial Plan prepared under OAC 165:35-33-5(a), each utility shall prepare a Plan Update Report by March 1 of each succeeding year, following the same format as the initial Plan with redlines of all new changes, marked "Highly Sensitive Confidential" and kept on site at the utility's business office.

(b) Each subsequent Plan Update Report shall update the previous year's report by indicating for each specific coded location, all costs and completion dates (actual and projected) for all current and prior additional security measures claimed under this Subchapter.

(c) For those security measures previously reported that have not yet been completed, revised estimated costs and estimated completion dates shall be provided.

(d) The Plan Update Report shall also include (by specific coded location) a description of each proposed security measure that has not been previously reported, the estimated costs for each, as well as the estimated completion date for each measure.

(e) Costs reflected in the initial Plan and in subsequent Plan Update Reports, whether estimated or actual, shall be identified as either capital or expense costs.

(f) Beginning August 1, 2005 and by March 1 of every year thereafter, each utility shall submit a Certification Letter to the Director of the Public Utility Division, marked as "Highly Sensitive Confidential" and certifying that as of the date of the Certification Letter:

(1) The utility does not have a Homeland Security and Critical Infrastructure Plan as contemplated and defined by this Subchapter;

(2) The utility does not have a Homeland Security and Critical Infrastructure Plan as contemplated or defined by this Subchapter but has otherwise taken steps to secure Critical Infrastructure and is not seeking cost recovery under this Subchapter;

(3) The utility does have a Plan but is not seeking cost recovery; or

(4) The utility has a Plan and/or has prepared its Plan Update Report updating the Plan and/or previous year's Plan Update Report;

(A) The redlines contained within the current Plan Update Report encompass in the entirety, all of the changes made to the utility's Plan since the Plan's inception or the previous year's certification; and

(B) The Plan is available for Commission and/or Attorney General review at the utility's local place of business.

(g) A utility shall not be required to file its initial Plan or any of its subsequent Plan Update Reports with the Commission. Each utility shall instead, secure and maintain on site, at the utility's local place of business, its initial Plan and all subsequent Plan Update Reports.

165:35-33-8. [RESERVED]

165:35-33-9. Cost recovery

(a) Each utility seeking cost recovery of expenditures outside of a general rate review related to securing its Critical Infrastructure shall prepare and make available for inspection, its Plan and any subsequent Plan Update Reports in accordance with this Subchapter.

(b) A utility shall file an application with the Commission for cost recovery as provided for within this Subchapter. Such cost recovery shall only occur to the extent the utility has incurred all or a portion of its actual security-related costs.

(c) Unless otherwise ordered by the Commission, the utility shall have the burden of proving compliance with all of the provisions of this Subchapter prior to obtaining any cost recovery for security related measures.

(d) Upon approval and Order of the Commission, a utility shall be allowed to recover a return based on its weighted cost of long-term debt and equity on all capital expenditures made for security measures. The utility shall also be allowed to recover related depreciation expense and ad valorem taxes. Such recoveries shall be based upon similar ratemaking treatment for corresponding cost elements from the utility's most recent general rate case.

(e) Upon approval and Order of the Commission, a utility shall be allowed to recover expenses typically classified as operations and maintenance expenses for ratemaking purposes. The utility may request inclusion of any such similar costs incurred as long as these costs are directly associated with the security measures taken.

(f) The total costs incurred under this Subchapter shall be combined for recovery purposes, for consideration by the Commission.

(g) All costs approved by the Commission for recovery, shall be recovered from the utility's customers through a "Security Cost Rider" based on the projected annual billing units for the utility and shall be subject to annual true-up.

(h) Unless otherwise ordered by the Commission, a utility shall immediately discontinue recovery of the "Security Cost Rider" when the earlier of the following occurs: natural expiration due to the full recovery provided for in a Rider granted under this Subchapter or forced expiration required pursuant to OAC 165:35-33-9(i) and/or OAC 165:35-33-9(j). Under no circumstances, shall the utility be permitted to double recover Homeland Security and Critical Infrastructure related costs.

(i) Unless otherwise ordered by the Commission, any utility with a "Security Cost Rider" currently in effect, that files for a general rate change, shall include in the rate case, all security-related costs and those costs shall be accorded standard ratemaking treatment. A utility shall discontinue its "Security Cost Rider" when the change in rates becomes effective upon Final Order in the rate case.

(j) Unless otherwise ordered by the Commission, all "Security Cost Riders" approved by the Commission, shall expire five years from the initial date of the "Security Cost Rider's" implementation.

(k) Upon the filing of a cost recovery request by a utility, Commission Staff, the state Attorney General's office (based upon that entity's statutory authority) and all other

Authorized Participants shall review the cost recovery proposal submitted by the utility and file testimony in accordance with:

(1) Any applicable protective orders issued by the Commission in the security-related cost recovery cause;

(2) OAC 165:35-33-11 (below);

(3) The Commission's Rules of Practice (OAC 165:5); and

(4) Any other protective measures or requirements prescribed by law or the Commission.

(l) Testimony of Commission Staff, the state Attorney General and all other Authorized Participants, shall detail each of the parties' respective recommendations and any objections to the utility's Plan and the utility's request for cost recovery related to the Plan. Also in accordance with the Commission's Rules of Practice, Commission Staff, the state Attorney General and all other Authorized Participants shall provide copies of their respective individual testimonies to one another, with redacted versions of each individual testimony filed with the Court Clerk at the Commission.

(m) Upon notice and hearing, the Commission shall issue an Order regarding any requests for security-related cost recovery.

165:35-33-10. Commission Authorized Participation

(a) **Commission Staff.** Only those Commission Staff and Staff's designees authorized by the Commission shall participate in a cause before the Commission regarding a utility's Plan and then, shall do so only after meeting all applicable requirements for Commission authorization, which shall be determined on a case-by-case basis. All Commission Staff and Staff's designees authorized to participate in a security cause shall comply with the requirements for protecting information obtained under the "Highly Sensitive Confidential" designation.

(b) **Attorney General.** Only those Attorney General personnel who have formally entered an appearance pursuant to Oklahoma Statute and the Commission's Rules of Practice and that entity's Commission authorized designees shall be granted review of a utility's Plan and/or Plan Update Reports. All Attorney General personnel and their designees authorized to participate in a security cause shall meet all applicable requirements for Commission authorization, to be determined on a case-by-case basis, and shall comply with the protections afforded information obtained under the "Highly Sensitive Confidential" designation.

(c) **Intervenors.**

(1) For the purposes of this Subchapter, all intervenors, including but not limited to counsel and experts for intervenors, shall be deemed "Authorized Participants" in accordance with OAC 165:35-33-3 above. All Authorized Participants wishing to participate in a security-related cause before the Commission shall meet all applicable requirements for Commission authorization, which shall be determined on a case-by-case basis, and shall comply with the protections afforded information obtained under the "Highly Sensitive Confidential" designation.

(2) In addition to acquiring "Authorized Participant" status from the Commission, each intervenor and its designees desiring to participate in a cause before the

Commission regarding a utility's Plan shall post a bond or other security acceptable to the Commission, in an amount to be determined by the Commission, to protect the utility from harm in the event the Authorized Participant breaches the confidentiality terms established under this Subchapter or as may otherwise be established by the Commission. A copy of such bond or other security shall be filed with the Commission's Court Clerk. This subsection shall not apply to the Attorney General of the State of Oklahoma or the Oklahoma Corporation Commission Commissioners and Staff.
(3) Any Authorized Participant found in violation of a Commission issued Protective Order and Proprietary Agreement, shall be liable for contempt penalties pursuant to the penalty provisions found in Article IX, § 19 of the Oklahoma Constitution, Title 17 of the Oklahoma Statutes and the Commission's Rules of Practice at OAC 165:5. This subsection shall not apply to the Attorney General of the State of Oklahoma or the Oklahoma Corporation Commission Commissioners and Staff.
(4) In addition to the above protections, all Authorized Participants may be required by the Commission to enter into a separate non-disclosure agreement as a pre-requisite to being granted intervention and "Authorized Participant" status.

165:35-33-11. Confidentiality

(a) Pursuant to the Commission's jurisdiction granted under Article IX, Section 18 of the Oklahoma Constitution, 51 O.S. (2001) §24A.22 of the Oklahoma Statutes and OAC 165:5, the Commission's Rules of Practice; all un-redacted documents related to a utility's Homeland Security and Critical Infrastructure Plan shall be considered "Highly Sensitive and Confidential" and shall only be admitted into evidence in en camera proceedings.
(b) "Highly Sensitive Confidential" designation and protection shall extend but not be limited to the following: initial Plans (including underlying documents), Plan Update Reports, Certification Letters, Annual Reports made by Commission Staff, recommendations submitted by the Attorney General of the State of Oklahoma and un-redacted documents used in cost recovery proceedings. For all other documents, the "Highly Sensitive Confidential" designation may be granted upon hearing and Final Order of the Commission.
(c) Each utility's Plan and/or Plan Update Report prepared in accordance with this Subchapter, shall be marked "Highly Sensitive Confidential" and shall be kept and maintained on site at the utility's business office in accordance with OAC 165:35-33-7(g), above. Only those individuals on the Staff of the Corporation Commission and in the State Attorney General's office and their respective experts who have been authorized by the Commission, shall have access to the Plan and Plan Update Reports prepared by each utility and any related or supporting documentation thereto. All other parties granted authorized intervenor status to a security cause pursuant to OAC 165:35-33-10(c) may also have access to the Plan, Plan Update Reports and supporting documentation after notice and hearing.

Appendix J

Oklahoma Corporation Commission's Proposed Telecommunications Service Rules

BEFORE THE CORPORATION COMMISSION OF THE STATE OF OKLAHOMA

IN THE MATTER OF A RULEMAKING OF THE OKLAHOMA CORPORATION COMMISSION AMENDING OAC 165:55, TELECOMMUNICATIONS SERVICE RULES	))))	CAUSE NO. RM 200400013

CHAPTER 55. TELECOMMUNICATIONS SERVICE RULES
(Critical Infrastructure Security Rules)

SUBCHAPTER 25

FINAL PROPOSED RULE

December 9, 2004

SUBCHAPTER 25. HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE

Section
165:55-25-1. Purpose and Scope
165:55-25-2. [Reserved]
165:55-25-3. Definitions
165:55-25-4. [Reserved]
165:55-25-5. Utility Security Plan
165:55-25-6. [Reserved]
165:55-25-7. Reporting Requirements
165:55-25-8. [Reserved]
165:55-25-9. Cost Recovery
165:55-25-10. Commission Authorized Participants
165:55-25-11. Confidentiality

165:55-25-1. Purpose and Scope

(a) The purpose of this Subchapter is to encourage facilities-based providers (FBPs) to take all reasonable measures necessary to protect their critical infrastructures from extended interruption of service from all extraordinary events, natural and man-made.

(b) The Corporation Commission encourages FBPs to develop, implement, and maintain Homeland Security and Critical Infrastructure Plans according to the industry standards enumerated in sub-section (d) below.

(c) To the extent that a FBP seeks cost recovery for the implementation of Homeland Security and/or Critical Infrastructure protections, the FBP shall comply with all provisions of this Subchapter.

(d) Each FBP serving Oklahoma jurisdictional customers is encouraged to follow the most current Network Reliability and lnteroperability Council (NRIC) Best Practices (www.bell-labs.com/cgi-user/krauscher/bestp.pl) security guidelines and standards and the National Fire Protection Association's ("NFPA") NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs (http://www.nfpa.org/PDF/nfpa1600.pdf?src=nfpa), as may be amended from time to time, for use as guidelines for protecting the FBP's Critical Infrastructure from extended service interruption.

(e) Each FBP seeking cost recovery for security measures from Oklahoma jurisdictional customers shall develop, implement, and maintain a Critical Infrastructure and Security Plan in accordance with this Subchapter.

(f) If the FBP has implemented a Security Plan or process in accordance with the applicable industry guidelines but is not seeking or receiving cost recovery for security-related costs, the FBP shall submit the Certification Letter required by OAC 165:55-25-7(f) and the Plan shall be subject to review pursuant to the Authorized Participation and Confidentiality provisions of OAC 165:55-25-10 and OAC 165:55-25-11. The FBP is not otherwise required to comply with the provisions of this Subchapter.

(g)The Commission retains its jurisdictional and supervisory authority to address the reasonableness and/or prudence of any proposed security cost recovery.
(h) Nothing in this Subchapter shall relieve any FBP from any duty otherwise prescribed by the laws of the State of Oklahoma or the Commission's rules.
(i) Nothing in this Subchapter is intended to divest the FBP of its right to object to any discovery requests from intervenors seeking access to "Highly Sensitive Confidential" materials.
(j) If any provision of this Subchapter is held invalid, such invalidity shall not affect other provisions or applications of this Subchapter which can be given effect without the invalid provision or application, and to this end, the provisions of this Subchapter are declared to be severable.

165:55-25-2. [Reserved]

165:55-25-3. Definitions

The following words and terms, when used in this Subchapter 25, shall have the following meaning, unless the context clearly indicates otherwise:

"Annual Report" means the Annual Report submitted by Commission Staff to the Commission beginning December 30, 2005 and by July 1 of each year thereafter, summarizing the results of Staff's review of each FBP's Security Plan (and any Plan Update Reports), along with any recommendations that Staff may have regarding such Plan(s).

"Authorized Participant" means those persons authorized by the FBP or as may otherwise be authorized by law and/or ordered by the Commission, to view highly sensitive confidential information. Such authorization shall be granted on a case-by-case basis and may extend to the FBP, state government officials, persons having been granted intervenor status by the Commission and Commission authorized designees of the parties.

"Certification Letter" means the written certification to the Director of the Public Utility Division made August 1, 2005 and March 1 of each subsequent year thereafter, indicating that the FBP has updated the Plan and/or previous Plan Update Reports, has a Plan but is not seeking cost recovery or has no Plan in place.

"Critical Infrastructure" means the property of a FBP located in the State of Oklahoma, comprised of either physical assets or computer software which, if severely damaged or destroyed, would have a significant impact on the ability of the FBP to serve large numbers of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the telecommunications grid, or would cause significant risk to public health and safety.

"FBP" or **"Facilities-Based Provider"** means all carriers regulated by the Commission, other than wireless Eligible Telecommunications Carriers, that own, operate or otherwise control facilities, network and /or other physical plant used to provide telecommunications to persons in Oklahoma.

"Highly Sensitive Confidential" means that the information is of such a sensitive

nature that its public disclosure could be harmful to the security of a FBP's critical infrastructure and as such it may only be viewed by those persons authorized by the FBP or as may otherwise be ordered by the Commission.

"NFPA" means National Fire Protection Association.

"NRIC" means Network Reliability and Interoperability Council.

"Plan" means a Homeland Security and Critical Infrastructure Plan including any subsequent Plan Update Reports that have been prepared with reference to NRIC and/or NFPA guidelines.

"Plan Update Report" means the written redlined changes made by the FBP updating the Plan and/or previous Plan Update Reports. At the FBP's option, changes will either be redlined or a history of changes may be maintained.

"Security Cost Rider" means the per billing unit rate mechanism whereby a FBP may, upon approval and Order of the Commission, recover the costs of providing security for its Critical Infrastructure as defined under this Subchapter 25.

165:55-25-4. [Reserved]

165:55-25-5. FBP Security Plan

(a) Each FBP is encouraged to prepare and make available for inspection, a "Homeland Security and Critical Infrastructure Plan" ("Plan") that has been prepared with reference to the NRIC safety guidelines and standards.

(b) The Plan shall be marked as "Highly Sensitive Confidential" and designate those facilities that the FBP considers to be Critical Infrastructure (physical assets and computer software as defined in OAC 165:55-25-3 above), and shall set forth the FBP's measures to secure such facilities from extended service interruption. The Plan shall also include an estimate of the costs necessary to achieve such measures.

(c) The Plan shall remain on site at the FBP's business office in accordance with OAC 165:55-25-7(g) below and shall have the most current version of the redlined Plan Update Report attached to the clean version of the FBP's latest Plan. At the FBP's option, changes will either be redlined or a history of changes may be maintained.

(d) The Plan shall list all locations deemed by the FBP to be critical as well as identification of any subsequently increased security measures. All locations and security measures shall be identified by code known only to the utility and designated state government officials and their designees.

(e) Any subsequent security measures identified in the Plan shall contain an estimate of the cost necessary to implement such measures, a description of the measures necessary to adequately secure each specific location and an estimated schedule for completion of each measure.

(f) All locations identified by the Plan that require additional security measures shall be prioritized by the FBP.

(g) Beginning December 30, 2005 and on July 1 of each year thereafter, Commission Staff shall submit an Annual Report marked as "Highly Sensitive Confidential" to the

Commission summarizing the results of Staff's review of each FBP's Plan (and any Plan Update Reports), along with any recommendations that Staff may have regarding such Plan(s).
(h) Beginning December 30, 2005, where the Attorney General elects to submit recommendations to the Commission regarding a FBP's Plan, such recommendations shall be marked as "Highly Sensitive Confidential" and shall also be due by July 1 of each subsequent year thereafter.

165:55-25-6. [Reserved]

165:55-25-7. Reporting requirements
(a) Subsequent to the preparation of the initial Plan prepared under OAC 165:55-25-5(a), each FBP shall prepare a Plan Update Report by March 1 of each succeeding year, following the same format as the initial Plan with redlines of all new changes, marked "Highly Sensitive Confidential" and kept on site at the FBP's business office.
(b) Each subsequent Plan Update Report shall update the previous year's report by indicating for each specific coded location, all costs and completion dates (actual and projected) for all current and prior additional security measures claimed under this Subchapter.
(c) For those security measures previously reported that have not yet been completed, revised estimated costs and estimated completion dates shall be provided.
(d) The Plan Update Report shall also include (by specific location) a description of each proposed security measure that has not been previously reported, the estimated costs for each, as well as the estimated completion date for each measure.
(e) Costs reflected in the initial Plan and in subsequent Plan Update Reports, whether estimated or actual, shall be identified as either capital or expense costs.
(f) Beginning August 1, 2005 and by March 1 of every year thereafter, each FBP shall submit a Certification Letter to the Director of the Public Utility Division, marked as "Highly Sensitive Confidential" and certifying that as of the date of the Certification Letter:

(1) The FBP does not have a Homeland Security and Critical Infrastructure Plan as contemplated and defined by this Subchapter;
(2) The FBP does not have a Homeland Security and Critical Infrastructure Plan as contemplated or defined by this Subchapter but has otherwise taken steps to secure its facilities and Critical Infrastructure and is not seeking cost recovery under this Subchapter;
(3) The FBP does have a Plan but is not seeking cost recovery; or
(4) The FBP has prepared its Plan Update Report updating the Plan and/or previous year's Plan Update Report and that the redlines contained within the current Plan Update Report encompass in the entirety, all of the changes made to the FBP's Plan since the Plan's inception or the previous year's certification and that the Plan is available for Commission and/or Attorney General review at the

FBP's local place of business.
(g) A FBP shall not be required to file its initial Plan or any of its subsequent Plan Update Reports with the Commission. Each FBP shall instead, secure and maintain on site, at the FBP's local place of business, its initial Plan and all subsequent Plan Update Reports.

165:55-25-8. [Reserved]

165:55-25-9. Cost recovery
(a) Each FBP seeking cost recovery of expenditures related to securing its Critical Infrastructure shall prepare and make available for inspection, its Plan and any subsequent Plan Update Reports in accordance with this Subchapter.
(b) Each FBP shall file an Application with the Commission for cost recovery as provided for within this Subchapter. Such cost recovery shall only occur to the extent the FBP has incurred all or a portion of its actual security-related costs.
(c) Unless otherwise ordered by the Commission, a FBP shall have the burden of proving compliance with all of the provisions of this Subchapter prior to obtaining cost recovery for security related measures.
(d) The total costs incurred under this Subchapter shall be combined for recovery purposes, for consideration by the Commission.
(e) All costs approved by the Commission for recovery, shall be recovered from the FBP's customers through a "Security Cost Rider" based upon the number of access lines for the FBP and shall be subject to annual true-up.
(f) Unless otherwise ordered by the Commission, A FBP shall immediately discontinue recovery of the "Security Cost Rider" when the earlier of the following occurs: natural expiration due to the full recovery provided for in a Rider granted under this Subchapter or forced expiration pursuant to OAC 165:55-25-9(g). Under no circumstances, shall the FBP be permitted to double recover Homeland Security and Critical Infrastructure related costs. Where a "Security Cost Rider" is utilized, Homeland Security and Critical Infrastructure related costs shall not be recoverable through a rate increase pursuant to 17 O.S. §137 et seq. or from the Oklahoma Universal Service Fund ("OUSF") pursuant to 17 O.S. §139.106.
(g) Unless otherwise ordered by the Commission, all "Security Cost Riders" approved by the Commission, shall expire five years from the initial date of the "Security Cost Rider's" implementation.
(h) Upon the filing of a cost recovery request by a FBP, Commission Staff, the state Attorney General's office (based upon that entity's statutory authority) and all other Authorized Participants shall review the cost recovery proposal submitted by the FBP and file testimony in accordance with:

(1) Any applicable protective orders issued by the Commission in the security-related cost recovery cause;
(2) OAC 165:55-25-11 (below);
(3) The Commission's Rules of Practice (OAC 165:5); and
(4) Any other protective measures or requirements prescribed by law or the

Commission.

(i) Testimony of Commission Staff, the state Attorney General and all other Authorized Participants shall detail each of the parties' respective recommendations and any objections to the FBP's Plan and the FBP's request for cost recovery related to the Plan. Also in accordance with the Commission's Rules of Practice, Commission Staff, the state Attorney General and all other Authorized Participants shall provide copies of their respective individual testimonies to one another, with redacted versions of each individual testimony filed with the Court Clerk at the Commission.

(j) Upon notice and hearing, the Commission shall issue an order regarding any requests for security-related cost recovery.

165:55-25-10. Commission Authorized Participation

(a) **Commission Staff.** Only those Commission Staff and Staff's designees authorized by the Commission shall participate in a cause before the Commission regarding a FBP's Plan, and then shall do so only after meeting all applicable requirements for Commission authorization, which shall be determined on a case-by-case basis. All Commission Staff and Staff's designees authorized to participate in a security cause shall comply with the requirements for protecting information obtained under the "Highly Sensitive Confidential" designation.

(b) **Attorney General.** Only those Attorney General personnel who have formally entered an appearance pursuant to Oklahoma Statute and the Commission's Rules of Practice and that entity's Commission authorized designees shall be granted review of a FBP's Plan and/or Plan Update Reports. All Attorney General designees authorized to participate in a security cause shall meet all applicable requirements for Commission authorization, to be determined on a case-by-case basis, and shall comply with the protections afforded information obtained under the "Highly Sensitive Confidential" designation.

(c) **Intervenors.**

(1) For the purposes of this Subchapter, all intervenors, including but not limited to counsel and experts for intervenors, shall be deemed "Authorized Participants" in accordance with OAC 165:55-25-3 above. All Authorized Participants wishing to participate in a security-related cause before the Commission shall meet all applicable requirements for Commission authorization, which shall be determined on a case-by-case basis, and shall comply with the protections afforded information obtained under the "Highly Sensitive Confidential" designation.

(2) In addition to acquiring "Authorized Participant" status from the Commission, each intervenor and its designees desiring to participate in a cause before the Commission regarding a FBP's Plan shall post a bond or other security acceptable to the Commission, in an amount to be determined by the Commission, to protect the utility from harm in the event the Authorized Participant breaches the confidentiality terms established under this Subchapter or as may otherwise be established by the Commission. A copy of such bond or other security shall be filed with the Commission's Court Clerk. This subsection shall not apply to the Attorney General of the State of Oklahoma or the Oklahoma Corporation

Commission Commissioners and Staff.
(3) Any Authorized Participant found in violation of a Commission issued Protective Order and Proprietary Agreement, shall be liable for contempt penalties pursuant to the penalty provisions found in Article IX, § 19 of the Oklahoma Constitution, Title 17 of the Oklahoma Statutes and the Commission's Rules of Practice at OAC 165:5. This subsection shall not apply to the Attorney General of the State of Oklahoma or the Oklahoma Corporation Commission Commissioners and Staff.
(4) In addition to the above protections, all Authorized Participants may be required by the Commission to enter into a separate non-disclosure agreement as a pre-requisite to being granted intervention and "Authorized Participant" status.