

MINUTES OF THE SENATE UTILITIES COMMITTEE.

The meeting was called to order by Chairperson Senator Stan Clark at 9:30 a.m. on March 17, 2003 in Room 231-N of the Capitol.

All members were present except: Senator Tyson, excused

Committee staff present: Raney Gilliland, Legislative Research
Bruce Kinzie, Revisor of Statutes
Ann McMorris, Secretary

Conferees appearing before the committee:

Mark Schreiber, Westar Energy
Larry Dolci, Great Plains Energy
Mike Bier, Great Plains Energy
Robert Nichols, Aquila
David Springe, CURB
Rep. Carl Krehbiel
Dick Rohlf, Westar Energy
Larry Holloway, KCC
Bruce Sneed, State Energy Resources Coordinating Council
Jim Ploger, KCC

Others attending: See attached list

Chair opened hearing on

HB 2037 - Repeal of sunsets on recovery of certain utility costs for use of public rights-of-way and for security

Proponents:

Mark Schreiber, Westar Energy (Attachment 1)
Larry Dolci, Great Plains Energy (Attachment 2)
Mike Bier, Great Plains Energy (Attachment 3)
Robert Nichols, Aquila (Attachment 4)
Written only - Bruce Graham, KEPCO (Attachment 5)

Opponents:

David Springe, CURB (Attachment 6)

Chair opened hearing on:

HB 2374 - Procedures for recovery of public utilities' security costs

Proponents:

Rep. Carl Krehbiel (Attachment 7)
Dick Rohlf, Westar Energy (Attachment 8)
Robert Nichols, Aquila (Attachment 4)
Larry Dolci, Great Plains Energy (Attachment 9)

Opponents:

Larry Holloway, KCC (Attachment 10)
David Springe, CURB (Attachment 11)

Some discussion on whether all utilities (water, gas, electric) should be included in this bill - Rep. Carl Holmes, chairman of the House Utilities Committee answered that the other utilities are regulated by FERC and private entities.

Due to lack of time, hearings on both **HB 2037** and **HB 2374** were left open for continued discussion at the next meeting of the Senate Utilities Committee on March 18.

Chair opened hearing on

HB 2131 - Update of energy efficiency standards for new commercial and industrial buildings.

CONTINUATION SHEET

MINUTES OF THE SENATE UTILITIES COMMITTEE at on March 17, 2003 in Room 231-N of the Capitol.

Proponents

Bruce Sneed, State Energy Resources Coordinating Council (Attachment 12)

Jim Ploger, KCC (Attachment 13)

Written testimony by Gene Meyer, KSU (Attachment 14)

Charles Benjamin, Sierra Club (Attachment 15)

Due to lack of time, testimony by proponents who have signed up will be continued at the next meeting of the Senate Utilities Committee on March 18, 2003.

Adjournment.

Respectfully submitted,

Ann McMorris, Secretary

Attachments – 15

SENATE UTILITIES COMMITTEE GUEST LIST

DATE: MARCH 17, 2003

Name	Representing
Joe Dub	KLBPU
Steve Johnson	Kansas Gas Service
Whitney Damron	KS Gas Service
Mark Schreiber	Westar Energy
Larry Dolci	GPE - KEPL
Michael Bier	KCPH
Larry Holloway	KCC
Tom Day	KCC
Dave Spriggs	Curh
Mark Holley	Wataco
Ben Hepper	KS Dairy Assoc
Dave HOLTHAUS	KEC
Tom DAY	KCC
Greg Smiter	GPE
Dana Sneed	SERCG
Joe Long	Aquila Inc

**Testimony before the
Senate Utilities Committee
By
Mark Schreiber, Senior Manager Government Affairs
Westar Energy
March 17, 2003**

Chairman Clark and members of the committee, I am Mark Schreiber, senior manager, government affairs for Westar Energy.

Westar Energy supports House Bill 2037 as amended. Our support for Section 1(b) is based on a commitment by the League of Kansas Municipalities to prepare and distribute a model right-of-way ordinance to its members in the next few months. Although cities are not required to follow the model ordinance, Westar Energy will watch as new right-of-way ordinances are prepared and implemented to see if the intent of the model ordinance is followed.

The security cost recovery sunset requested for repeal concerns the recovery of prudent costs associated with providing security to a utility's generation and transmission assets. This sunset is set to take effect June 30, 2004. The protection of these vital assets is essential for our economy and benefits every customer. Security is a 24-hour a day, 365 day a year activity. Securing our assets will not end June 30, 2004. Thus recovery of those costs is needed as long as is prudent and allowed by the Kansas Corporation Commission.

Westar Energy requests that you approve House Bill 2037 as amended to ensure security costs are recovered appropriately and in a reasonable manner.

Senate Utilities
March 17, 2003
Attachment 1-1

Testimony Before the Kansas Senate Utilities Committee On HB2037
Recovery of Certain Costs by Utilities
Submitted by Lawrence Dolci
Director Resource Protection
Great Plains Energy
March 17, 2003

Great Plains Energy Company and its electrical company, Kansas City Power & Light Company support the passage of Kansas House Bill 2037 that would repeal the two year sunset provision of K.S.A. 66-1233 that was enacted last session.

House Bill 2037 should be passed because the current two-year recovery period in K.S.A. 66-1233 is not adequate to allow recovery of utility security expenditures that will have to be made over the next several years to ensure reliable service to the citizens of Kansas.

Substitute Senate Bill 545, passed during the last legislative session recognized the need to recover the considerable costs expended to provide security for utilities in the aftermath of the terrorist attacks of September 11, 2001. That bill, which became part of the statute cited above, contained a sunset provision effective July 1, 2004.

In the period immediately following the terrorist attacks of September 11th. Many utilities increased their security in anticipation of additional attacks. A number of voluntary and mandatory guidelines and regulations on cyber and physical security were issued in the months after the attacks that required or recommended additional security. New regulations and guidelines have been issued and have required utilities to spend significant additional amounts on security. For example the Nuclear Regulatory Commission, NRC, immediately after the September 11th attacks ordered nuclear power plants to upgrade security. The NRC has continued to issue new, tighter regulations on a regular basis and has proposed even more stringent guidelines. While the details of the NRC regulations cannot be discussed, because they are classified, their impact will be increases in equipment and manpower costs at the Wolf Creek Nuclear plant near Burlington.

The Federal Energy Regulatory Commission, FERC, has issued proposed guidelines that will require significant security improvements for electric utilities that market wholesale power. A copy of these guidelines is attached as exhibit 1. Implementation of these guidelines will extend well beyond the current sunset date of July 1, 2004.

The North American Electric Reliability Council, NERC, that is responsible for the reliability of the national electric grid has issued a series of cyber and physical security guidelines and plans to issue more. A copy of some of these relevant guidelines is attached as exhibit 2. Compliance with the existing NERC guidelines is a process that will take many years and there is every reason to believe that additional guidelines will be issued. Setting an arbitrary two year time limit for recovery will not allow recovery of

the unanticipated substantial outlays for security that are being required or strongly suggested for utilities.

The United States Department of Energy also issued a list of best practices for utilities shortly after the attacks of September 11th. While these guidelines are voluntary they do set a standard against which utilities will be judged in the security area. A set of these guidelines is attached as Exhibit Three.

Electric utilities have just begun a process of evaluating ways to protect or replace crucial cyber and physical pieces of the electrical grid should they be attacked. This work is being done at the national level through NERC and at the state level by the Kansas electric utilities. The process of identifying the critical pieces of the electrical grid and determining the best way to protect or repair them if attacked will take years. For example, after the identification of critical components utilities must evaluate whether a stockpile of spare equipment should be established. Such a stockpile is only feasible if the components can be readily interchanged between utilities, an issue that requires more study.

The electric utilities are also conducting studies on vulnerabilities of large components of the transmission system and how they might be protected on site. Specific tests have identified vulnerabilities but studies on ways to mitigate these physical threats have just begun.

Work also continues on identifying cyber vulnerabilities and mitigating them. This is critical since the electrical grid is controlled by automated systems that could be attacked remotely. The United States Department of Energy has issued guidelines on protecting these systems. The DOE guidelines are attached in exhibit 3 referenced earlier. Implementation of the DOE guidelines will also take years

Other states are addressing the issue of cost recovery for security measures as Kansas did in the last legislative session. SB 290 was introduced this session in the Missouri Senate to allow recovery of security costs by utilities. A similar bill was introduced in the Missouri House. These bills are very similar to the current Kansas Statute; however, they do not include sunset provisions.

Removal of the sunset provision from K.S.A. 66-1233 as proposed in HB 2037 will benefit the citizens of Kansas by helping to make sure utilities have the funding available to follow sound security practices, practices that will provide for reliable utility systems for the foreseeable future.

Security Standards for Electric Market Participants

PURPOSE

Wholesale electric grid operations are highly interdependent, and a failure of one part of the generation, transmission or grid management system can compromise the reliable operation of a major portion of the regional grid. Similarly, the wholesale electric market – as a network of economic transactions and interdependencies – relies on the continuing reliable operation of not only physical grid resources, but also the operational infrastructure of monitoring, dispatch and market software and systems. Because of this mutual vulnerability and interdependence, it is necessary to safeguard the electric grid and market resources and systems by establishing minimum standards for all market participants, to assure that a lack of security for one resource does not compromise security and risk grid and market failure for the market or grid as a whole.

The purpose of these standards is to ensure that electric market participants have a basic Security Program protecting the electric grid and market from the impacts of acts, either accidental or malicious, that aren't authentic or could cause wide-ranging, harmful impacts on grid operations and market resources. A basic Security Program for electric grid and market resources (hereafter referred to as market resources) shall cover governance, planning, prevention, operations, incident response, and business continuity.

Security standards for market resources will primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact the grid or market, and personnel (hereafter the word cyber shall refer to all of these

aspects). In addition, physical security will be addressed to the extent that it is necessary to assure a secure physical environment for cyber resources.

This initial set of security standards represent a minimum set of measures derived from commonly accepted industry standards and practices, such as the Common Criteria, CTSEC, ITSEC, IPSEC, ISO 17799, NIST Guidelines, and the NERC Security Guidelines. Market participants are encouraged to review their individual situation and tolerance for risk and implement a Security Program that goes beyond these basic security standards herein.

APPLICATION

These standards are intended to ensure that appropriate mitigating plans and actions are in place, recognizing the role of the participant in the marketplace and the risks being managed. For the purpose of these security standards, participants are defined as, and the standards shall apply to:

- The market operations of RTO's and ISO's, and their market connections to Control Areas,
- Marketers,
- Transmission Owners,
- Power Producers,
- Load serving entities and other power purchasers,
- NERC and the Reliability Authorities, and
- Tagging (or other similar dispatching) Organizations.

Further, if a power-generating unit participates directly in the grid (i.e. it is electronically dispatched by control centers), the plant control system shall comply with these security

standards. If a power-generating unit participates directly in the electric market (i.e. submits Tagging requests), its market systems shall also comply with these security standards.

COMPLIANCE

These security standards shall become effective on January 1, 2004. Beginning 2004, on January 1 of each year, every participant shall file with FERC a self-certification signed by an officer of the company indicating compliance with these standards and identifying any areas of non-compliance. Failure to comply with these security standards will result in loss of direct access privileges to the electric market.

Malicious acts directed against the electric market, shall be prosecuted by FERC and law enforcement agencies to the full extent of the law, including the recovery of damages.

SECURITY STANDARDS

Governance:

Participant senior management shall designate a management official to be responsible for establishing and managing a basic Security Program for electric market functions and resources.

Security Scope:

Participants shall define their security perimeter, identify the boundaries and defenses for physical and cyber security that delineate and protect the critical resources under their control. The security perimeter shall identify all entry and exit points and the requirements for access controls. A Security Program and policy based on, and implementing these security standards shall be developed to protect critical electric grid and market functions and resources within the security perimeter and at entry and exit points where personnel, supplies or communications may

come and go. Additionally, related procedures shall be created that guide implementation and enforcement of the security standards. Policy and procedures shall be reviewed for appropriateness (due to changes in personnel, technology, equipment configuration, vulnerabilities and threats) as necessary, and at least annually.

Asset Classification and Control:

Electric market assets within the security perimeter shall be classified as to their criticality in maintaining and protecting electric market functions. A classification system shall further define appropriate levels of protection for each level of criticality, and access rights that will be granted for each level of criticality. All critical assets within the perimeter (computers, networks, doorways, etc.) shall have a custodian who ensures that those assets are handled in accordance with their assigned classification scheme.

Personnel:

Any personnel who are authorized access within the security perimeter, or are authorized access to administer, operate or maintain assets within the security perimeter shall be trained on the Security Program and security standards related to their respective positions. This training shall start upon employment, be repeated annually and at career points where significant responsibilities change. Security awareness training shall be provided to all staff.

To the extent permitted by law, personnel required to administer or operate assets classified as critical (according to the participant's classification system) shall undergo background investigation conducted prior to employment, upon promotion to such positions (if not a new hire), and at periodic intervals (not to exceed five years). The participant shall review the results of the background checks and take appropriate action. Individuals shall be disqualified from

administering, operating or accessing critical assets if the individual meets any disqualifying criteria specified by the Federal Bureau of Investigation, Office of Homeland Security, RCMP, or other federal agency.

Access Control:

A process such as transaction logs shall be in place to identify individual users of critical systems and their time of access. Procedures for critical electric grid and market resources within the security perimeter shall be developed that establish and monitor controls for:

- 1) The assignment of both logical and physical access rights (as defined in the classification system);
- 2) The prompt disabling of access rights when positions are terminated or job responsibilities no longer require access; and
- 3) The annual re-evaluation of assigned access rights.

Such authorized personnel -- including visitors and service vendors -- shall only have access (whether logical or physical) to electric market resources within the security perimeter that they are authorized for. Any and all unauthorized personnel allowed temporary access within the security perimeter shall be escorted at all times.

Systems Management:

Procedures for critical electric market resources within the security perimeter shall be developed to monitor and control cyber assets, such as:

- Computers,
- Software,
- Data,
- Servers,

- Routers,
- Modems, and
- Communications channels, whether owned or leased.

At a minimum, these procedures shall address:

- 1) The use of effective password routines that periodically require changing of passwords, including the replacement of default passwords on newly installed equipment;
- 2) Authorization and re-validation of computer accounts;
- 3) Disabling of unauthorized (invalidated, expired) or unused computer accounts;
- 4) Disabling of unused network services and ports;
- 5) Secure dial-up modem connections;
- 6) Firewall software (for routed Internet access);
- 7) Intrusion Detection Systems (for networked routers and firewalls);
- 8) Host based intrusion or system failure detection for critical systems;
- 9) Patch management;
- 10) Installation and update of anti-virus software checkers.

For critical electric systems, operator logs and Intrusion Detection System logs shall be maintained for the purpose of checking system anomalies and for evidence of suspected unauthorized activity. Appropriate procedures for securing control systems that are critical to the grid or market shall be developed and employed. The procedures shall address:

- 1) Remote access including modems and other means;
- 2) Security patch management, as appropriate;
- 3) Assurance that communication channels are adequate so as not to impact the performance of the control system and its critical functions; and

- 4) Assurance that system procedures do not impact the performance of the control system and its critical functions.

Procedures for critical electric resources within the security perimeter shall be established to monitor and control physical features, such as:

- Doors,
- Windows,
- Floor space,
- Environmental systems,
- Backup power systems – whether owned or leased.

At a minimum, these procedures shall address:

- 1) Appropriate security barriers and entry controls; 2)
- 2) Mechanical and electronic key and badge programs; 3)
- 3) Access locking of unattended assets; and, 4)
- 4) Protection from environmental threats and hazards (e.g., loss of cooling).

Critical electric facilities shall restrict the distribution of maps, floor plans and equipment layouts pertaining to those facilities, and restrict the use of signage indicating critical facility locations.

Planning:

Security requirements for critical electric systems within the security perimeter shall be identified, documented and agreed upon prior to development, procurement, enhancement to, installation of and acceptance testing for cyber resources or related physical features. For critical control systems, this means developing cyber security procedures to augment existing test and/or acceptance procedures.

Development and testing of critical electric market systems shall be conducted in system environments that are not interconnected with operational system environments.

Incident Response:

Organizations with critical electric market resources shall have incident response procedures, which define roles, responsibilities and actions to rapidly detect and protect electric resources in the event of harmful or unusual incidents, whether accidental or malicious.

Organizations with critical electric market resources shall report incidents to the Electricity Sector – Information Sharing and Analysis Center (ES-ISAC) and use reporting criteria, thresholds and procedures contained in NERC's Indications, Analysis and Warning (IAW) Program.

Business Continuity:

Every participant operating a critical electric resource shall have contingency plans that define roles, responsibilities and actions for protecting the rest of the electric grid and market from the failure of its own critical resources. Those plans should further define the roles, responsibilities and actions needed to quickly recover or reestablish electric grid and market functions, processes and systems, in the event that a critical physical or cyber resource fails or suffers harm or attack. Such plans shall be tested or exercised regularly.

REFERENCES

The North American Electric Reliability Council (NERC) has established and maintains Security Guidelines for the Electricity Sector. NERC also provides a list of additional sources for security

best practices. These references shall be helpful in developing organization specific security standards and procedures for critical market resources.

ADDENDUM

Annual Self-Certification of Compliance with FERC Security Standards
(Due January 31, 2004, and every January 31st thereafter)

Date: _____

Subject: FERC Filing, Annual Self-Certification re: FERC Security Standards

From: _____(organization name)
_____(organization address)
_____(organization address)
_____(organization address)

This organization certifies the following items regarding FERC security standards for grid-market systems, as of this date:

Compliant	Non-Compliant	
?	?	Management assignment of grid-market system security.
?	?	Security Perimeter defined and documented.
?	?	Security Program and Policy developed and documented.
?	?	Policy, standards, and procedures reviewed at least annually.
?	?	An Asset Classification system defined and implemented.
?	?	Security training requirements for personnel with access to critical assets have been met.
?	?	All personnel receive security awareness training at least annually.
?	?	Critical asset administrators and operators have had background screening within last five years.
?	?	Access control procedures for authorized personnel are implemented.
?	?	Unauthorized personnel inside security perimeter are escorted at all times.
?	?	Cyber procedures for system security have been developed and implementation monitored for compliance.
?	?	Physical procedures for system security have been developed and implementation monitored for compliance.
?	?	Security requirements for developing and testing critical systems have been documented.
?	?	Software development systems are not interconnected with operational systems.
?	?	Incident response plans are implemented.
?	?	ES-ISAC reporting and alert notification procedures are implemented.
?	?	Business continuity plans are established and exercised.

Explanation for Non-Compliant Items:

Name: _____(print)

_____ (title)

_____ (signature)

**Security Guidelines for the Electricity Sector:
Physical Security**

<i>NERC</i>	<i>Guideline</i>
Guideline Title: Physical Security	Version: 1.0
Revision Date:	Effective Date: June 14, 2002

Purpose:

Each company should consider implementing physical security measures to safeguard personnel and prevent unauthorized access to critical equipment, systems, material, and information at critical facilities.

Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

Guideline Statement:

This guideline recommends "best practices" for the electricity sector in the area of physical security for facilities or functions identified as critical. It may be used in conjunction with the Vulnerability and Risk Assessment guideline, which assists companies in identifying critical facilities.

Table of Contents:

Security Guidelines for the Electricity Sector: Physical Security

Guideline Detail:

Physical security typically comprises five distinct elements, or systems:

- deterrence
- detection
- assessment
- communications
- response

Together, these elements provide a consistent "systems approach" to protecting critical assets.

Each company should prioritize its critical facilities and assets; characterize risks based on factors such as prior history of incidents, threat warnings from law enforcement agencies, system redundancies, overall operating requirements, etc. Each company also should consider an inspection and survey program to review existing security systems and to make recommendations for appropriate changes. (See guideline for conducting vulnerability assessments.)

In determining the types of physical security systems required for critical facilities, companies should consider the following:

- fencing and gates to restrict access to the facility for both safety and security purposes;
- limiting access to authorized persons through measures such as unique keying systems, "smart locks," access card systems, or the use of security personnel;
- access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e. photo ids, visitors passes, contractor ids) to be displayed while on company property;
- alarm systems to monitor entry into control rooms or other critical facilities;
- perimeter alarm systems to monitor unauthorized intrusion into the facility;
- recorded CCTV systems which can provide local or remote surveillance capability of a given facility;

Security Guidelines for the Electricity Sector: Physical Security

- roving security patrols or fixed station security staffing;
- alarms, CCTV, and other security systems reporting to the facility or to a central security station which can then be evaluated and company personnel or law enforcement authorities dispatched to investigate a potential problem;
- vehicle barriers;
- projectile barriers;
- security survey program;
- adequate lighting;
- signage; and
- a comprehensive security awareness program.

Physical security systems should be augmented based on changes in threat levels, scenarios, and categories. In designing a physical security system, the objective of the aggressor should be considered. The four major objectives in describing an aggressor's behavior are:

- Destroying or damaging critical facilities, property, or equipment,
- Stealing or damaging critical equipment, materials, or information,
- Posing a threat to the safety of personnel or customers, and
- Creating adverse publicity.

Exceptions:

Certified Products/Tools:

Security Guidelines for the Electricity Sector: Physical Security

Related Documents:

- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
 - Vulnerability and Threat Assessment
 - Threat Response
 - Emergency Plans
 - Continuity of Business Processes
 - Communications
 - Cyber Security
 - Employment Background Screening
 - Protecting Potentially Sensitive Information
- *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, <http://www.nerc.com>
- *Threat Alert Levels and Physical Response Guidelines*, NERC, November, 2001, <http://www.nerc.com>
- *Threat Alert Levels and Cyber Response Guidelines*, NERC, March 2002, <http://www.nerc.com>

Revision History:

Date	Version Number	Reason/Comments

DRAFT

VULNERABILITY AND RISK ANALYSIS PROGRAM

Lessons Learned and Best Practices



U.S. Department of Energy
Office of Critical Infrastructure Protection

September 28, 2001

2-18

CONTENTS

1	Introduction.....	1
2	Best Practices	3
3	Lessons Learned	9
4	Summary.....	13

1 INTRODUCTION

1.1 OBJECTIVE

This report summarizes initial lessons learned and best practices that have been captured as part of a multifaceted effort by the U.S. Department of Energy's Office of Critical Infrastructure Protection (OCIP) to work with the Energy Sector in developing the capability required for protecting the nation's energy infrastructures. Over the last three years, a team of national laboratory experts, working in partnership with the energy industry, has performed a series of vulnerability assessments as part of OCIP's Vulnerability and Risk Analysis Program (VRAP) (formerly the Infrastructure Assurance Outreach Program [IAOP]). The goal is to help energy-sector organizations identify and understand the threats to and vulnerabilities (physical and cyber) of their infrastructures, and to stimulate action to mitigate significant problems. Because the assessments are conducted on a confidential basis, the information in this report is intentionally presented at a high level so as not to reflect on specific companies or industry segments. A separate report entitled *Vulnerability and Risk Analysis Program Assessment Methodology* describes, at a high-level, the methodology developed for the program.

1.2 BACKGROUND

The U.S. Department of Energy established the Office of Critical Infrastructure Protection within the Office of Security and Emergency Operations in October 1999 to direct the Department's activities in accordance with Presidential Decision Directive 63 (PDD-63) and the priorities established by the Secretary of Energy. The primary mission of the Office is to work with the national Energy Sector in developing the capability required for assuring the Nation's energy infrastructures. This mission encompasses the physical and cyber components of the electric power, oil, and natural gas infrastructures, the interdependencies among these components, and the interdependencies with the other critical national infrastructures. The mission also includes identifying DOE technologies and capabilities that can help assure our nation's critical energy infrastructures and facilitating their use by the private sector and other federal agencies.

The VRAP is an integral part of the overall OCIP strategy in Critical Infrastructure Protection where the Department, as the federal government lead agency for the Energy Sector, partner's with industry to address vital issues of mutual interest. The specific objective of the VRAP program is to partner with the energy industry (electric power, oil, and natural gas) to "develop and implement a Vulnerability Awareness and Education Program for their sector" to enhance the security of the energy infrastructure, as directed by PDD-63. To accomplish the mission, the program is designed to develop, validate, and disseminate an assessment methodology with associated tools to assist in the implementation; provide training and technical assistance; and stimulate action to mitigate significant problems.

Eleven voluntary assessments have been completed under the VRAP initiative (several more are in progress and in the planning stages). The initial assessments focused on the electric power

industry, with efforts aimed at the broadest level of the industry. Assessments addressed key energy organizations whose operations, if disrupted, would have broad regional or national impact. More recently, assessments have included the natural gas industry, and discussions have begun with the oil industry.

In addition to VRAP, OCIP has initiated a multiyear research and development program—the Energy Infrastructure Interdependency Program—to develop cost-effective technologies and capabilities (e.g., databases, methodologies, and tools) for increasing our understanding of and our ability to analyze interdependencies among the energy infrastructures and between energy infrastructures and other critical national infrastructures (e.g., water supply systems, telecommunications, transportation, banking and finance, and emergency and government services). These technologies and capabilities will help the Department, Energy Sector organizations, and other public and private-sector infrastructure service providers assess the technical, economic, and national security implications of energy technology and policy decisions designed to ensure the security of our nation’s interdependent energy systems. Other OCIP initiatives are aimed at working with industry and government to develop/enhance plans for response and reconstitution of essential capabilities and services and working with state and municipal government organizations and utilities to prepare energy disruption guidelines for local communities. All of OCIP’s activities are closely coordinated and mutually supportive.

1.3 REPORT ORGANIZATION

The remainder of this report is organized as follows. Section 2 presents and discusses best practices. Section 3 discusses the lessons learned compiled by the VRAP team. These lessons are organized around the ten interrelated elements of the assessment methodology. Finally, Section 4 provides a summary of this effort.

2 BEST PRACTICES

2.1 BACKGROUND AND SCOPE

Effective operation of the U.S. energy production, transmission, and distribution systems are critical to the health and safety, national security, and economic viability of the nation. Such system operations are becoming increasingly dependent on information systems and other interdependent infrastructures. Even though energy sector information systems have not yet been subject to the same type or intensity of physical and information attacks as other infrastructures, there is growing concern that these systems are becoming more vulnerable. Furthermore, threats associated with critical infrastructures appear to be increasing, thus raising concerns for vital energy infrastructure components and systems. Utility deregulation and advances in technology also contribute to the potential for increased vulnerabilities of our critical energy supply and delivery systems. In addition, as the business model adapts to the new, information-intensive economy, supply chain dependencies increase and interdependencies grow.

The modern energy industry is in the midst of a dynamic era defined by rapid changes in technology (the Internet, information technology), the development of new business models (driven by deregulation, acquisition, and diversification), and the emergence of new internal and external threats (ranging from disgruntled employees to hackers to terrorists). At the same time, there is limited knowledge about threat assessment processes, vulnerability assessment methodologies and tools, and integrated risk management approaches. Descriptions of the new threats and vulnerabilities facing the industry, and recommended actions to address those threats and vulnerabilities, are provided in the recently released North American Electric Reliability Council report *An Approach to Action for the Electricity Sector* and the National Petroleum Council report *Securing Oil and Natural Gas Infrastructures in the New Economy*. The underlying theme in these reports is that vulnerabilities are increasing, they relate to the fundamental evolution of energy enterprises, and holistic efforts are required to address them.

The initial best practices presented below have been assembled as part of the Department's VRAP initiative to help energy-sector organizations identify and understand the threats to and vulnerabilities of their infrastructures. They are intended to highlight key issues relating to the protection of the nation's energy infrastructures, and to stimulate action where appropriate.

2.2 BEST PRACTICE RECOMMENDATIONS

To facilitate discussion, the best practices are grouped into three major issue categories: organization, education and awareness, and staffing. In each category, a series of best practice recommendations are stated followed by supporting background information. While the best practices were derived from the VRAP assessments, they are illustrative, and should not be viewed as comprehensive. That is, because the VRAP assessments are conducted on a

confidential basis, the information is intentionally presented at a high level so as not to reflect on specific companies or industry segments.

Organizational Issues

Organizational issues focus on best practices from a holistic approach. Specifically, they represent activities that should be on going at an enterprise-wide level.

- 1. Best Practice: Develop an overarching enterprise security model that is comprehensive, consistent with the mission and values of the organization, and widely accepted within the organization.**

Organizations should have an overarching security model that integrates both physical and cyber security. A security model establishes the suite of goals that guide development and implementation of security systems, processes, policies, and procedures. The model functionally embodies the risk posture of the organization, at least in the context of security. Such a model enables more balanced decisions on security-based risk acceptance and helps reconcile consideration of competing factors that have an impact on the risk and security condition of the enterprise. Such a model forms the basis for many security-related policies and procedures that can be disseminated throughout the organization. It also is particularly useful when dealing with organizational partners and suppliers.

- 2. Best Practice: Develop clear and direct lines of authority with dedicated staff for security, and ensure that responsibility and authority for security is integrated, not dispersed. A strong, accountable advocate at the executive level, with broad corporate acceptance of the role of security in protecting enterprise interests, is vital.**

Organizations should have dedicated staff with clear lines of authority regarding security that require or at least encourage uniform treatment of security. Many organizations have evolved lines of authority that parse security functions, responsibility, and authority among several organizational elements. This often creates confusion and conflict in developing security policies, their implementation, and administration. Furthermore, it enables (in some cases inspires) some organizational elements to conduct their missions in ways that clearly expose other elements to increased risk. Having dedicated, responsible staff for implementing security is desirable if not essential for effective security.

- 3. Best Practice: Incorporate security into enterprise risk management processes.**

Security should be incorporated into existing risk management processes. For many organizations, risk management is a purely financial function that relates more to acquisitions and mergers, facility siting, safety, or insurance than to asset protection, particularly for information systems. This has two principal impacts. First, security investment decisions lack the benefits that could be provided by a rigorous risk management approach. Second, the lack of integration of security in other risk management investment decisions means that gaps will likely exist in risk acceptance.

2.23

Furthermore, investments in vulnerability mitigation will likely be lower than is merited by the risk exposure.

4. Best Practice: Implement structured security requirements for critical suppliers and partners. Make security reviews an element of contracts for critical services and periodically evaluate compliance.

Contracts for supplies and services should include provisions addressing security. The same is true of partnering agreements. Since many of the suppliers, service providers, and partners require either or both physical and electronic access, their vulnerabilities are inherited by the enterprise contacting or partnering with them. Additionally, if the supplies are software, firmware, hardware, or information technology (IT) systems, the capacity to provide secure products or services depends on *their* internal security controls. While traditional remedies exist (e.g., lawsuits and financial losses through degradation of reputation), these are never desired options and they are compromised if there has been no expression of the need for security. Mutual understanding of security expectations at the outset of a relationship is important, and establishing expectations in the original contract will facilitate such understanding and avoid undesirable events and their consequences. The further benefit of establishing such contract requirements is that corporate policies must be established to provide a reasoned basis for establishing expectations of the subcontractor.

5. Best Practice: Develop a consistent designation and valuation of critical assets, and develop the means to assure the security of these assets.

Organizations should establish procedures for identifying critical assets. This is particularly important for information technology assets, which are not as fully understood as physical assets. Understanding asset criticality is important for several reasons. First, decisions regarding protection of enterprise assets are more difficult than for an element of the enterprise because it requires a comprehensive knowledge of all assets to be protected. Second, the likelihood that all employees and partners will have a common appreciation for the importance of an asset is low, making inadvertent loss more probable. Third, the likelihood of human error, particularly by new employees, that compromises an important asset is higher. Lastly, an enterprise often relies upon other infrastructures for support, ranging from law enforcement to telecommunication services.

6. Best Practice: Carefully consider security issues associated with any organizational changes and communicate the issues to all staff potentially affected by the changes. Make security part of the corporate culture and corporate goals.

Organizational change generally increases vulnerabilities. Utilities that change their organizational structures or create uncertainty about such changes are more vulnerable for two reasons. First, clear delineation and universal understanding of roles, responsibilities, authorities, and accountabilities (R^2A^2), as well as organizational functions and processes, are absent following organizational changes. Gaps can develop as the new organization is implemented, creating weaknesses and vulnerabilities that may go undiscovered for lengthy periods. The greater the change in organizational mission or structure, the more profound the potential vulnerabilities and duration of their existence. Second, uncertainty regarding organizational change (especially mission, goals,

functions, etc.) serves to delay implementation of prudent security measures. At a more fundamental level, dysfunctional elements of the organization compound the problem by creating confusion. A culture of security should be developed within the organization.

7. Best Practice: Monitor security efficiency and performance to ensure a robust security program and to ensure that corporate competitive strategies do not undermine security.

Ill-considered competitive strategies can erode security. The energy industry, like other industries, is under pressure to reduce costs. Organizations must be careful as they reduce costs so that they do not also erode security. Outsourcing is one activity that must be carefully considered and structured if security is to be maintained. Mergers and acquisitions increase vulnerabilities during the periods when disparate systems are being integrated, legacy system access is increased, and organizational elements are merged (or discarded). Globalization may decrease costs or offer larger markets, but open enterprises to cultures with different business priorities and motivations. Similarly, internal functions that cannot be directly traced to revenue generation are often targets for cost reduction. Security is rarely viewed as a means to ensure continued revenue flow or growth, but more often as potentially unnecessary or even as an impediment to implementation of low-cost business systems or processes. Finally, downsizing can affect security posture in many ways, such as increasing the pool of disgruntled current or former employees; but principally by reducing the skill level of those entrusted with security functions, or overtaxing the remaining security team.

8. Best Practice: Periodically review and update emergency plans to include newer threats and vulnerabilities, and test these plans regularly.

Emergency plans and business continuity plans need updating and testing regularly through emergency drills and exercises. Employees should be educated about the existence of plans, when they are activated, and what their roles and responsibilities are when they are activated. Because threats and vulnerabilities continue to evolve, these emergency plans should be reviewed, updated, and tested to ensure that these concerns are properly addressed.

9. Best Practice: Implement appropriate configuration management across all enterprise IT systems. Be particularly attentive to systems that interface with critical assets.

Configuration management is crucial even for “non-critical” systems. Absence of good configuration control inevitably opens information networks and systems to vulnerabilities. Lack of adequate staffing, lack of universal awareness of the value of the information and systems, and incomplete, outdated, or unenforced security policies and procedures increase the likelihood that such systems will be violated. The increasing trend to connect administrative computing networks to energy control networks (albeit with safeguards) increases the likelihood that vulnerabilities in non-critical systems will migrate to critical systems.

Education and Awareness Issues

Education and awareness issues focus on activities that organizations can perform to train and educate their employees, contractors, vendors, and customers. These activities, when implemented properly, can cost-effectively increase the level of security across the entire enterprise.

10. Best Practice: Raise employee awareness to be more proactive on security. Establish and implement policies and procedures for controlling and validating “trust” allocation.

Trust is often extended beyond appropriate levels. Industry has enjoyed and valued a culture of trust that is increasingly imprudent, particularly in the cyber dimension. Access to important systems, networks, and facilities should only be granted with due consideration of the need for such access. Increasing threats due to growing competition, erosion of workforce loyalty, growing sophistication of hackers, dependence on contract employees, and outsourcing argue for more discretion and control in assigning trust. Organizations should establish the means to differentiate trust levels and associated accesses and privileges. They should also establish processes to implement that differentiation.

11. Best Practice: Develop a means to raise and sustain management and employee awareness of physical and cyber threats.

Physical and cyber threat awareness needs to be increased enterprise wide. Utilities have only recently begun to experience external cyber attacks, or be the targets of organized groups. For example, the electric power industry has experienced no customer loss of service due to cyber attack. However, major changes in the industry, technology, and society, have created a more hostile world (e.g., the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon). While many organizations understand this and have begun to take steps to address this new world, general awareness and coordinated efforts to ensure protection have not been broadly adopted. In part, the message is that the threats are ubiquitous and growing, but this has not been effectively communicated to the domestic energy industry. Utilities should have programs that increase staff awareness of threats. In general, law enforcement and government have only marginally aided this awareness. They are hindered by a culture that focuses on reaction rather than prevention, and secrecy rather than communication. These cultures are changing, but slowly. Existing communications mechanisms (e.g., through NERC and industry security groups) need to be enhanced and new mechanisms need to be established, where necessary, to provide sensitive threat information to industry.

12. Best Practice: Develop and adopt means to ensure that both reliability and security missions are understood, as well as their respective roles in ensuring enterprise success.

Reliability is often confused with security. Reliability is being able to sustain delivery of service with few and/or minor disruptions. Security however protects the means to provide such reliability as well as achieve the many other desired outcomes of the enterprise (e.g., stockholder confidence, profitability, growth, customer loyalty, positive

brand image). Many people in the energy industry confuse these two topics. Indeed, one of the common terms in assuring electric reliability is “security” (basically, the ability of the electric grid to withstand some level of disruption and still function effectively). Since reliability is predominantly defined by natural events, human error, or random equipment failure, few pay significant attention to potential for malicious events and coordinated attacks (particularly when the history of the industry is one of relatively little domestic malicious activity, and essentially no terrorist activity).

13. Best Practice: Senior management should be periodically briefed and trained on information systems technology and their security, as well as risk management methodologies, analysis, and tools.

“New economy” vulnerabilities are elusive for management. The explosion of information technology and its use in vital business functions, has created a knowledge and experience gulf between those in senior management, many of whom have little experience with such technologies, and those younger managers who have such experience. Many senior managers, faced with decisions regarding the myriad of risks they do understand, have difficulty allocating the resources (organizational, managerial, and monetary) to addressing information security challenges that they do not understand. The challenge of information security is educating senior decision makers on the information technologies employed, the vulnerabilities their use presents, and the means to mitigate risks associated with those vulnerabilities.

Staffing Issues

Staffing issues focus on the difficulty of obtaining the right mix of physical and IT security staff.

14. Best Practice: Security training should be supported as a vital element of risk reduction. Participation in associations advancing security knowledge should be encouraged.

The energy industry is suffering from the same shortage of skilled information security staff as all other organizations. Many organizations have resorted to “home grown” information security expertise. While many of these staff are committed, talented, and knowledgeable people, unless large investments in training are made, these individuals can have significant gaps in their knowledge and experience. Even staff assigned traditional security functions (such as physical security) can suffer from inadequate training, particularly in small organizations.

3 LESSONS LEARNED

In addition to the best practices described in Section 2, the VRAP assessment teams have documented a number of lessons learned that correspond to each of the ten interrelated elements of the assessment methodology. These elements are: analyze the network architecture; assess the threat environment; conduct penetration testing; assess physical security; conduct a physical asset analysis; assess operations security; examine policies and procedures; conduct an impact analysis; assess infrastructure interdependencies; and conduct a risk characterization. In most cases, these lessons illustrate and highlight the best practices. They are presented to stimulate industry thinking towards more secure infrastructures as new threats and vulnerabilities evolve and as old threats and vulnerabilities resurface.

3.1 NETWORK ARCHITECTURE

- The corporate network of the modern utility has numerous external connections to public and private networks. Connections are used to communicate with customers and offer new electronic services such as online bill presentment and payment. Cyber security should be a primary concern of utilities operating in this new interconnected environment. An enterprise-wide IT security architecture should be developed.
- LAN/WAN networks and system architectures should be documented fully.
- The trend in IT is to outsource more and more functions. Cyber security, however, should remain as an enterprise function, and not become a contractor function.
- Logging and reporting should be enabled on routers and firewalls to gain a better understanding of remote systems and user access.
- Mission critical systems should be identified, and scanning should be performed on these systems. In addition, intrusion detection should be used to detect both internal and external intrusions into critical network systems. Additional layers of security should be included with critical systems (e.g., SCADA systems).

3.2 THREAT ENVIRONMENT

- Disenchanted current and discharged employees pose a significant threat to utilities.
- Criminal threats need to be considered (both organized crime and white-collar crime).
- Background investigations for new hires and periodic updates for current employees can assist in avoiding problems.

- Increased coordination with local law enforcement agencies can assist utilities in better understanding their threats.

3.3 PENETRATION TESTING

- Sensitive and confidential documents should not be placed on websites. Appropriate document review, classification, and access controls should be implemented. This also applies to documents and other information that is found in newsgroups, media sites, and other linked sites.
- Security measures such as traffic filtering, authorized controls, encryption and access controls, minimizing or disabling of unnecessary services and commands, minimizing banner information, and email filtering and virus control should be implemented.

3.4 PHYSICAL SECURITY

- A formal physical security program is essential. Such a program should include listing critical assets, developing a mission statement, defining threats, defining acceptable risks, and applying a vulnerability assessment methodology.
- A formal process for accessing relevant threat information and for contacting the proper law enforcement agencies should be instituted (if it does not already exist) and reviewed and updated on a regular basis. Industry needs to work with government to obtain security clearances for appropriate personnel.
- Appropriate security measures (e.g., access controls, barriers, badges, intrusion detection devices, alarm reporting and display, closed circuit television cameras, communication equipment, lighting, and security officers) should be implemented.
- Top management support is critical in ensuring a successful security program.
- Security training programs should be formalized.
- Procedures for escorting contractors into sensitive areas should be enhanced.
- Security should be incorporated in the company goals as well as in its corporate culture.

3.5 PHYSICAL ASSET ANALYSIS

- Capital expenditures for physical security should be compared to other capital expenditures to ensure proper levels of investment.

- Companies should compare their operating procedures with best practices and procedures used by other industry members to ensure efficiency, reliability, and security.

3.6 OPERATIONS SECURITY

- A five-step program of identifying critical assets, analyzing threats, analyzing indicators and vulnerabilities, assessing risk, and applying appropriate countermeasures should be implemented to enhance the security of a company's sensitive assets.
- The foundation for security is well-informed employees acting responsibly.
- A formal review process should be established for all information released to the public, particularly through the company's web site. A periodic review of "public" information should be performed to audit performance.
- A utility should be particularly careful about the loss of sensitive information to the press or competitors. Information available on personnel (especially executives) should be minimized.
- Security training and awareness should be provided to all employees on a regular basis.
- At a minimum, an annual audit of overall security should be conducted.

3.7 POLICIES AND PROCEDURES

- Formalized policies and procedures provide a foundation for achieving the desired level of security.
- Security policies and procedures need to be promulgated and integrated throughout the organization. Inconsistencies, confusion, and ultimately security gaps can result if business units or sub-organizational groups establish their own policies and procedures.
- Awareness training and education should include security policies and procedures.

3.8 IMPACT ANALYSIS

- Estimates of the potential consequences, including economic implications, of not mitigating identified vulnerabilities or addressing security concerns are necessary in order to effectively apply risk management approaches to evaluate mitigation and security recommendations.
- Outages resulting from a security failure(s) can lead to degradation of company reputation and loss of business in a competitive marketplace.

3.9 INFRASTRUCTURE INTERDEPENDENCIES

- Interdependencies among the infrastructures must be thoroughly investigated because they can create subtle interactions and feedback mechanisms that often lead to unintended behaviors and consequences. Problems in one infrastructure can cascade to other infrastructures.
- Interdependencies increase the complexity of the infrastructures and introduce additional vulnerabilities.
- Interdependencies among the infrastructures vary significantly in scale and complexity, and they also typically involve many system components. The process of identifying and analyzing these linkages requires a detailed understanding of how the components of each infrastructure and their associated functions or activities depend on, or are supported by, each of the other infrastructures.
- Contingency and response plans need to be evaluated from an infrastructure interdependencies perspective and coordination with other infrastructure providers needs to be enhanced.

3.10 RISK CHARACTERIZATION

- A more complete understanding of risk and risk management, as well as more effective risk communication, is needed at all levels of management.
- A risk management process needs to address the costs, benefits, and uncertainties associated with security and vulnerability mitigation recommendations. Such information will aid in establishing priorities and developing a defensible plan of action.
- The risk management process for addressing security concerns should be integrated into the corporate risk management process.

4 SUMMARY

The initial lessons learned, best practices, and observations presented in this report are intended to highlight key issues relating to the protection of the nation's energy infrastructures, and to stimulate action where appropriate. The information was assembled as part of the Department's VRAP initiative to help energy-sector organizations identify and understand the threats to and vulnerabilities (physical and cyber) of their infrastructures. Additional lessons learned and best practices are being captured and documented by the national laboratory team as part of the ongoing VRAP assessment program, and this draft report will be periodically expanded and enhanced to disseminate relevant information.

On the basis of the eleven assessments that have been conducted, it is clear that comprehensive vulnerability assessments can play a major role in helping energy organizations identify and address risks. It is also clear that such assessments should be conducted on a regular basis to identify new vulnerabilities that may have emerged as a result of the changing threat environment and efforts by organizations to evolve in the competitive marketplace.

The energy industry is not alone in facing these risks. Many of the same vulnerabilities would likely be identified in the other critical infrastructures (e.g., water supply systems, telecommunications, transportation, banking and finance, and emergency and government services). Nevertheless, the industry as a whole would benefit from more concerted attention to common vulnerabilities, particularly those that cross enterprise boundaries. This includes addressing interdependencies with the other critical infrastructures, which adds a whole new dimension to the risk equation. The development and application of risk management methodologies and tools that explicitly incorporate security should be a high priority.

Testimony
Before the Kansas Senate Utilities Committee
Hearing on House Bill 2037
Recovery of Certain Costs by Utilities
March 17, 2003

Michael E. Bier
Director, Engineering & Asset Management
Kansas City Power & Light

Kansas City Power & Light appreciates the opportunity to submit this testimony on House Bill 2037. My testimony will address Section 1 of the bill, regarding recovery of right-of-way fees and other cost imposed upon utilities by the municipalities they serve.

We respect the processes that Kansas municipalities may choose to govern or manage right-of way use within their respective city limits. Furthermore, we respect the right of cities and towns within our service territory to assess reasonable charges and fees for certain types of utility operations notwithstanding that KCP&L already pays annual franchise fees ranging from approximately three to ten percent in the 43 Kansas municipalities that we serve. In addition to higher assessed fees, policies and requirements imposed by a municipality can significantly increase a utility's cost.

We believe that law passed last year is a fair solution for allowing recovery of additional costs incurred by a public utility due to actions of a city's governing body. The law also allows the municipalities to recover actual costs beyond those covered in established franchise fees but encourages restraint in using increasing fees and other requirements as a revenue-producer for the municipality's general fund.

As originally introduced, H. 2037 removed the sunset provision entirely, but was amended in the House Utilities Committee to be extended only one year. We contend that the law is working, and ask that the provisions established last year be enacted permanently, and that a scheduled expiration date be eliminated from the law.

We continue to observe signs of interest by cities in using the rights of way as revenue-producing assets *and, in effect, using the utilities as their tax collectors*. The pressures on local budgets will only increase this threat. Obviously, increased fees expose utilities to additional cost pressures that further add to the challenges of maintaining rate stability.

More importantly, without the law these costs ultimately would be incorporated into the general rate structure for all customers, meaning that customers living outside of such municipalities may be asked to bear a portion of these fees. We feel that such a scenario is inherently unfair.

The activity that caused the utilities to ask for this legislation last year has waned, and we have yet to use the cost recovery mechanism. Again, we contend that is because the law has worked by having a deterrent effect on collecting tax revenue through fees imposed on utilities. Attached is an example of fees increases adopted last fall that will go into effect in May just over the state line in Kansas City, Missouri. This table is for lane closure fees – not a cost-based fee -- and shows some increases of more than 300 percent.

We encourage you to vote in favor of H 2037, and also consider completely repealing the sunset date in Section 1. Thank you for allowing us to submit testimony on this important bill.

Table Comparing Fees for Closure Permits

Example	Existing	ORD # 011729 25-Feb-02 Draft	ORD # 011729 14-Mar-02 Draft	ORD # 011729 28-Mar-02 Draft	Proposed Fee Schedule 22-May-02	Increase From Existing
1	\$45.00	\$381.30	\$202.50	\$162.00	\$200.00	344%
2	\$50.00	\$247.82	\$228.14	\$228.14	\$200.00	300%
3	\$50.00	\$74.84	\$63.34	\$62.13	\$100.00	100%
4	\$3,165.00	\$28,636.80	\$13,211.90	\$9,715.20	\$3,980.00	26%
5	\$20,886.00	\$52,411.13	\$28,032.66	\$25,293.49	\$26,202.00	25%
6	\$440.00	\$6,110.22	\$3,195.59	\$2,685.43	\$1,420.00	223%

- #1 Closure of one lane and adjacent walk of 10th St. between McGee and Oak for 10 days.
- #2 Closure of residential street for 3 days.
- #3 Closure of northbound lanes and adjacent walk of Grand between 10th and 11th on a weekend for 1 day.
- #4 Closure of north curb lane and adjacent walk of 13th street between Broadway and Washington for 730 days.
- #5 Oak St. Garage. 3 west lanes of Oak and adjacent walk. South curb lane and adjacent walk of 11th and North curb lane and adjacent walk of 12th, for 557 days.
- #6 Closure of the east curb lane and adjacent walk of Grand south of 12th & the south curb lane of 12th and adjacent walk east of Grand, for 185 days.

Substitute for SENATE BILL No. 545

AN ACT relating to public utilities; concerning public right-of-way and certain fees and costs; providing for recovery of certain costs of security measures of certain public utilities.

Be it enacted by the Legislature of the State of Kansas:

Section 1. As used in sections 1 and 2, and amendments thereto:

(a) "Public right-of-way" means only the area of real property in which the city has a dedicated or acquired right-of-way interest in the real property. It shall include the area on, below or above the present and future streets, alleys, avenues, roads, highways, parkways or boulevards dedicated or acquired as right-of-way. The term does not include the easements obtained by utilities or private easements in platted subdivisions or tracts.

(b) "Public utility" means all public utilities as defined in K.S.A. 66-104, and amendments thereto, except that it does not include any public utilities included in the definitions set forth in K.S.A. 66-1,187, and amendments thereto.

Sec. 2. (a) Without prejudice to a public utility's other rights and authorities, a public utility which is assessed by a city and collects and remits fees associated with the utility's use, occupancy or maintenance of such utility's facilities in the public right-of-way may file a tariff with the state corporation commission to add to such utility's end-user customer's bill, statement or invoice a surcharge equal to the pro rata share of any such fees.

(b) Costs which are incurred by a public utility in excess of those normal and reasonable costs incurred by a public utility applying good utility practices due to actions of a city's governing body may file a tariff with the state corporation commission to add to the bill, statement or invoice of each end-user customer located within such city through a surcharge equal to a pro rata share of such costs.

(c) For purposes of this section and section 2, and amendments thereto, costs shall not include expenses specifically covered by any other cost recovery mechanism in existence as of April 1, 2002, including but not limited to franchise fees and relocation expenses.

(d) The fees and costs incurred by the utility identified in subsections (a) and (b) in excess of the amount included in the utility's existing rates shall be subject to review by the state corporation commission upon filing for recovery of the costs in a surcharge. Upon a finding by the commission that (1) the fees included for recovery in such surcharge were required to be paid by the utility as the result of action of the governing body of a city, (2) the costs were incurred as a result of action of the governing body of such city, (3) such costs were reasonably incurred to meet the requirements imposed by the governing body of such city and (4) the surcharge is applied to bills in a reasonable manner and is calculated to substantially collect the increase in fees and costs charged on the books and records of the utility, or reduce any existing surcharge based upon a decrease in fees and costs incurred on the books and records of the utility, the commission shall approve such tariffs within 30 days of the filing. If the commission determines that the surcharge is not applied to bills in a reasonable manner, the costs or portions thereof do not meet the above requirements or that the calculation is not adequately supported by the documentation provided in the filing, the commission, at its option, may either disapprove such tariff within 30 days of the filing and require re-submission by the utility, suspend the effective date of the tariff for an additional 60 days to receive appropriate documentation from the utility and/or modify such tariff in a manner that recovers in a reasonable manner the costs or portions thereof which meet the above requirements. Any over or under collection of the actual fees and costs charged to expense on the books of the utility shall be either credited or collected through the surcharge in subsequent periods. The establishment of a surcharge under this section shall not be deemed to be a rate increase for purposes of this act.

(e) Upon the filing of a tariff with the corporation commission pursuant to this act, the utility shall deliver to the affected city a complete copy of the filing. Such copy shall be delivered within 10 days of the filing with the corporation commission.

Sec. 3. (a) Section 1, and amendments thereto, shall affect only such costs and fees which are incurred between April 1, 2002, and June 30, 2003.

(b) The provisions of this section and sections 1 and 2, and amendments thereto, shall expire on June 30, 2003.

Sec. 4. (a) As used in this section:

(1) "Electric public utility" means any electric public utility, as defined in K.S.A. 66-101a, and amendments thereto.

(2) "Natural gas public utility" means any natural gas public utility, as defined in K.S.A. 66-1,200, and amendments thereto.

(b) On and after July 1, 2002, the state corporation commission, upon application and request, shall authorize electric public utilities and natural gas public utilities to recover the utility's prudent expenditures for security measures reasonably required to protect the utility's electric generation and transmission assets or natural gas production and transportation assets by an adjustment to the utility's customers' bills. The application and request shall be subject to such procedures and conditions, including review, in an expedited manner, of the prudence of the expenditures and the reasonableness of the measures, as the commission deems appropriate. Such application and request shall be confidential and subject to protective order of the commission.

(c) The provisions of this section shall expire on July 1, 2004.

Sec. 5. This act shall take effect and be in force from and after its publication in the Kansas register.

I hereby certify that the above BILL originated in the SENATE, and passed that body

SENATE concurred in _____
HOUSE amendments _____

President of the Senate.

Secretary of the Senate.

Passed the HOUSE _____
as amended _____

Speaker of the House.

Chief Clerk of the House.

APPROVED _____

Governor.

Testimony of
Robert Nichols, Security Consultant
Aquila, Inc.
In Support of House Bills 2037 & 2374

Chairman and Members of the Committee:

My name is Robert Nichols and I am a Security Consultant for Aquila, Inc. formerly UtiliCorp United, Inc., WestPlains Energy, Peoples Natural Gas and Kansas Public Service. Aquila serves over 165,000 natural gas and electric customers in 154 cities and towns in central and western Kansas. I appear before you today in support of House Bills 2037 & 2374 that would aid in the protection of the critical infrastructures within Kansas for the following reasons:

1. Aquila supports of House Bill 2037, which would repeal the sunset provision on security measures, we believe that the current political, regulatory and threat environment will require more security enhancements that cannot be completed within the present sunset provision. Specific examples of this intent include:
 - a. Tom Ridge's recent declaration from the Department of Homeland Security (01/24/03), that states more than 80 percent of the nation's critical infrastructure is owned and operated by the private sector, and an attack against a business or industry is an attack against the U.S.
 - b. FERC Hearing, Washington, D.C. (01/06/03), in which they comment that current security requirements are not "best practices" and they intend to establish more security standards.
 - c. The potential for conflict with Iraq and/or other countries will create a greater threat to U.S. Critical Infrastructure from both domestic and international terrorist organizations, which will require greater security-related expenditures.
2. Aquila acknowledges beyond the probability of further enhancements, that we and many other utilities are still deploying security enhancements needed to meet current regulatory and industry guidelines, and that these efforts will likely go beyond the initial sunset provision.
3. Additionally, the Kansas Corporation Commission ("KCC" or "Commission") just recently, on January 31, 2003, established a process by which the utilities are allowed to request and seek recovery of their homeland security-related costs and capital expenditures. This delay has thus far impacted the utilities ability to meet the sunset provision.
4. In addressing our support of House Bill No. 2374, it should be noted that the bill does not ask the Commission to forego its responsibilities to the citizens of Kansas, nor does it prohibit the Commission from meeting that responsibility. Rather, House Bill No. 2374, sets forth clear mandates that sufficient information be presented to the Commission for its decision. House Bill 2374 simply goes the

extra step of protecting that information against unwarranted release. Since it is a known, proven fact that enemies of the U.S. and terrorists, routinely use open source information and the Freedom of Information Act to obtain large quantities of published government documents and information that has been damaging to the U.S.

5. In its recent January 31, 2003 order, the Commission created several instances where information can be released to the general public. Specifically, the release of information to the Citizens' Utility Ratepayer Board ("CURB"), without a protective order, creates an immediate opportunity for release of information already recognized by both the Commission and this legislature, as being confidential and potentially harmful to the security of the Kansas infrastructure. Only after extensive debate has the Commission stated in its recent Order on Reconsideration, dated March 7, 2003, that it would issue such protective order in advance of release. We feel it is prudent to provide regulatory protection so that such specific security information will be automatically protected without relying on specific, additional steps.
6. Similarly, the identification of the recovery periods, amounts and locations of security enhancements approved by the Commission provides information, when used with other data, that can potentially identify those facilities deemed critical, and those companies actively protecting their facilities. Such information, when used with other data, can provide valuable information in identifying weaknesses or key targets of opportunity.
7. While the Commission has recently issued its order on how to apply for such cost recovery, the Commission has repeatedly stated that there is no prudent reason for expedited recovery of these security enhancements, as the present system of recovery adequately addresses the recovery process.

Aquila feels that the Commission has failed to note that there is a difference in the type and nature of these costs, as compared to normal recovery processes. This difference is in the nature, durability and "usable" lifetime of security products. The Commission routinely addresses capital equipment and construction that has usable lifetimes varying from 9 years to several decades, as these are more permanent structures and equipment. Unfortunately, the usable lifetime for security components are measured from a few days or weeks (such as with cyber security processes relating to patches, virus protection, intrusion protection and detection systems) to no more than a few years (e.g. digital video recording, and card access systems and badges that normally last no more than 3 to 5 years).

The reasons for this relatively short usable lifetime for security components and processes are simple. These systems are not designed, nor built to withstand environmental and industrial applications normally found at utility sites. However, more importantly, is the fact that once security systems are established, these systems are then probed and examined by the enemies of the U.S. or persons

with criminal intent, actively seeking and identifying methods to neutralize the security systems. Once a weakness or vulnerability is identified, the security system must then be enhanced and/or new countermeasures developed and deployed to further protect the facility. It is this on-going “protect-probe-penetrate-protect” cycle that creates such short usable lifetimes.

When considering the industrial nature of utility facilities, the vulnerability probing and corrective actions needed, the potential for losses stemming from deliberate attacks on these security systems, and needed technical advances/changes, delaying recovery of costs for these systems, especially during the present time, is not prudent. Such delays, further negatively financially impact the utility companies and the Kansas consumers, who will eventually be paying for multiple security systems, at the same time, from which they will not derive the benefit.

In consideration of the information provided above, Aquila requests that the Kansas Legislature adopt House Bills 2037 and 2374. I will now stand for any questions from the committee, or will remain for committee questions at a later time.

Respectfully Submitted:

Robert Nichols
Security Consultant
Aquila Inc



Kansas Electric Power Cooperative, Inc.

Testimony on House Bill 2037 Senate Utilities Committee – March 17, 2003

*Bruce Graham, Vice President of Member Services and External Affairs
Kansas Electric Power Cooperative, Inc. (KEPCo)*

Kansas Electric Power Cooperative, Inc. (KEPCo) supports House Bill 2037. This bill would remove the sunset provision on a law approved in 2002 (Sub SB 545) that was designed to expedite the recovery of reasonable and prudent costs to improve security at Kansas generation, transmission and other critical utility facilities. The bill also authorized utilities to recover increasing costs imposed by municipalities without the need for a rate proceeding.

Many jurisdictional utilities in Kansas have recently undergone a comprehensive rate review. KEPCo, for example, completed a full rate case in February 2002 but the rate case was developed and filed in the first part of 2001. Since that time, homeland security mandates have required and will continue to require significant unanticipated investment in generation and transmission safety. New requirements are being implemented by the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, National Electric Reliability Council and other organizations. These voluntary and mandatory measures are likely to become part of our standard operations and such expenditures will necessarily be considered in a subsequent rate filing.

Parties understood that before a security cost adjustment would be enacted under the provisions of Sub SB 545, the filing would be subject to some level of review by the KCC. In fact, in an order dated March 7, 2003, the KCC completed the rules and regulations for that evaluation. Consequently, without the passage of HB 2037, by the time a utility prepares the necessary documents to file and ultimately receive a regulatory decision, there may be less than a year before the authority to recover these expenses evaporates. Furthermore, the KCC order indicates that it intends to fully review the utility request before allowing the recovery of demonstrated and required incremental security cost increases. Therefore, KCC oversight renders a security cost sunset provision unnecessary.

Thank you for the opportunity to submit these comments in support of HB 2037.

KEPCo is a generation and transmission utility that provides wholesale electricity and other services to 19 rural distribution cooperatives with member/consumers spanning two-thirds of rural Kansas.

Senate Utilities
March 17, 2003
Attachment 5-1

Phone: 785.273.7010

Fax: 785.271.4888

www.kepco.org

P.O. Box 4877

Topeka, KS 66604-0877

600 Corporate View

Topeka, KS 66615

Citizens' Utility Ratepayer Board

Board Members:

Gene Merry, Chair
A.W. Dirks, Vice-Chair
Frank Weimer, Member
Francis X. Thorne, Member
Nancy Wilkens, Member
David Springe, Consumer Counsel



State of Kansas

Kathleen Sebelius, Governor

1500 S.W. Arrowhead Road
Topeka, Kansas 66604-4027
Phone: (785) 271-3200
Fax: (785) 271-3116

SENATE UTILITIES COMMITTEE H.B. 2037

Testimony on Behalf of the Citizens' Utility Ratepayer Board
By David Springe, Consumer Counsel
March 17, 2003

Chairman Clark and members of the committee:

Thank you for this opportunity to appear before you today and offer testimony on H.B. 2037. The Citizens' Utility Ratepayer Board is opposed to this bill for the following reasons:

While CURB does not favor the existing security cost recovery law as expressed in K.S.A. 66-1233, CURB respects that it is the law and is participating before the KCC in the process implementing the law. However, the existing law allowing utility companies to recover security costs through a surcharge on consumer bills will sunset on July 1, 2004.

H.B. 2037 (at page 1, line 43) removes the existing sunset provision in K.S.A. 66-1233, making the recovery of utility security costs through consumer surcharges a continuing regulatory obligation. CURB would prefer that the sunset provision remain in the existing law, that this law be allowed to sunset and that the law be allowed to go away.

In the alternative, if the Committee believes that the existing sunset provision results in this law ending too soon, CURB would prefer a short extension of the sunset rather than an outright removal of the sunset provision.

CURB would also note that H.B. 2374 also modifies K.S.A. 66-1233. CURB is strongly opposed to H.B. 2374. If H.B. 2374 does become law, it would further strengthen CURB's opinion that K.S.A. 66-1233 should sunset and end, and would further strengthen CURB's opposition to H.B. 2037.

Senate Utilities
March 17, 2003
Attachment 6-1

TESTIMONY BEFORE THE SENATE UTILITIES COMMITTEE
ON HB 2374
BY
REP. CARL KREHBIEL

I am Representative Carl Krehbiel and I serve as Vice Chairman of the House Utilities Committee and the House Select Committee on Kansas Security and I appear as a proponent of HB 2374. The genesis of HB 2374 was actually documents captured by troops in Afghanistan and also some subsequent information developed by U.S. law enforcement and intelligence authorities in this country regarding the evaluation by El Quida of the possibility of striking electric utilities distribution systems as a means of conducting another economic terrorism attack on the United States and also the results of what could be called a command post exercise conducted in the American Northwest that showed what devastating results would occur if terrorists were successful in taking out certain critical components of the electrical distribution system. And the Legislature looked at what it would mean to the State of Kansas for our economy and state revenues. If there were to be a prolonged shutdown of electrical distribution system in significant parts of the state, the information is pretty scary.

As a result of this the legislature passed last year Substitute for Senate Bill 545 which basically told the Kansas Corporation Commission to provide for expedited cost of recovery for expenditures that the electric utilities make for security purposes and the intent of this bill was to incent the utilities to go ahead and make investments in equipment, security procedures, measures, etc. and do it expeditiously. There would be no business case for doing this if utilities following the standard rate of return regulatory procedures and waited until they had their next rate case and certainly the amount of money we are talking about here would not be enough to justify a utility going in with a request for a rate case which is a very burdensome and time consuming and expensive procedure. So that was the intent behind Sub for Senate Bill 545.

The Commission issued an order on January 31 in response to the utilities requesting procedures for requesting this cost recovery and in essence the Commission disregarded what the Legislature had told them to do in Sub. For SB 545. One thing that was quite striking about this order, I thought the Legislature had made it very clear that we were concerned about this unique set of circumstances and the threat we would face and that we wanted action taken. In response the Commission said they wouldn't do that because to do so would be "contrary to accepted regulatory principles". There are four separate instances in this order, three of them in one paragraph where the Commission basically says "no we are not going to do that because that's not standard operating procedures and that's not standard regulatory principles".

After seeing the January 31 letter, Chairman Holmes appointed a subcommittee to consider further legislation that would do what the legislature had intended with Sub for SB 545 and the product of that sub committee is HB 2374. That subcommittee also sent a letter to the Commission in which we outlined specifically their points in their January 31 order that we disagreed with. In addition a couple of utilities filed a request for petition of reconsideration with the Commission for that January 31 order. The commission came out with an order of reconsideration on March 7 and they said in essence that they didn't see any need to do anything

different. So not only are they ignoring the law and not only are they ignoring the petition for reconsideration, they basically told us what we could do with the letter from the nine or ten legislators and the letter from the subcommittee. That is the genesis of HB 2374.

HB 2374 cites the threat of terrorism, the importance of utilities to the state and the need for extraordinary regulatory treatment to enable to government to perform its most basic function - to provide for the security of the citizens and protecting the public welfare. It tells KCC to follow certain procedures when considering cost recovery by utilities - cost of security measures - and it is to be expedited in order to incent the utilities to upgrade their security. We do not want to make it specifically known which utility is spending how much money. We don't want any potential terrorist to know that and be able to identify which utility to attack and consequently confidentiality of information is provided. However, there will be a full review possible by the Commission with participation by CURB which is explicitly mentioned in this legislation and the Commission is to review any expenditures the utilities come in with - first of all to make sure they are security related. We aren't giving utilities a blank check to spend money on anything and everything and claim its for security and secondly the Commission is determine whether the investments are prudent.

Shutting down electrical service in significant parts of Kansas for weeks or even months would ~~be~~ obviously have very grave consequences. There is no business case for utilities to make investments to buy critical pieces of equipment perhaps on a pool basis and set them aside and have them just sitting there to come in, in the event of an attack. That is the intent of this bill to provide them the incentive to spend money on security precautions by expediting the cost recovery. There were two main objections raised in the House when we debated this bill on the floor. The first was an assertion that this represented an automatic pass through of costs from the utilities to their customers. I don't think that is the case because the bill explicitly provides for KCC review with CURB participation in order to establish the expenditures are in fact security related and that they are prudent. The second objection raised was with regard to the confidentiality of the information and specifically that there would be no line item on the customer's bill to identify an extra charge for security measures. My response to that isIt is a good thing if it gets out to the world that Kansas has passed this legislation; it is a good thing that the utilities let it be know that they are taking advantage of this legislation in expending money on security but that's where we need to draw the line. My experience for 20 years as a military intelligence analyst and I know very well how bits and pieces of information and put them together to solve the puzzle. A separate line item on utility bills that identified how much money was being spent, would be a very useful tool for anyone trying to identify a soft target. It would identify which utilities are or are not spending money on security. It is very important to have that confidentiality. This is by no means unprecedented as the utilities are doing it now by listing several items under customer charge or energy charge on their bills. How much money are we really talking about that the customer would pay - low end would be about \$1.50 per year or it might go to about \$2.50 a year as a high. This is form of insurance.

I stand for questions.

**Testimony before the
Senate Utilities Committee
By
Dick Rohlfs, Director Retail Rates
Westar Energy
March 17, 2003**

Chairman Clark and members of the committee, I am Dick Rohlfs, Director Retail Rates for Westar Energy.

Westar Energy supports House Bill 2374. Last year the Legislature recognized the need for utilities to increase security and be able to recover related costs in a timely fashion. While a year and a half has passed since the tragic attacks of September 11, 2001, it remains clear that complacency has no place in protecting our state's infrastructure. Westar Energy, like other utilities, must maintain and improve the security of our infrastructure to ensure reliable electric energy for Kansans.

H.B. 2374 maintains and improves upon two important safeguards that the Legislature approved last year. The first is confidentiality. Any security steps we take will be less effective if the cost or other information about the improved security measures is released. Potential attackers could analyze information filed with the Kansas Corporation Commission to exploit weaknesses if that information is made public. The second is oversight. H.B. 2374 assures that any filing will be for enhanced security measures and the costs are reasonable, prudent and/or required by regulatory agencies.

H.B. 2374 does more than protect utilities. It protects Kansans. I encourage you to support H.B. 2374.

Senate Utilities
March 17, 2003
Attachment 8-1

Testimony of Lawrence Dolci
Director of Resource Protection
Great Plains Energy Services Company
Before the
Kansas Senate Utilities Committee In Support of House Bill 2374 Relating to Recovery of
Certain Utility Costs
March 17, 2003

I appreciate the opportunity to address the Senate Utilities Committee on the issue of cost recovery for security improvements in the electrical industry. Great Plains Energy Company, GPE, and its company, Kansas City Power & Light Company, KCP&L, support the passage of HB 2374. The passage of this bill will improve the security of electric utilities within the state and assist them in providing reliable and low cost service.

HB-2374 would enact the Kansas Energy Security Act, which would direct the Kansas Corporation Commission to adopt certain procedures to implement KSA 66-1233 (Sub SB 545) that became law last legislative session. Sub SB 545 was passed in response to the events of September 11, 2001. Its purpose was to encourage gas and electric companies to invest in security infrastructure to protect their facilities by providing an expedited means of recovering reasonable and prudent security costs incurred since September 11, 2001.

Recent orders of the Kansas Corporation Commission, KCC, including its orders of January 31, 2003 and March 7, 2003 are not consistent with the legislative intent of Sub SB 545. Passage of SB 2374 would ensure the original intent of Sub SB 545 is followed by the KCC.

The private sector and government, including the military establishment of the U.S. are highly dependent on infrastructures like power. These systems are owned and operated by the private

sector that is responsible for their protection. Warnings from the FBI, Secret Service and other intelligence and law enforcement agencies state this infrastructure is a top potential target of terrorists, domestic and international, and hostile nation states. Terrorists in the Philippines, Afghanistan, Europe and Columbia attack electrical facilities frequently.

In the aftermath of the attacks of September 11, 2001, KCP&L and other utilities increased their security in anticipation of more attacks. The increase in security was consistent with warnings issued by federal law enforcement and intelligence agencies. Although security levels have been reduced from the immediate post September 11 levels, utilities are still operating at a higher level of security than prior to September 11th and there is no sign these levels will be reduced. The higher security posture has been expensive for utilities. In addition, a variety of industry and government organizations have issued new security guidelines, some voluntary, and some mandatory. Compliance with these guidelines will take years and cost millions.

Sub SB545 was intended to provide for an expedited, confidential process to ensure that reasonable and prudent costs related to security were recovered. It was not intended to require a full review of a utility's financial position with its lengthy timetable and associated costs.

Interpretations of Sub SB545 by the Kansas Corporation Commission are not consistent with the legislative intent of Sub SB545 and would be corrected by the passage of HB 2374.

Specifically HB 2374 requires the KCC to:

- Protect the confidentiality of security information submitted by utilities.
- Issue protective orders to protect confidentiality should CURB intervene.

- Create procedures consistent with federal rules on release of information.
- Prevent security cost information from appearing on bills.
- Expedite the review of security related filings.
- Review security related items to ensure they enhance security and are prudent.
- Allow recovery of capital items over no more than 1/3 of their usable life.

The adoption of these procedures through the passage of HB 2374 would not only allow the recovery of security costs in an expedited manner but also ensure that confidential information is protected. The interests of ratepayers would be protected under HB 2374 by the KCC staff who would have full access to all data related to the request for recovery and the CURB who would be provided with information subject to protective orders.

The January 31, 2003 and March 7, 2003 orders of the KCC do not recognize the need to protect the amounts spent on security by each utility from public disclosure. As noted above, the interests of the public will be protected by the complete review by KCC staff of the expenditures and in some cases review by the CURB. Disclosure of amounts spent could allow a terrorist to target utilities that have spent the least on security.

HB 2374 provides for accelerated depreciation of security costs that would allow recovery of capital security expenditures over a period equal to not more than 1/3 the usable lifetime of the capital investment. This concept, which would encourage utilities to increase security, was rejected by the KCC in its January 31, 2003 and March 7, 2003 orders.

Passage of HB 2374 will encourage utilities to protect the vital services provided to the citizens of Kansas while protecting the interests of ratepayers. I urge the Senate to pass this bill.

9-4

**BEFORE THE SENATE UTILITIES COMMITTEE
PRESENTATION OF THE
KANSAS CORPORATION COMMISSION
ON HB 2374**

March 17, 2003

Thank you, Chairman, and members of the Committee. I am Larry Holloway, Chief of Energy Operations for the Kansas Corporation Commission. I appreciate the opportunity to be here today to testify on behalf of the Commission on HB 2374.

The purpose of my testimony is to provide information and perspective on HB 2374. This legislation proposes to expand upon the security measures passed in last year's legislative session by prescribing practices and procedures by which the Commission is required to review expenses sought to be collected under K.S.A. 66-1233. In short, this legislation: (1) seeks to expand on the confidentiality of requests for recovery of security-related expenses under K.S.A. 66-1233 to include not merely the application and request, but also the amount of recovery requested, the amount of recovery allowed, the method of cost recovery and the method of cost recovery allowed; (2) once a request has been reviewed, passes the allowed cost onto ratepayers' bills in an unidentifiable manner; (3) sets out the time period over which the cost may be recovered; and (4) indicates that the Commission should ignore standard regulatory principles in carrying out the intent of this legislation. For the below reasons, the Commission does not support HB 2374.

First, the Commission believes this legislation represents poor public policy relating to the confidential treatment of documents filed with state agencies. The intent of the Kansas Open Records Act is to ensure that all documents, which legitimately can be open to public inspection, should be open to public inspection. The Commission has consistently espoused the philosophy

Senate Utilities
March 17, 2003
Attachment 10-1

that its regulatory function should be conducted in the open. However, even with that general policy in place, the Commission is mindful that at times, utilities, the Commission's Staff and interveners might need the protection afforded by confidential treatment of certain documents. In those legitimate instances, the Commission has well-established policies and procedures in place to protect confidential information.

Second, the Commission is concerned about fundamental due process issues raised by this legislation. This legislation only allows the Citizens' Utility Ratepayer Board (CURB) the right to participate, without provision for participation by other legitimate interveners. Legitimate interveners should be allowed to participate, subject, of course, to the provisions of the Commission's standard Protective Order and non-disclosure agreements.

Third, the Commission believes that certain customers will be able to calculate the incremental increase related to the recovery of security costs regardless of whether specifically identified on the bill. A customer need only compare his monthly billing statements to detect a difference in his charge per kilowatt-hour or question an unidentified line item imposing a surcharge.

Fourth, with regard to the recovery period of the security-related capital expenditures contemplated in this legislation, the Commission suggests that it be allowed to use its discretion, recognizing that like expenses might be recovered over a different time period than "1/3 of the usable lifetime of the capital investment" or that it might be appropriate to allow recovery of these critical, extraordinary costs over even a shorter time period. It is important to recognize that recovery of capital investment over an appropriate amount of time is key to fair and equitable treatment between generations of ratepayers. For example, in terms of equity and fairness, there is no difference between asking a specific generation of ratepayers to pay for a

utility's investment that benefits other generations of ratepayers, and asking one class of customers to pay the entire cost of an investment that benefits all customers. Premature recovery of a utility's capital investment is discriminatory treatment between generations of ratepayers. The Commission fully supports utility recovery on and of its prudent and needed security investments; the only issue is that of equitable timing of the recovery.

Finally, the Commission acknowledges that this legislation represents a policy decision of the Legislature in reaction to the extraordinary events of September 11, 2001; however, the Commission believes that there are practical implications that make carrying out the mandates of this legislation difficult.

Citizens' Utility Ratepayer Board

Board Members:

Gene Merry, Chair
A.W. Dirks, Vice-Chair
Frank Weimer, Member
Francis X. Thorne, Member
Nancy Wilkens, Member
David Springe, Consumer Counsel



State of Kansas
Kathleen Sebelius, Governor

1500 S.W. Arrowhead Road
Topeka, Kansas 66604-4027
Phone: (785) 271-3200
Fax: (785) 271-3116

SENATE UTILITIES COMMITTEE H.B. 2374

Testimony on Behalf of the Citizens' Utility Ratepayer Board
By David Springe, Consumer Counsel
March 17, 2003

Chairman Clark and members of the committee:

Thank you for this opportunity to appear before you today and offer testimony on H.B. 2374. The Citizens' Utility Ratepayer Board is opposed to this bill for the following reasons:

While CURB does not favor the existing security cost recovery law as expressed in K.S.A. 66-1233, CURB respects that it is the law and is participating in the process before the KCC. CURB does want to make clear to the Committee its position, as filed at the Kansas Corporation Commission, as related to recovery of security costs.

- CURB does believe that residential and small commercial ratepayers are concerned about the safety and security of the utility infrastructure in the state.
- Residential and small commercial customers are likely willing to pay some fee for prudently incurred necessary security expenditures.
- CURB strongly believes that residential and small commercial customers expect that any security fee or charge placed on a utility bill has been thoroughly reviewed by the Commission and found to be prudently incurred.
- CURB strongly believes that residential and small commercial customers expect that any security fee or charge placed in a utility bill will not be duplicative of charges that are already contained in base rates.
- CURB strongly believes that residential and small commercial customers expect that any security fee or charge that they are expected to pay is also being shared with all other utility system customers in the most equitable manner possible.

Senate Utilities
March 17, 2003
Attachment 11-1

However CURB is strongly opposed to what H.B. 2374 proposes to do. For the following three reasons, CURB believes that H.B. 2374 moves the existing law to a new unprecedented level that is not in the interest of Kansas utility consumers and should not be the policy of this State.

- The level of secrecy contained in Section 3 (a)(1). CURB does acknowledge that many elements of a utility's security plan are sensitive and should rightly be accorded confidential protections. CURB has no desire to advertise each and every aspect of a utility's plan to deal with security or how security measures are being implemented. However, secrecy must also be balanced against a consumers right to know why, and by how much utility rates are increasing. CURB does not believe that disclosing the name of the utility, the total amount of money the utility is requesting as a rate increase and the proposed method of recovery the utility is proposing represents information containing the type of specificity that warrants being withheld from the public. There is nothing inherently sensitive in this information. CURB believes that these three elements are the minimum information necessary to meet notice and due process requirements.
- Hiding the rate increase on consumer bills as required by Section 3 (a)(4). If it is the public policy of the State of Kansas that security costs are to be accorded extraordinary rate treatment, including expedited review and expedited recovery of capital expenditures, then this fact should be apparent to consumers when they view their utility bills.
- Expedited recovery of capital expenditures as required by Section 3 (a)(7). CURB believes that capital equipment expenditures for security should be recovered over a time period consistent with the recovery period of like capital equipment in normal rates. CURB understands that new security requirements force a utility to expend money that was not anticipated in the utility's last rate case. CURB also understands that a utility may not want to file a general rate case to get recovery of these security expenditures. The security surcharge in K.S.A. 66-1233 and in this bill allows a utility to begin recovery of, and begin receiving a return on, the expenditures made for security purposes. At the time of the utility's next rate case, the security related capital expenditures can be placed in base rates and the capital recovery will be consistent with other like capital equipment. This method of recovery is consistent with good ratemaking practices, will eliminate confusion over time as to the accounting accorded similar capital assets, will provide the utility with a return of and a return on its expenditures, and will protect consumers from the potential large rate increases caused by expedited recovery of capital expenditures.

11-2

If this bill does progress, CURB would offer the following suggestions:

- Add to Sec. 3(a)(4), “*and shall be added to all wholesale and retail rates and contracts.*” CURB cannot stress enough that this language must be added to this bill. CURB is concerned that as written, this bill will result in only tariff customers paying the security costs envisioned by K.S.A 66-1233 and this bill. If extraordinary circumstances dictate that security costs shall be recovered in a manner different than ordinarily applied in rate proceedings, it is not equitable that wholesale and retail customers that purchase utility service under a contract are able to escape these security charges. If it is the public policy of the State of Kansas to authorize extraordinary recovery of security costs, it must also be the public policy of the State of Kansas that all users of the utility system that benefit from the enhanced security pay an equitable portion of the costs, whether service is taken by tariff, or by contract and whether at the wholesale or retail level.
- Language on “Prudent expenditures” is inconsistent and vague. **In Section 3 (a)(6)**, the Commission shall deny any expenditure that the Commission determines “*is not prudent or is not for security measures*”. This language seems clear. However, **Section 3(b)** states that “*a determination by the Commission of the prudence of an expenditure for security measures shall not be based on standard regulatory principles of methods of recovery and shall take fully into account the findings as intent of the legislature as states in Section 2*”. The language in **Section 3 (b)** makes it virtually impossible to argue that any expenditure is not prudent if it is related to security. Arguably, the intent of the legislature expressed in Section 2 is to suspend normal regulatory procedures and allow the utilities to expend whatever is necessary to secure the system. Given that intent, how can anything ever be defined as not a prudent expenditure?
- **Section 3 (a)(2)**. While CURB appreciates the acknowledgement that CURB should be part of this process, and should have a standard protective order issued, CURB does not believe that it is necessary to put this language in statute. The Commission routinely issues protective orders in cases, and CURB certainly anticipates it will do so in security cost case. This language likely stems from the utilities concern about providing CURB security information without the restrictions of a protective order. While this concern is valid, and CURB certainly does not want this information in its possession without a protective order, this can be dealt with in a routine manner by the Commission by making the issuance of a protective order a standard procedure in security dockets. **This language can be left in the statute, but CURB does not believe it is necessary.**

**Utilities Committee
Kansas Senate
Written Testimony of Bruce Snead
March 17, 2003**

HB 2131

At Dr. Lee Allison's request, I have the privilege of serving on the External Committee of the State Energy Resources Coordinating Council, which assisted the Council regarding renewable energy and energy efficiency topics. Dr. Allison and the entire Council should be congratulated for accomplishing so much with incredibly limited time. Such a tight schedule inevitably made it likely that legislative action items might need additional refinement as you move forward with implementation. The changes that have been accomplished through the legislative process and amendments made to HB 2131 and committee additions have been very productive and have improved the bill.

I support the bill in its current form and believe it:

- Creates appropriate and comprehensive thermal energy efficiency design standards policy for the State of Kansas, for residential, industrial and commercial buildings. This will help keep future energy costs of building ownership and operation more affordable by guiding design and construction decisions with the most current approaches providing flexibility ⁱⁿ compliance, technologies and practices.
- Recognizes the work and unification of code setting authorities that has occurred since the last Kansas Legislature action in this arena and helps provide a comprehensive reference and maintains a flexible approach for municipalities in the code adoption process.
- Does not increase the cost to builders of meeting energy efficiency codes and guidelines or require them to do anything different than they are currently doing, other than provide information that they already have available about the residential structure, either upon request, or at the latest during contract negotiations.
- Increases the opportunity for consumers to access timely energy efficiency/building information critical to the operating costs, purchase price, contract negotiation decisions and ultimate affordability for what is the largest investment they may ever make, buying a home.

Senate Utilities
March 17, 2003
Attachment 12-1

I urge you to take positive action on this bill, as it represents a fair and appropriate update to the long term energy policy for the future building stock of Kansas, is beneficial for Kansas home buyers and fair to builders, and will help ensure the design and construction of buildings which will reduce demand for energy throughout their useful life. I would be happy to answer questions or respond to concerns the committee may have.

Bruce Snead

A handwritten signature in black ink, appearing to read "Bruce Snead". The signature is written in a cursive style with a large initial "B".

Member, External Committee, State Energy Resources Coordinating Council

Home

810 Pierre St.

Manhattan, KS 66502

785-537-7260 Home

785-532-4992 Work



KANSAS

CORPORATION COMMISSION

KATHLEEN SEBELIUS, GOVERNOR
JOHN WINE, CHAIR
CYNTHIA L. CLAUS, COMMISSIONER
BRIAN J. MOLINE, COMMISSIONER

**Utilities Committee
Kansas Senate
Written Testimony of the Kansas Corporation Commission Staff
February 17, 2003**

HB 2131

Chairman Clark and members of the Committee. I am Jim Ploger, manager of the Kansas Corporation Commission's Energy Programs Division.

I want to convey my appreciation for the leadership and work of the State Energy Resources Coordination Council (SERCC) and its Chair, Dr. Lee Allison, and Vice Chair, John Wine.

One of the three priorities selected by SERCC for the 2003 Kansas Legislative Session was to bring the State of Kansas into modern energy codes compliance. House Bill 2131, introduced by the Committee, is a good faith effort to do just that.

The KCC Energy Programs involvement in promoting progressive energy building codes and standards during the past several years has been routinely recognized by the United States Department of Energy's Building Energy Codes Program, administered by the Pacific Northwest National Laboratory in Richland, Washington.

As a result of this leadership, Kansas has received over a \$1 million dollars of federal aid during the past 6 years to help educate the building community and public on the value of energy efficient residential and commercial buildings. Dozens of workshops and hundreds of builders, engineers, architects, and building code officials during the past several years have benefited from our educational activities.

As in many areas in today's fast moving world, building codes and standards are also changing fast. The "state-of-the-art" energy codes is the 2003 International Energy Conservation Code, just off the press last month.

A number of Kansas jurisdictions have or are in the process of adopting the IECC as their guidelines for energy building codes.

As suggested by energy efficiency experts at Kansas State University here today, I encourage the passage of HB 2131 as amended that would adopt the IECC 2003 to make Kansas a leader in constructing efficient buildings.

Senate Utilities
March 17, 2003
Attachment 13-1

If the IECC is adopted, our office will be submitting a proposal in the next few weeks as part of the Department of Energy's "Special Projects" grants program. We will be requesting DOE funds to help us fund training and support for contractors, architects, engineers, code officials and others in the building community for the new International Energy Conservation Code.

Our office looks forward to our continuing role in providing leadership in the area of education and training of the citizens of Kansas in the art of constructing energy efficient buildings.

Thank you for your consideration.

13-²✶



**Utilities Committee
Kansas Senate
Written Testimony of Gene Meyer
March 17, 2003**

Engineering Extension
133 Ward Hall
Manhattan, KS 66506 -2508
785-532-6026
Fax: 785-532-6952
www.engext.ksu.edu/

RE: HB 2131

Chairman Clark and members of the Committee. I am Gene Meyer, Extension Mechanical Engineer with Engineering Extension of Kansas State University.

The State Energy Resources Coordination Council is to be applauded for what was accomplished, especially in the brief time available. Recognition of the role building energy performance and conservation plays in Kansas' energy future is insightful and welcome. Modernizing building energy codes, while not assuring high performance buildings, will help raise the minimum performance of new buildings while, reduce consumption of precious resources, delay construction of new power plants, and reducing associated emissions.

Kansas energy codes have evolved over the last several years. In 1997, the legislature adopted statues requiring compliance with ASHRAE Std. 90.1 – 1989 for commercial buildings and either compliance with the Model Energy Code of 1993 or disclosure to the buyer the energy performance features of new homes.

ASHRAE Std. 90.1 – 1989 was written in the mid 1980s and represented a significant improvement over Kansas' lighting and thermal standards of the 1970s. The residential requirements, while not establishing true minimum standards, were intended to provide a market-driven approach by providing the new home buyer with information needed to make an informed decision.

In 1999, ASHRAE released a major revision to the standard that recognized and integrated advances made in lighting, heating, and air conditioning equipment and systems and removed requirements rendered obsolete by these advances.

During this same time, the three model building code councils joined to form a single code setting authority and released the International Code series including an updated energy code, the International Energy Conservation Code (IECC), for both commercial and residential buildings. The residential provisions of the IECC are similar to the older Model Energy Code but include advances in building technologies. The commercial provisions of the IECC provide two compliance paths for commercial building compliance. One path is to meet the requirements of ASHRAE Std. 90.1. A second path, often viewed as parallel to ASHRAE Std. 90.1, provides a less complicated but less flexible approach.

In 2000 and 2001, cities across Kansas reviewed the International Code series and many have adopted them. While some cities excluded the IECC 2000, others adopted it. None have adopted recent versions of ASHRAE Std. 90.1. A new version of the International

Senate Utilities
March 17, 2003
Attachment 14-1

Code including the IECC 2003 released in early 2003. Cities will begin the review and adoption process afresh in the coming months.

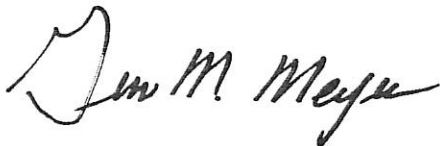
House Bill 2131, as amended, references the IECC 2003 for commercial buildings. This will align state law with the direction being taken by local communities while providing building design professionals with either the flexibility of ASHRAE Std. 90.1 – 2001 or the simplicity of the IECC 2003 rules.

The recommendation of the State Energy Resources Coordination Council was directed at “*all new construction*” but only addressed new commercial buildings. H.B. 2131 as amended would update K.S.A. 1228 to reference a residential energy code in line with what is being adopted by Kansas communities, provide the builder with greater flexibility in meeting energy codes should they choose to comply, and improve market-driven energy decisions by the consumer should the builder choose only to disclose the energy performance features. Proposed revisions include an update of the referenced standard to the *IECC 2003*, adding a Home Energy Rating of 80 or better as an option for compliance, and providing for disclosure of energy performance features to prospective buyers upon their request or during contract negotiations, not just the final buyer.

Energy codes are viewed by some in the building community as having no place in the code arena because they do not directly impact health and safety issues. However, the energy future of Kansas is in part controlled by the performance of the buildings we construct. Over 35 percent of the energy used in Kansas goes to commercial and residential buildings. HB 2131 only updates minimum standards, provides the builder of commercial and residential buildings greater flexibility when complying, and empowers the consumer with greater knowledge for making purchasing decisions.

As an engineer at Engineering Extension and having worked on energy code issues for many years, I encourage your consideration of these points in your deliberations of HB 2131.

Cordially,

A handwritten signature in black ink that reads "Gene M. Meyer". The signature is written in a cursive style with a large, stylized initial "G".

Gene M. Meyer, P.E.
Engineering Extension
Kansas State University
ASHRAE member

Kansas Senate Committee on Utilities

March 17, 2003

Testimony in Support of HB 2131

By

Bill Griffith

Kansas Chapter of the Sierra Club

Thank you Mr. Chairman and members of the Senate Utilities Committee for the opportunity to give testimony on behalf of HB 2131. As passed by the House, HB 2131 adopts the updated standards for thermal efficiency of ASHRAE/IESNA. This legislation will update the standards in this state for the first time in over ten years. Given the upgrades in technology since 1989 this bill will allow Kansans to obtain better energy efficiencies in their homes and businesses.

Energy efficiency is the least expensive form of energy. Many studies have shown that the costs of efficiency upgrades cost far less money than building new power plants or the cost of electricity, natural gas, or propane. With the volatility of natural gas expected to continue over the next decade energy efficiency is a logical and intelligent choice whenever it can be implemented or encouraged.

We would encourage the Senate and House Utilities Committees to further investigate where it might be possible to assist our state with energy efficiency options and upgrades in order to cut utility bills and decrease air pollution and greenhouse gases. Thank you.

Senate Utilities
March 17, 2003
Attachment 15-1