Approved: March 21, 2002
Date

MINUTES OF THE SENATE UTILITIES COMMITTEE.

The meeting was called to order by Chairperson Senator Stan Clark at 9:30 a.m. on March 13, 2002 in Room 231-N of the Capitol.

All members were present except:

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

Conferees appearing before the committee:
Rep. Carl Holmes
Sandy Jacquot, League of Kansas Municipalities
Colin Hansen, Kansas Municipal Utilities
Rick Thames, Kansas Press Association
John Lewis, Kansas Sun Coalition for Open Government
Richard Good, Westar Energy
Ron Appletoft, Water District #1 of Johnson County

Others attending: See attached list

Chair opened hearing on:
Sub for HB 2644 - Automatic pass through to customers of certain electric and natural gas utility costs for security measures

Proponents:

Rep. Carl Holmes noted this bill was requested to address the needs of utility companies to recover expenditures for security measures required to protect their generation, transmission, production and transportation assets. (Attachment 1)

Richard Good, Senior Manager, Disaster Recovery and Infrastructure Security, Westar Energy, spoke in support of **Sub. for HB 2644.** (Attachment 2)

Written testimony was received from Larry Dolci, Kansas City Power & Light Company and supports the passage of this bill which would improve the security of the electrical industry in Kansas and provide a significant benefit to the State and Nation. (Attachment 3)

Closed hearing on **HB 2644.**

Chair opened the hearing on
HB 2959 - Open Records Act exception for records related to security of utilities

Proponents:

Rep. Carl Holmes noted the request for this bill is the result of the need for non-disclosure of security information designed to protect energy and communications assets in Kansas (Attachment 4)

Sandy Jacquot of the League of Kansas Municipalities spoke in favor of **HB 2959**. The recent amendment of the Kansas Open Records Act to exempt records of "emergency information or procedures of a public agency" was an important first step but does not address records which are not specifically related to security procedures but which may poase a security risk if disclosed. (Attachment 5)

Colin Hansen, Kansas Municipal Utilities, spoke in strong support of **HB 2959.** (Attachment 6)

MINUTES OF THE SENATE UTILITIES COMMITTEE at on March 13, 2002 in Room 231-N of the Capitol.

Ron Appletoft, Water District No. 1 of Johnson County supports **HB 2959** if it is amended to include water systems. (Attachment 7)

Opponents:

Rick Thames, Kansas Press Association, opposed **HB 2959** and urged the committee to adopt language that appropriately addresses concerns regarding security while preserving the public's right to monitor the operation of these vital utilities. (Attachment 8)

The Kansas Press Association offered alternative language for (45) in **HB 2959**. (Attachment 9)

John Lewis of Kansas Sunshine Coalition for Open Government, testified that it was felt specificity is grossly lacking in the language for **HB 2959**. He commented the new language on security might be inserted under Section 12, page 2 of the Kansas Open Records Act. (Attachment 10)

Continued hearing on **HB 2959**.

The next meeting of the committee will be held on March 14, 2002.

Adjournment.

Respectfully submitted,

Ann McMorris, Secretary

Attachments - 10

SENATE UTILITIES COMMITTEE GUEST LIST

DATE: **MARCH 13, 2002**

Name	Representing
Ron Appletoft	Water Dist. No 1 of Jo Co
Joe Dick	KCK BPU
Anne Tymeson	KCC
Karla Olsen	Westar Energy
Mark Schreiber	Westar Energy
Richard Good	Westar Energy
Doug Haasted	KMU
Sandy Jacquot	LKM
J C Long	UtiliCorp United/Aquila
Phil Hurley	Pat Hurley & Co./Wolf Creek
Crystal Suing	KCPL
Ron Gaches	GBBA
Tom Day	KCC

STATE OF KANSAS

CARL D. HOLMES
REPRESENTATIVE, 125TH DISTRICT
LIBERAL ADDRESS
P.O. BOX 2288
LIBERAL, KANSAS 67905
(620) 624-7361
TOPEKA ADDRESS
STATE CAPITOL, ROOM 115-S
TOPEKA, KANSAS 66612-1504
(785) 296-7670
e-mail: repcarl@aol.com

TOPEKA

HOUSE OF
REPRESENTATIVES

COMMITTEE ASSIGNMENTS
CHAIRMAN: UTILITIES COMMITTEE
CHAIRMAN: FISCAL OVERSIGHT COMMITTEE
MEMBER: E-GOVERNMENT COMMITTEE
MEMBER: AGRICULTURE & NATURAL RESOURCES BUDGET COMMITTEE
MEMBER: JOINT COMMITTEE ON ADMINISTRATIVE RULES AND REGULATIONS
MEMBER: NATIONAL CONFERENCE OF STATE LEGISLATURES - ASSEMBLY OF FEDERAL ISSUES

LEGISLATIVE HOTLINE
1-800-432-3924

Chairman Clark and Senate Utilities committee members, I appreciate the opportunity to testify on substitute for HB 2644.

This bill was requested to address the needs of utility companies to recover expenditures for security measures required to protect their generation, transmission, production, and transportation assets. This recovery would be made through adjustments to customers' bills. The utility would first have to make an application and a request to the Kansas Corporation Commission. This request would be subject to procedures and conditions, including review of the prudence of the expenditures and the reasonableness of the measures, as considered appropriate by the Commission. The application and request shall be confidential and subject to protective order of the commission. The bill would sunset on July 1, 2004.

This legislation is needed to allow utilities to recover the costs of additional security needed for protection from terrorist attack. When steps are taken to protect the utility assets, I want the steps to be

Senate Utilities Committee
March 13, 2002
Attachment 1-1

confidential and not open for public review. When security measures are put in place, we don't want to make the plans available to those who are intent on terrorist actions. The level of protection could be indicated by the cost of the plan for each site. This allows for cost recovery in a procedure similar to the natural gas costs to gas utility companies without a separate rate case.

I appreciate the opportunity to present the reasons behind this bill. I will stand for questions at the appropriate time.

Westar Energy™

Testimony before the
Senate Utilities Committee
By
Richard Good
Senior Manager, Disaster Recovery and Infrastructure Security
Westar Energy
March 13, 2002

Chairman Clark and members of the committee, I am Richard Good, senior manager, disaster recovery and infrastructure security for Westar Energy.

Westar Energy supports Substitute for House Bill 2644. In these uncertain times, it is vital that we be able to take the steps needed to secure our energy generation and transmission facilities quickly and effectively. During the past six months, we have tightened security at our energy centers; and, at the direction of the Nuclear Regulatory Commission, new safeguards have been put in place at the Wolf Creek Generating Station.

Such upgrades are a necessary expense, and it is important that we are able to recover those costs efficiently. Kansas Corporation Commission review of the requests will ensure that the costs to be recovered are fair and were necessary expenditures. The bill also directs that such applications will be held confidential, which will contribute greatly to the effectiveness of security measures that are taken.

Substitute for House Bill 2644 takes important steps in protecting the energy infrastructure of our state and country. I encourage you to approve this measure.

Senate Utilities Committee
March 13, 2002
Attachment 2-1

818 South Kansas Avenue / P.O. Box 889 / Topeka, Kansas 66601
Office Telephone: (785) 575-6300

Testimony
In Support of Substitute for House Bill 2644

Larry Dolci, Director of Resource Protection
Kansas City Power & Light Company

Senate Utilities Committee
March 13, 2002

Mr. Chairman and Members of the Senate Utilities Committee, Kansas City Power & Light Company (KCPL), supports the passage of the Substitute for House Bill 2644 passed by the Kansas House and now under consideration by the Kansas Senate. The passage of this bill would improve the security of the electrical industry in Kansas and provide a significant benefit to the State and Nation.

The need to improve the security of the nation's infrastructure was recognized long before the events of September 11, 2001. Vulnerabilities in the nation's infrastructure were recognized in the report of the President's Commission on Critical Infrastructure published in 1996. The Commission found the private sector and government, including the military establishment of the U.S. are highly dependent on infrastructure like power, telecommunications, and transportation that are owned and operated by the private sector. They also found this infrastructure was a top potential target of terrorists and hostile nation states.

The publication of the report of the President's Commission led to the issuance of Presidential Decision Directive 63, PDD 63. This directive requires a voluntary and cooperative effort by the public and private sectors to improve the security of the nation's infrastructure. The key portions of PDD 63 have been adopted by the current Bush administration. A federal agency was assigned to work with each sector to improve security. The U.S. Department of Energy was designated to work with the electrical sector. A number of steps have been taken to improve security but much more remains to be done. A set of best security practices and lessons learned for the energy sector was developed by the Department of Energy. This document is attached as an exhibit.

The recommendations outlined by the Department of Energy deal with improvements in physical and cyber security for the energy sector. Implementation of these recommendations will require significant time,

effort and dollars. The Nuclear Regulatory Commission ordered even more far-reaching security improvements for nuclear power plants on February 26, 2002. These requirements will have a significant financial and operational impact on Wolf Creek Nuclear Generating Station near Burlington. Adopting new recommended and required security practices and processes will cost Kansas utilities millions of dollars. Kansas residents and government agencies will benefit directly from the improved security and reliability of electrical service resulting from these upgrades and should bear some of the costs of the new security actions required by the environment in which utilities now operate. Passage of this bill will allow such cost sharing.

The need to protect the electrical sector has been illustrated by the many warnings issued by government law enforcement and intelligence agencies before and after September 11, 2001. These agencies warn of direct threats by terrorists and hostile nations to the electrical sector. These potential threats are not only aimed at the power plants, substations and transmission lines of electrical companies but at the computer systems that are used to control the generation and distribution of energy. Computer hackers continue to target utilities including those in Kansas on a regular basis. At least two bomb plots against energy facilities were disrupted by the FBI prior to Y2K. Terrorists in the Philippines, Afghanistan and Columbia attack native electrical facilities on a regular basis.

Information is readily available on the Internet on how attacks can be mounted against U.S. infrastructure, often under the guise of how to improve security. Web sites allow terrorists to access material on mounting a variety of attacks on everything from power plants to the president.

The web sites clearly illustrate not only the vulnerabilities of certain key pieces of the nation's critical infrastructure but show how easily terrorists can find detailed plans to mount attacks on these installations. To meet the challenges posed by these vulnerabilities, utilities will need considerable assistance from government in a cooperative effort to improve security. Passage of the Substitute for House Bill 2644 would be a major step forward in this process and would benefit all Kansans.

Exhibit 1

DRAFT

VULNERABILITY AND RISK ANALYSIS PROGRAM

Lessons Learned and Best Practices

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

September 28, 2001

CONTENTS

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.

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 polices 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 on-going 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.

STATE OF KANSAS

CARL D. HOLMES
REPRESENTATIVE, 125TH DISTRICT
LIBERAL ADDRESS
P.O. BOX 2288
LIBERAL, KANSAS 67905
(620) 624-7361
TOPEKA ADDRESS
STATE CAPITOL, ROOM 115-S
TOPEKA, KANSAS 66612-1504
(785) 296-7670
e-mail: repcarl@aol.com

TOPEKA

HOUSE OF
REPRESENTATIVES

COMMITTEE ASSIGNMENTS
CHAIRMAN: UTILITIES COMMITTEE
CHAIRMAN: FISCAL OVERSIGHT COMMITTEE
MEMBER: E-GOVERNMENT COMMITTEE
MEMBER: AGRICULTURE & NATURAL RESOURCES BUDGET COMMITTEE
MEMBER: JOINT COMMITTEE ON ADMINISTRATIVE RULES AND REGULATIONS
MEMBER: NATIONAL CONFERENCE OF STATE LEGISLATURES - ASSEMBLY OF FEDERAL ISSUES

LEGISLATIVE HOTLINE
1-800-432-3924

Chairman Clark and Senate Utilities committee members, I appreciate the opportunity to testify on HB 2959. The request for this bill is the result of the need for non disclosure of security information designed to protect energy and communications assets in Kansas.

As a member of the NCSL Advisory Committee on Energy, I had the opportunity to attend a closed national security briefing and discussion on utility related security issues in January. The main presenter on the subject was Jim McDonnell, Director of the Energy Assurance Section, United States Department of Energy. His role is to protect the utility assets in the United States. The presentation and discussion was on "the State and Federal role in assessing and mitigating critical infrastructure vulnerabilities." Jim made the statement that the Federal Government was not willing to share critical intelligence and security information with state governments because of the possibility of the information becoming public information. He indicated the need to examine the problems caused by security classification of information that states need. States often do not receive pertinent information from industry and the federal government because of the fear the information will go public (Freedom of Information Acts).

In the process of drafting this bill, I had a meeting with John Campbell of the attorney general's office. We discussed the need to make an addition to the open records act for security purposes concerning energy. Mary Torrence and John worked together on the language on page 6

of the bill, lines 6-8. "**Records the disclosure of which may jeopardize the security of systems, facilities or equipment used in the production, transmission or distribution of energy or communications services.**"

I discussed changing of the word "may" to "will" in line 6 with the attorney generals office. They said not to change the word as the change would make it too narrow for the needed application.

This language is the only language approved by the attorney generals office. I ask the committee not to amend this bill. Their agreement is only for this language. There may be other security concerns that need to be addressed, but they need to be considered in separate bills.

I view this bill as a companion bill to the security section of HB 2644 in making our electric, gas and telecommunications services less vulnerable.

As you may be aware, many utility maps are not available now because of security reasons after September 11th. As we look at the potential for terrorist attack, we cannot protect all utility assets because of the costs. When we take steps to protect the energy and communications assets in Kansas, let us not make the security information available to those who desire to harm us.

I appreciate the opportunity to present the reasons behind this bill.

LKM
League of Kansas Municipalities

300 SW 8th Avenue
Topeka, Kansas 66603-3912
Phone: (785) 354-9565
Fax: (785) 354-4186

TO: Senate Utilities Committee

FROM: Sandy Jacquot, Director of Law/Legal Counsel

DATE: March 13, 2002

RE: HB 2959

I want to thank you on behalf of the League of Kansas Municipalities and its member cities for the opportunity to testify today in favor of HB 2959. The events of last September 11th have put security issues at the top of the agenda for public officials at all levels of government and city officials are certainly no exception. In addition to a number of public buildings and facilities, public water supplies and other utility facilities were identified by the federal government as potential terrorist targets. Police, fire, and public works personnel have been working together to evaluate and increase security procedures as necessary.

The Kansas Open Records Act was recently amended to exempt records of "emergency information or procedures of a public agency..." K.S.A. 45-221(a)(12). This exemption was a very important first step in protecting information concerning the security plans and procedures of public agencies. However, this section does not address records which are not specifically related to security procedures, but which may pose a security risk if disclosed.

The risk involved is real. Last summer, another state league reported that an individual walked into a county courthouse and requested aerial photos of ammunition plants in the area. A similar situation could arise in the context of public utilities. For example, an individual could walk into the county courthouse in Reno County and ask for aerial photos displaying the metes and bounds of all of the water wells for the City of Hutchinson. There is nothing in the Kansas Open Records Act that would prohibit the disclosure of this information.

HB 2959 provides an exemption from disclosure for records that may jeopardize the security of certain utility systems. We respectfully request that water and sewer services be added to the list of protected utilities. While the security of facilities involving electric and gas energy and communications is very important, they are no more important than water and sewer facilities. In fact, the utility that has been subject to the most publicized threat of terrorism is the public water supply. There is absolutely no rational basis to distinguish between utilities and provide protection for some, without providing protection for all.

The League appreciates your consideration of this very important and timely issue. For the policy reasons that I have outlined, we urge your favorable action on this bill and the proposed addition of water and sewer utilities.

kansasmunicipalutilities

Testimony Before the

Senate Utilities Committee

March 13, 2002

Colin Hansen
Executive Director, Kansas Municipal Utilities

House Bill 2959 – Utility Security

Kansas Municipal Utilities is a statewide trade association composed of 154 municipal electric, natural gas, and water utilities. In addition to electric, gas and water, all of our member cities are involved in the operation of municipal wastewater systems. These publicly owned utilities are subject to the provisions of the Kansas Open Records Act (KORA). The act generally mandates that all records of these publicly-owned utilities shall be open for public inspection, with few exceptions. Records subject to inspection include all documents, papers, maps, plans and other materials developed or received by the public entity.

In most cases, public record laws provide an effective mechanism for interested citizens to investigate and review the operation and maintenance of their municipally owned utility. In matters of security, however, the public records laws can be used to actually harm the very people that public records laws were intended to protect. Unscrupulous competitors, criminals and even terrorists can use public records laws to the detriment of the consumer owners of municipal utilities.

The Kansas open records law creates a significant and unnecessary security risk to the nation's public utility infrastructure, public utility employees, and the consumers of municipal utilities. Individuals could use the public records laws to access public utility information, such as plans, specifications and documents on the infrastructure of the utility as well as the name and address of any customer. Those individuals could then use that information to target utility facilities or individual customers for acts of violence or terrorism.

Since the tragedies of September 11th, the security of our utility facilities has become paramount. In many cases, a simple attack on a strategic element of utility infrastructure could cause lengthy disruption of service and perhaps even cost lives. KMU members over the past several months have reported receiving curious phone calls asking for sensitive power plant information, municipal utility web sites in the region have seen numerous "hits" from Internet users in the Middle east, and notices of potential threats continue to come

421 N. Main, Suite 3 • McPherson, KS 67460-3434 • 620.241.1423 ph •
email - kmu@kmunet.org • www.kmunet.org

down from the Department of Energy, the National Infrastructure Protection Center (NIPC) and the National Threat Warning System (NTWS). In fact, one such warning from the Department of Energy on January 16, 2002 illustrates the seriousness of the utility security obligation:

"WE HAVE RECEIVED INDICATIONS THAT MEMBERS OF AL-QAIDA MAY BE USING U.S. MUNICIPAL AND STATE WEB SITES TO OBTAIN INFORMATION ON LOCAL ENERGY INFRASTRUCTURES, WATER RESERVOIRS, DAMS, HIGHLY-ENRICHED URANIUM STORAGE SITES, NUCLEAR AND GAS FACILITIES, AND EMERGENCY FIRE AND RESCUE RESPONSE PROCEDURES. WE HAVE ALSO RECEIVED INDICATIONS FROM AROUND THE COUNTRY OF MULTIPLE CASINGS OF SITES SUCH AS THESE. YOU SHOULD REMAIN ALERT TO ANY UNUSUAL ACTIVITY AROUND SUCH FACILITIES, OR QUESTIONS ABOUT THEM. WE REQUEST YOU ALSO BE ALERT AND REPORT ANY SUSPICIOUS ACCESSES TO MUNICIPAL, UTILITY AND OTHER PUBLIC WEB SITES, AND REVIEW THE SECURITY IMPLICATIONS OF INFRASTRUCTURE CONTENT POSTED TO SUCH WEB SITES."

Department of Energy Security Notice
January 16, 2002

I might also note that KMU has been actively supporting member communities in their efforts to increase utility security. In fact, the association has recently been awarded a national grant through the American Public Power Association to develop utility security guidelines for all public power systems.

KMU strongly supports HB 2959. The bill would allow the prudent use of restraint with critical utility information in areas where public safety and security may be at risk.

In addition, KMU would request that data security provisions for municipal water and wastewater utilities be added to the bill language, so that they might receive the same protection as electric, natural gas and telecommunications systems. In fact, we believe that public water systems may be at an even greater risk in the current environment, given the potential for bioterrorism in municipal water plants.

WaterOne

Water District No. 1 of Johnson County

One Mission. . .
Quality Water

H.B. 2959 – Amending the Open Records Act

Testimony Presented at the
Senate Utilities Committee
On March 12, 2002
By Ron Appletoft, Governmental Affairs Coordinator

Water District No. 1 of Johnson County appears in support of H.B. 2959 if it is amended to include water systems. This bill would amend the Open Records Act allowing an exemption for energy or communications services when disclosure of records would jeopardize the security of systems.

Water District No. 1 is organized as a regional public water utility and serves over 330,000 consumers in and around Johnson County. The Water District is operated as a quasi-municipal corporation pursuant to K.S.A. 19-3501 et seq.

In general, the Water District supports legislation that will allow utilities to protect records that could jeopardize their security. However, this bill only mentions energy and communications and we believe that water systems should also be included. Therefore, we support the amendment being offered by the League of Kansas Municipalities to include water systems.

We also have two suggestions. Subsection (12) on page 2 of the bill already has language related to exemptions dealing with security. It appears the new language in subsection (45) should be incorporated into subsection (12) so security issues are not referenced in two subsections in the bill. In addition, several years ago the Open Meetings Act was amended to include an executive session exemption for security issues. To be consistent and to avoid confusion, it appears that the language in the Open Meetings Act should be identical to the language in the Open Records Act.

With the adoption of the League's amendment the Water District urges your support of H.B. 2959.

Senate Utilities Committee
March 13, 2002
Attachment 7-1

10747 Renner Boulevard . Lenexa, Kansas 66219 . tel: 913.895.5500

To: Kansas Senate Utilities Committee
From: Rick Thames, representing the Wichita Eagle and the Kansas Press Association
Subj: HB 2959 (Open Records Act exception for records related to security of utilities)
Date: March 13, 2002

Thank you for this opportunity to discuss House Bill 2959. I am the editor of The Wichita Eagle. I am also speaking to you today on behalf of the more than 200 newspapers that comprise the Kansas Press Association, as I am a member of its board of directors and chair of its legislative committee.

We're not here today to discourage you from taking some action on this issue. Having talked to the chair of the House Utilities Committee, Carl Holmes, I recognize that you have some legitimate concerns regarding security.

What we are asking is that you adopt language that appropriately addresses those concerns, while preserving the public's right to monitor the operation of these vital utilities.

As this proposal is now worded, we believe that KDHE, the KCC and other state agencies could be inclined to withhold many, many records that should remain open in the best interest of the public. It is simply too broad in its scope. And unnecessarily broad for its intended purpose.

To explain what I mean by that, I'll first review the wording of HB 2959:

> **"Records the disclosure of which may jeopardize the security of systems, facilities or equipment used in the production, transmission or distribution of energy or communications services."**

Here are some examples of the unintended harm possible under this wording.

The Hutchinson gas explosion.

Under this law, Kansas Natural Gas conceivably could have declined to explain:
-- Locations of underground pipelines
-- The amount and type of gas stored in the salt caverns
-- The pressure at which the gas was stored
-- What safeguards were established to find leaks in the gas system
-- What measures were being put into place to prevent this from ever happening again

All of this data was obtained from the KCC and other public agencies as city officials and journalists simultaneously worked to determine exactly what happening between Yaggy Field and Hutchinson. All were working in the public's interest. People had been killed and thousands of residents were justifiably panicked. What they needed was information.

Jim Bloom, the publisher of the Hutchinson News, told me yesterday that this exemption, as worded, could have significantly hampered that effort to inform the public. And he asked me, on his behalf, to register his opposition to it.

Other potential environmental hazards.

Pipeline safety inspection reports could fall under this exemption. So could environmental reports that explain what caused leaks and accidents.

Will farmers and other property owners be informed about the location of utility lines that could affect their safety and property values? This exemption may well prevent that.

Suppose the nuclear industry begins trucking power plant waste across the state to disposal sites. Could it claim a security risk in disclosing its route to the public that is endangered by this operation? It appears entirely possible.

Lack of important public notice.

Where are cell phone and microwave towers planned for your community? Will they be located disproportionately on a particular side of town? You could be told that disclosure is a security risk.

Where are the gas and electric substations? Can't tell you. Can we see the permits for them? No. How many state inspectors oversee them and what do their checks show? It's a matter of security.

Are the power company's generating facilities adequately staffed to provide power and be run safely? Staffing could also be termed a matter of security.

There are dozens more examples, but we hope we've raised enough here to demonstrate that a narrower focus clearly is in the public's best interest. We propose more specific language that focuses squarely on security issues. It reads as follows:

> **"Records the disclosure of which would pose a substantial likelihood of revealing security measures that protect systems, facilities or equipment used in the production, transmission or distribution of energy or communications services. For purposes of this provision, security means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination, or kidnapping."**

We believe this language actually reflects the intentions of the House bill. It's also more rational, more logical.

As an analogy, consider the federal government's efforts to make airline flights more secure. If those efforts followed the broad-brush approach of HB 2959, airlines might avoid telling you in advance your departure and arrival times. They might delay your luggage by a day. Deliberately, I mean.

Instead, they only keep secret their actual security *measures*, such as how they profile passengers, or specifically how their metal detectors and other screening procedures work.

To best protect the public's interest all around, we urge that the Legislature also focus on actual security measures. That is the spirit of the new language proposed here.

Thank you for your time and your consideration.

Sincerely,

Rick Thames

Rick Thames

8-2

Kansas Press Association alternative language:

(45) Records the disclosure of which would pose a substantial likelihood of revealing security measures that protect systems, facilities or equipment used in the production, transmission or distribution of energy or communications services. For purposes of this provision, security means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination, or kidnapping.

2954

HB 2959

Testimony of John Lewis
Immediate Past President, Kansas Sunshine Coalition for Open Government

On the surface, this bill might seem a bit difficult to argue against, given the current national security climate. It seems to comport with the national focus on security, but even well-intended legislation can be unnecessarily flawed.

It seems to me that this bill presents an enormous danger to open government due to the broad language of exemption no. 45. Specificity is grossly lacking.

• Which records, specifically, "may jeopardize" security?

• Who makes this determination? It shouldn't be the "custodian" of the records, as that person is merely a caretaker and could be a low-level one at that.

• How do we define "security"? I'm not asking what the definition of "is" is. The point is that, in the hands of an arrogant bureaucrat (of which there are many), "security" could be used as a pretext for the nondisclosure of just about anything. That's not good government; that's irresponsible government.

• What "communications services" are we talking about here? Telephones and Internet, I suppose, but does that also mean that the terms of the local cable television franchise could be withheld under the pretext of jeopardizing "security?" The word "communications" is a loaded word, and it's especially loaded with ambiguity.

The broad sweep of this language is rife with potential abuses. We simply don't know what specific services are covered and, more importantly, who would be making that determination. Non-specific legislation is dangerous legislation, especially when it covers public records, which constitute the only documentation available to the citizenry to make sure their government is performing in a responsible fashion.

This bill if far too nebulous in its current form, and it will therefore most certainly be misused as an illegitimate barrier for purposes well beyond its intended purposes.

In sum, I believe this bill, as to exemption no. 45, needs enormously more definition.

Senate Utilities Committee
March 13, 2002
Attachment 10-1