2007

Information Sharing Practices in Regulated Critical Infrastructure States

Analysis and Recommendations

NARUC

The National Association of Regulatory Utility Commissioners

Prepared for the consideration of the NARUC membership by SRA International, Inc.

June 2007

Funded by the U.S. Department of Homeland Security

DISCLAIMER

This report was prepared as an account of work sponsored by the National Association of Regulatory Utility Commissioners through the support of the United States Department of Homeland Security. Neither the U.S. Department of Homeland Security (U.S. DHS) nor the National Association of Regulatory Commissioners (NARUC), nor any person acting on their behalf:

A. Makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately-owned rights.
B. Assumes any liabilities with the report as to the use, or damages resulting from the use of, any information, apparatus, method, or process disclosed in this report.

Reference therein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. DHS. The views and opinions of authors expressed therein do not necessarily state or reflect those of the U.S. DHS.

The views and recommendations in this report do not represent NARUC policy positions, though some report recommendations may coincide with existing NARUC policy positions.

LETTER FROM THE CHAIR

Chairman Sandra Hochstetter, June, 2007

As Chair of the NARUC Committee on Critical Infrastructure, I am proud to present to public utility regulators, policymakers, utility industry leaders, and consumers, this landmark paper on a complex set of issues pertaining to our nation's critical utility infrastructure systems. This paper, entitled Information Sharing Practices in Regulated Critical Infrastructure States: Analysis and Recommendations examines the role of State and Federal governments and regulated utilities to protect and share information concerning threats, vulnerabilities, or disaster recovery. This paper focuses on the roles State public utility commissioners play in this process.

I trust that this report will enhance the understanding and appreciation of critical infrastructure protection, particularly with respect to the role of State public utility commissions, as well as assist in the development of appropriate policies and strategies in this vital area.

The Committee appreciates and is grateful for the assistance in preparing this report by Emily Frye and Andrew Spahn of SRA, International and Matthew Brown of InterEnery Solutions. I also acknowledge the support and funding provided by the U.S. Department of Homeland Security. I also want to thank those who guided, reviewed, edited, and helped shape this paper, including the staff of the National Association of Regulatory Commissioners' Charles Gray and Miles Keogh, and the NARUC Staff Subcommittee on Critical Infrastructure including Jeff Pillon of the Michigan Public Service Commission, Thomas Pearce of the Public Utilities Commission of Ohio, Chuck Seel of the Iowa Utilities Board, Joe Sukaskas of the Maine Public Utilities Commission, David Featherstone and Katie Rich of the Public Utilities Commission of Texas, Bob Rosenthal of the Pennsylvania Public Utilities Commission, and John Sennett of the New York Division of Public Service.

Chairman Sandra Hochstetter
Arkansas Public Service Commission
Chair, NARUC Committee on Critical Infrastructure
June, 2007

Table of Contents

I. Introduction and Executive Summary

It is tempting to look at water, electricity, and telecommunications infrastructure and think only about improving the most obvious manifestations of their security systems: guns, gates, guards, data protection, and cyber-security. These elements are important, but regulated utilities and utility commissions must consider additional aspects of their security strategy, a key element of which is protection of information. State governments, the federal government, regulated utilities and others must not only be able to *protect*, but also *share*, information with one another about threats, vulnerabilities, or disaster recovery. This paper focuses on the role of state public utility commissions in this process. It attempts to answer four questions:

1. How is the federal government taking steps to create an atmosphere of trust in which the private sector, state, federal, and local governments are comfortable sharing information about critical infrastructure vulnerabilities, threats, disaster recovery mechanisms, and related issues?
2. What are state governments, and specifically utility commissions, doing to create this same atmosphere of trusted information sharing?
3. What can or should be the relationship between state and federal actions on this front?
4. What new protocols or practices for sharing information might utility commissions consider? Where are the gaps in information protection coverage and what questions remain unanswered?

This paper explores the importance and challenges of sharing critical infrastructure information in the federal and state context. Much of the discussion focuses on the Protected Critical Infrastructure Information (PCII) Program, because that program offers a new mechanism for states, local government, the federal government, and private industry to share information about critical infrastructure.

In addition to exploring the role of the PCII Program in the context of state commissions, this study outlines other state level information sharing protocols by discussing specific methods for gathering, storing, and protecting hard copy and electronic information. Such processes are also an evolving area, particularly because many information protection protocols up until this point have focused heavily on protecting commercial information rather than security-sensitive critical infrastructure information (CII)

This paper offers a set of next steps for states to consider. The most compelling – that is, the steps most likely to generate a measurable improvement in the ease of dealing with CII – are threefold. This paper recommends that states and state PUCs consider:

1. Adopting PCII into the state, explicitly making the PUC an authorized user;
2. Promoting the consistent use of the term and definition of CII; and
3. Establishing a confidential hearing process for CII matters (where one does not exist).

II. Background and Definitions

This Section Offers:

(1) A brief perspective on the challenges to protection of CII from disclosure

(2) A definition of critical infrastructure

(3) A broad picture of considerations in critical infrastructure information protection

(4) Four common situations in which utility commissions deal with critical infrastructure information

Challenges to Information Protection

After years of preparation, major parts of state and federal plans to protect critical infrastructure and key resources and prevent future attacks are being implemented, such as the U.S. Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP), the DHS' PCII Program, and state laws and regulations such as H.B. 854 in Pennsylvania. The effectiveness of these new plans face two unique challenges: (1) they must create a partnership between government and the private sector; and (2) they must foster an atmosphere of trust among the different levels of government that have responsibility for critical infrastructures.

Private-Public Sector Partnership is Critical

Approximately 85% of critical infrastructure in the United States is owned and operated by the private sector, and as such, the private sector's involvement is imperative. Although legal, regulatory, and other issues may have hindered this involvement in the past, successful collaboration requires new thinking and approaches that consider the different circumstances of the public and private sectors. Otherwise, regulated utilities may remain reluctant to provide information about critical infrastructure to utility commissions out of concern that the information will be released to the public or otherwise disclosed.

Many Levels of Government Have Critical Infrastructure Protection Responsibility

Unlike most governmental functions, CIP does not fall neatly into the divisions of the federal system. Whereas defense- and police-related activities are parts of the national and state governments, respectively, CIP—among some other homeland-security-related functions—is under the purview of federal, state, local, and tribal governments. This shared, and often uncoordinated, responsibility adds an additional set of hurdles to programs that address CIP.

What is Critical Infrastructure?

Critical infrastructure is understood by those working in the field to be those assets, goods and services that are essential to the US economy and national security.[1] HSPD-7 recognizes 17 different sectors of critical infrastructure and key resources.[2] These sectors include energy, water, and telecommunications: the utilities sector is largely regulated at the state level.

Not all critical infrastructure can or should be physically protected in the same way. Utilities employ much greater effort to protect nuclear power plants than almost any other part of the nation's critical infrastructure. Coal plants receive a measure of protection that is less than a nuclear plant, but far greater than power lines on the distribution system. It is in fact not practical to physically protect all lines on the power or

[1]Homeland Security Presidential Directive 7, issued December 17, 2003, specifies under Subpart 4 that: Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

[2] Critical Infrastructure is often linked with "key resources" (KR); consequently, many plans refer to "CI/KR" as a single conceptual unit.

telecommunications system, or every part of a water distribution system, although it is possible to build a system that has enough redundancy built in to it to diminish the overall risk.

Critical Infrastructure Information Protection: A Broad Perspective

Beyond physical and cyber protection of the utility systems, utilities and state utility commissions must be concerned about preventing widespread disclosure of information about system vulnerabilities and protective measures. The information that commissions are trying to protect from widespread disclosure falls into several categories, such as:

a. Vulnerability-related information. For example, major switching stations on telecommunications systems, power plants, or power lines that are critical to the reliability of the power system.

b. Interdependencies. For example, information describing the effects that an attack on energy networks could have in disrupting telecommunications, water systems, or other infrastructure.

c. Threat-related information. For example, detailed information about threats to drinking water systems which could cause widespread panic from the general public or undesirable scrutiny from regulators;

d. Plans and blueprints for telecommunications, water or power systems. Such plans, if released indiscriminately or accidentally, could facilitate an attack on those systems; and

e. Disaster-response and recovery plans.

Is Protecting Critical Information Really a Problem?

Not everyone is convinced that utility commissions will have difficulty collecting and securing CII. For example, the Arkansas commission's General Counsel issued an opinion that the Commission's procedures for collecting and securing such information were adequate to keep that information from falling into the wrong hands. A 2003 National Regulatory Research Institute survey of state commissions found that more than 80% offered some form of information protection for security related information and that utilities were reluctant to share security-related information – but less reluctant to do so than they had been a in 2002.[1] By contrast, the Iowa commission made a choice shortly after the September 11, 2001, attacks not to collect such information because it could not guarantee its security. Although situations and regulations differ from one state to another, anecdotal evidence suggests that many utilities still do not feel convinced that the information they provide can be legally protected from widespread public disclosure.

Within each of these categories of information is another triage process that requires utility commissions, utilities, and other levels of government to filter out which information is most important to protect and which information should be left in the public domain. Information that is already widely available and that would be of little help to someone planning an attack requires no particular protection. Highly specific information, such as blueprints, detailed analysis of which pipelines or transmission lines are most critical, or security plans for major water systems or power plants do require high levels of protection. Some states and the federal government categorize information according to this triage system, and give the most critical information a higher level of protection.

It is possible to view this issue on a continuum, where the most sensitive information is protected at the highest level (classified information) and the least sensitive is widely available on the Internet. In between those two extremes are different levels of protection – information that is technically accessible but not easy to get (not available electronically or by mail, for instance); information that is available only to people who can demonstrate an official need for it but for which there is not a criminal sanction for releasing it; information that is restricted to those who have an official need for it and have signed waivers specifying precisely how they will handle the information yet still face no criminal sanction for releasing it; information that is highly restricted, released only to those who demonstrate a need for it and who are certified by a federal agency, and for which there is a financial or criminal penalty for release beyond those authorized people. The following chart shows a graphic representation of this continuum. In general, the federal and state information sharing protocols described in this paper fit along some part of this continuum.

Figure II.A. Information Protection Continuum.

As a general rule, federal information-protection systems are likely to provide more uniform coverage, and therefore reduce uncertainty – a prime concern among industry information providers. Note that some parts of DoE also use FOUO.[3]

When Do Utility Commissions Deal with Security-Sensitive Information?

Utility commissions have regularly dealt with CII since they were established; many commission activities require commissioners and staff to become custodians of this kind of information. Appendix A describes in more detail the situations in which state commissions address information protection through their own protocols. In general, commissions deal with, or have potential to deal with, CII in four situations: rate cases, siting applications, reports and special investigations and in their capacity as energy advisors to governors, other agencies or other levels of state government. Not every state commission is involved in all four of these activities.

These rate cases, siting applications, utility and commission reports, and commissions acting as advisors demonstrate a number of important issues:

1. Utility commissions regularly ask for and then become custodians of CII during the course of their proceedings;

[3] *Thanks to Alice Lippert and Jeff Pillon for their generous contribution of both concept and content.*

2. The commissions typically have a process for handling such information, including a classification system that dictates who gets access to information, and under what circumstances;
3. Companies are often comfortable sending some information to their Commissions, but have concerns as the information gets more detailed. In some cases, they have concerns about what happens to information over time, as it is stored at the commission; and
4. Companies are sometimes not comfortable with the way in which commission's non-disclosure agreements bind those who signed them.

Why is Protecting Critical Infrastructure Information Important?

Why Is Protecting CII Important?

- Critical Infrastructure Information Impacts National Security
- Information Sharing Touches on Constitutional and Political Issues Regarding the Balance of Security and the Free Flow of Information
- Strong Information-Sharing Networks Are Useful for Preventing and Responding to Emergencies.

Critical Infrastructure Information Impacts National Security

Critical Infrastructures are, in general, systems of systems; they are highly interdependent. Failure in one infrastructure (telecommunications) can cascade quickly through the others (banking and finance, and electricity, for example). The key to keeping the system running is not only adequate investment and physical protection of the systems from disasters, but also trusted communication about vulnerabilities, threats, and recovery procedures. Regulators and other parts of government and industry must be able to share information about the security of this interconnected infrastructure network.

Information Sharing Touches on Constitutional and Political Issues Regarding the Balance of Security and the Free Flow of Information

Utility commissions serve in a delicate role. They are trusted by the public to operate in a transparent and open fashion, while also occasionally becoming custodians of CII that regulated utilities give to them in the course of commission proceedings or that they use in their role as advisors to Governors, homeland security offices, and law enforcement agencies in their states.[4] Utility commissions can only do their job well if the companies they regulate share information with them in an atmosphere of trust and confidence, and the regulated companies may be reluctant to initiate a rate case if they feel that it will likely require them to divulge sensitive information about their systems. CII protection protocols help to make these systems more secure by establishing widely accepted regulations and procedures for how utility commissions treat that sensitive information.

Strong Information-Sharing Networks Are Useful for Preventing and Responding to Emergencies

Utilities, DHS, and state agencies, among others, each conduct vulnerability studies, and each entity has an idea about how its systems (water, electric, telecommunications, or gas) could be vulnerable to malicious attacks or to natural disasters. Each knows how to reduce risk by doing so on its own. However, the risk of a malicious attack, or the risk of serious disruptions as a result of a malicious attack falls when all of these entities work together, talk to one another, and share information. Disaster recovery and emergency response functions are no different – they work on the basis of trusted communication and fail when that communication breaks down.

[4] Not all utility commissions serve in this extended role.

III. A Federal Review: Relevant Federal Framework

This section provides an overview of the PCII Rule and FERC actions to address CII sharing practices.

The purpose of this section of the paper is to address how this new culture of shared-governmental responsibility and private-sector engagement relates to NARUC members, specifically with regard to CIP. This section focuses on two key programs and rules that call for intense federal-state-private-sector collaboration: the DHS PCII Program and FERC Rules 630, 630-a, and 649. These programs and rules attempt to bring different governments together—federal, state, local—to further CIP. Although each, particularly the PCII Program, has faced numerous hurdles, an analysis and consideration of them and their improvements will benefit state utility commissions by introducing new ways to protect CII and foster this unprecedented multi-government approach to CIP.

DHS' Protected Critical Infrastructure Information (PCII) Program

The PCII Program, part of DHS' Office of Infrastructure Protection,[5] is designed to encourage private industry to voluntarily share its sensitive security-related information with the Federal government in an effort to reduce its vulnerability to terrorist attacks. [6] The PCII Program is an information-protection tool that facilitates information sharing between the government—at all levels—and the private sector. Appendix B describes the steps necessary for states to become accredited by the PCII Program.

Under provisions of the Critical Infrastructure Information Act of 2002 (CII Act), appropriate information voluntarily submitted to the PCII Program Office will be exempted from information-disclosure laws at the federal, state, and local levels of government. The CII Act, or Section 214 of the Homeland Security Act,[7] provides for the establishment of a CIP program that exempts any CII from disclosure under federal, state, and local information-disclosure laws.[8] The CII Act authorized DHS to accept information relating to critical infrastructure from the public, owners and operators of critical infrastructure, and state, local, and tribal governmental entities, while limiting public disclosure of that sensitive information under the Freedom of Information Act, 5 U.S.C. 552 (FOIA), and other laws, rules, and processes. If validated as PCII, the information remains exempt from public disclosure. DHS will return submissions in almost all cases when it does not qualify as PCII. (site: http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-7378.htm).[9]

There are severe penalties for the misuse of PCII:

- Federal and state fines
- Imprisonment
- Removal from office
- Penalties as prescribed by state law
- Endangerment of the ACAMS program

[5] DHS will be reorganizing shortly.
[6] "Protected Critical Infrastructure Information (PCII) Program," http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm
[7] The CII Act is a subpart of a larger law, the Homeland Security Act. It is common for certain parts of laws to acquire separate labels when they spark widespread discussion or have significant impact.
[8] http://www.fas.org/sgp/news/2003/04/fr041503.html
[9] 6 C.F.R § 29.8 (g) – (i).

FERC Rules 630, 630-a, and 649

After September 11, 2001, FERC promptly took steps to enhance the procedural protections surrounding CII within its purview (called "Critical Energy Infrastructure Information," or CEII, in the FERC context). The protections in the FERC rules pertain to data that is exempt from mandatory disclosure under FOIA. In some ways, the FERC rules look like an energy-specific version of the PCII Program. Most notably, a special office was created to handle the data and requests about the data, as well as to ensure that protective requests do not overreach. Whereas these rules apply neatly to data collected by FERC, they are not particularly helpful to state utility commissions. There are at least two reasons why the FERC rules should be embraced with caution.

First, FERC rules are federal in nature, and do not by definition cover state issues. The relevance of FERC Rules 630 and 649 in state environments is questionable.

Second, and more important, the legal relationship of the FERC rules to the now-Final PCII Rule is unknown. If a direct challenge of one or the other were to enter the judicial system, it is extremely difficult to determine which would stand. The FERC rules, for instance, explicitly exclude coverage of merely geographic (or location) data. PCII – at least, if the current views at DHS prevail – may very well include geographic data.

Related to this second issue is the administrative burden that courts may be reluctant to impose upon agencies dealing with this data. Since the FERC rules apply only to a subset of CII, but the PCII Rule is designed to cover all CII, many courts would lean toward a simple adoption of the PCII Rule as the standard and may be reluctant to impose multiple management and compliance regimes upon administrative bodies.

Whereas the PCII Rule – if properly promulgated and adopted by states – has great potential to assuage the concerns of private industry, there are certainly limits on its applicability. On November 16, 2006, FERC issued its final rule on Filing Applications for Permits to Site Interstate Transmission Facilities (18 CFR Parts 50 and 380). As this study was being prepared, various stakeholders inquired whether PCII or the FERC CEII rules would interact constructively with the new siting rule. To some extent, confusion is inevitable and only time will provide assurance. But some well-informed assessments can be offered.

Under the final rule on Filing Applications for Permits to Site Interstate Transmission Facilities, FERC can effectively convert a state transmission siting process into a federal process if the state-based processes are subject to undue delay[10] or a lack of sufficient legal authority.

Under the present regime, there is no legal basis on which to assert any CII-type of protection for the data involved in such cases. When determining the proper application of a law, courts look first to the letter of the law, and second to the existing application or industry standard pertaining to the law. In the authors' view,[11] there would be no foundation at this time for sustaining an argument that CEII rules are sufficiently broad or that the PCII Rule applies.

IV. The Status of CII Sharing Practices in PUCs

This section reviews the major challenges that states face in protecting CII.

A survey of CII-sharing practices at the state level presents a wide variance of approaches to attempting to ensure that CII is not disclosed under applicable sunshine laws and Freedom of Information Acts. "Critical infrastructure information," for example, does not have a uniform definition and, in many cases, the term is not even used by state laws or policies. Furthermore, in some cases, "security-related information" is not a term used to categorize exempted information from disclosure; instead, "commercial information" is sometimes read to include security-related information and, in many cases by extension, "critical

[10] In most cases, "undue delay" means more than twelve months.
[11] The authors of this section are attorneys with a core expertise in CIP.

infrastructure information." Over time, astute litigators will realize the conflation of the two sets of data is likely to result in some inaccurate – or what lawyers often call "overbroad" – exemptions. The last thing that utilities and regulators want to spend time doing is litigating the definitions of terms. This paper, therefore, promotes the adoption of clear distinctions between these types of information.

NARUC, which represents many jurisdictions with many definitions (and in some cases, no definitions) for terms such as "CII," is an ideal venue in which to raise the lack of understanding of how different states define and apply terms. This is especially important when recognizing the national nature of sectors such as telecommunications, water, and energy. Consistent definitions across jurisdictions can build trust and create an atmosphere of confidence in decision-making. The proliferation of disparate nomenclature has become increasingly noted: a January 2007 study by the Information Sharing Environment Office[12] found that more than 100 labels for handling, distributing, and storing information have proliferated federally in the unclassified environment alone – very likely the environment in which most CII will remain. These labels range from "For Official Use Only" to "Information Related to a Continuity of Operations Plan" to "Sensitive but Unclassified." None of these labels has a clear legal definition. One program manager described the result as "chaos."[13]

While the general proliferation of inconsistently defined terms is beyond the scope of this study, the short lesson is that PUCs are likely to benefit from adopting terms that are, or are likely to be, recognized in the judicial system. In addition, promoting a uniform semantic furthers the national goals of homeland security, including CIP. Through directives such as Homeland Security Presidential Directive-7 and the NIPP, the federal government is approaching homeland security and CIP via an inter-governmental manner. Although federal guidance has not always effectively articulated how states and local governments should align themselves for these initiatives, defining terms, such as CII, similarly would be an effective step forward that not only clearly distinguishes definitions, but would also be a tangible demonstration of how all entities are working together. In the case of a legal question, the customary use of these terms would help to more clearly define what they mean.

Not solely as a result of a lack of uniform terminology and definitions, states and local governments are facing challenges in complying with federal rules, laws, and initiatives involving CIP. In many cases, this has been partially caused by the creation of DHS and the unprecedented partnership among governments necessitated by CIP. In addition, the necessary cooperation of the private sector has proven difficult, and the evolving nature of DHS has helped to exacerbate these difficulties. States, then, are seeking clarification about these new laws and programs in order to comply. Time is of the essence because the longer it takes to understand the programs, the greater the risk of prospective participants becoming disaffected with them. Further delay could disrupt the construction of these unprecedented public/private partnerships.

The NIPP specifies general roles for states, such as collecting information for the National Asset Database, dealing with issues that arise from geographical anomalies, and helping share information across various levels of government. It appears likely that more direction about state-level involvement will emerge once a state-focused office is established within DHS. This is anticipated in 2007.

[12] Part of the federal intelligence community, the ISE is a relatively new group established after the issuance of the 9-11 Commission.

[13] "Group Attempting to Simplify Byzantine Terror-Alert System," by Elizabeth Williamson. Washington Post, January 24, 2007, page A21.

V. Interactions Between Federal and State Programs: Challenges at the State Level to PCII Compliance

This section addresses the complex interactions between federal and state policies, particularly related to the PCII Program.

No federal government initiative involving CIP has been more confounding to stakeholders than the DHS PCII Program. However, this program appears to offer promise in alleviating concerns surrounding the sharing and protection of CII. At its inception, the PCII Program did not recognize how important it could be to state and local jurisdictions in their interactions with the private sector. This left many with a negative impression. It appears now, however, that this impression of the PCII Program may be changing.

As states began to present DHS with their approaches to CIP and the *de facto* requirement in the private sector that their CII could not be disclosed to the public via applicable sunshine laws, the PCII Program began to recognize how its broad authority could be applied to state and local-level programs. Standing alone, the PCII Program did not appear significant; as soon as it was applied to actual programs—and tailored to them—its benefits provided the cornerstone to many a CIP program.

In the case of Maryland, for example, the state was developing its CIP Program and private-sector entities did not want to participate lest their information would be disclosed under the Maryland Public Information Act. The State then approached the PCII Program, and together, they tailored the PCII Program process to the program requirements of Maryland. This sort of fact-based application was also used in Los Angeles by Archangel in its implementation of the Automated Critical Asset Management System / Project Constellation.[14] The result of these developments helped to create the Final Rule for the PCII Program, which seeks to tailor the program to a broad array of initiatives and requirements.[15]

Among the array of initiatives that the Final Rule may cover is the transfer of CII to PUCs. Although the applicability of the PCII Program did not seem relevant to this exchange prior to the Final Rule's publication, it now appears that PCII could offer an important mechanism to transmit CII to utility commissions. In effect, CII could be provided to the PUCs via the PCII Program. By the PCII Program serving as a conduit of sorts in this transfer of information, information subsequently received by the PUCs would be exempt from disclosure under local, state, and federal information-disclosure laws and, thus, would alleviate many of the private sectors' concerns about sharing CII. This is, of course, a change from the traditional ways by which information would be transferred from the utility to the PUC. Importantly, though, the addition of the PCII Program to the path of CII transfer would be, essentially, unnoticeable because it can be done electronically and securely.[16]

There is, then, a great deal of interest in how the PCII Program can affect PUCs and their handling of CII that utilities submit. With the developments of the PCII Final Rule and the improved performance of the PCII Program, the program deserves a hard look from NARUC, utility commissions, and utility owners and operators. To be clear, the PCII Program is not a panacea. It may, though, help to alleviate the concerns of many utilities about sharing information with the PUCs .

---

[14] ACAMS / Constellation is a secure, web-based information management tool designed specifically to capture, store, and view critical asset data. This DHS Program provides two functions: 1) Collecting and communicating information for prevention, and 2) strategic pre-incident planning measures to assist in an effective response to critical incidents including, but not limited to, terrorism.

[15] 6 C.F.R. § 29, "Procedures for Handling Critical Infrastructure Information; Final Rule."

[16] Observers have noted that this approach may result in challenges for intervenors, who will also want access to the information. Intervenors may be able to obtain the information through different legal channels that are generally applicable in their state's proceedings.

An analysis of the PCII Program is not particularly helpful unless the program can be applied to a specific set of facts. For that reason, this analysis tailors the application of the PCII Program to particular PUC interests: rate cases, siting applications, required reporting, and incident reporting. By using these four cases as the prism through which to apply the PCII Program, actual facts can be placed in the context of the rules and requirements of the PCII Program. It should be said, though, that the analysis of all four is quite similar as each involves the submission of entity-owned CII to the PCII Program and, via the PCII Program, to the PUC. At the time of a previous report prepared by the Institute of Public Utilities at Michigan State University for NARUC, the PCII Program Final Rule had not yet been issued and it was, as a result, very difficult to apply the Program to real situations and facts. We have attempted to do so in this overview.

In summary, as long as the CII is transferred in accordance with PCII Program's rules from the utility to the PCII Program and then to the state, then that CII, when in the hands of the PUC, is exempt from disclosure under applicable state and local information-disclosure laws (and the Federal FOIA) as well as during civil litigation. For this process to work, the state must be accredited by the PCII Program, and the PUC must be involved in, and considered during, the accreditation. If the handling of CII by the PUC in the aforementioned cases—rate cases/siting, required reporting, and incident reporting—is of concern to utilities for information-disclosure law purposes, then the PCII Program may be beneficial.

Although states have begun to access PCII data in many cases, no state PUCs had received PCII data as of February 2007. In large part, this may result from the fact that many states' "Critical Infrastructure Protection Plans" are housed in a governor's office, state police department, or with the National Guard.[17] These offices have often not realized how helpful CII-protection regimes could be to the utility commissions in their states. For example, Maryland's CIP program barely took the PUC into account. Several states are already PCII accredited, but the fact that no state PUC has yet received PCII data demonstrates that the connection between the PUCs and the agencies that house the CIP program has not been made. Even if the PUC ultimately decides not to use the PCII Program, it will be helpful for the particular PUC to establish or enhance a relationship with the office responsible for CIP in that state. Therefore, NARUC should begin to encourage the collaboration among those PUCs and the PCII Program Officers in the accredited states to foster a dialogue and partnership about CIP.

The PCII Program seeks to accredit entire states, and not specific agencies or consortia at the state level (exceptions to this rule are possible, however). That way, all entities falling under the auspices of the state can receive PCII (so long as the recipients comply with the user requirements). If, however, a state entity or locality expresses interest in accessing PCII data and the entire state is not on board, the PCII Program will accredit at those levels.

In the case of the State of Maryland, the first state accredited by the PCII Program, it was initially interested in possessing PCII at the Maryland Emergency Management Agency (MEMA) because that is where the State's CIP Program is located. After consultation with the PCII Program, it became clear that accrediting the entire State—and not just MEMA—was more in its interest because PCII could then move among interested, disconnected state entities without worry about whether the particular state entity was accredited. Notably, an official with MEMA became the PCII Officer for the entire State of Maryland. The State signed the Memorandum of Agreement with the PCII Program Office. The PCII Officer, who is a state official, now trains state handlers of PCII and provides oversight of the use of PCII within the State of Maryland to ensure that PCII safeguarding and handling requirements are being met.

This policy of accrediting at the highest level of state government is also useful when an accredited state's CIP entity, such as a police department, realizes that it needs to coordinate with a PUC for CIP purposes or when a PUC realizes it needs protections similar to those afforded by the PCII Program; in these cases, the PCII Program does not need to "reaccredit" an additional agency. The PCII Officer at the state level can confer authorization upon the PUC and it is, thus, a PCII-authorized entity in a PCII-accredited state.

[17] See also the NARUC brief on State Organizational Issues, available through NARUC.

Specific Considerations for PUCs and PCII

Whereas it seems apparent that PUCs must integrate with state and local CIP plans—and likely become part of the state or locality's PCII regime—it is imperative that the PUCs also understand the PCII Final Rule, especially its broad applicability to state and local entities. There are a number of specific questions related to the PCII Program for PUCs to consider. The following section offers perspective on these issues.

Is the Information Submitted to PCII Security Related?

The Rule states that the PCII must be used for security-related purposes. The Final Rule allows for other uses of PCII, however, the submitting entity must consent to that usage. The initial question, then, is whether the PCII Program can be used for rate cases/siting, incident reports, and required reports. This is an issue underlying other points of discussion in this study. At this point– with much uncertainty, and further developments likely – the situation appears to be this: At the least, if the information submitted through the PCII Program is requested by a PCII-accredited PUC for a non-security related use, and the utility consents to that use, then the data could be used for purposes such as rate cases/siting, incident reports, and required reports. It is likely, though, that the use of CII in situations such as rate cases/siting, incident reports, and required reports would qualify as a "security-related purpose." Importantly, it is likely that non-PCII authorized requesters (or any party not designated by the submitter as being eligible to receive the PCII) would have a limited likelihood of acquiring the PCII; they would have to make an extraordinary legal argument to obtain the PCII.[18] This rigid standard ought to provide comfort to utilities and PUCs alike. The reasoning behind these conclusions is lengthy, but straightforward.

The Final Rule defines CII as having the same meaning as established in Section 212 of the CII Act of 2002 and means "information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, or other information concerning…[a]ny planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation."[19] According to this definition, then, the security-related information involved in rate cases/siting, required reporting, and incident reporting would likely qualify as CII.

CII submitted to the PCII Program must meet particular requirements before it can be protected by the Program. In order to receive the official protection afforded to CII by the PCII Program, the information needs to be:

1. Voluntarily submitted to the PCII Program Manager or PCII Program Manager Designee;
2. Submitted for a particular purpose, which relates to a class of protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purposes including, the identification, analysis, prevention, preemption, disruption, defense against, and/or mitigation of terrorist threats;
3. Labeled with an express statement, such as: "This information is voluntarily submitted to the official PCII office within DHS [or within the relevant state, or state entity] in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Act of 2002"; and

[18] 6 C.F.R. § 29.8(e). The "exigent circumstances" exception applies first and foremost to first responders, but it is possible (in theory) that competitors and potential litigants could learn some sensitive information during an emergency response, if they respond via mutual aid agreements and thereby are covered for the duration by a temporary PCII admonishment. This is no greater a risk, however, than is currently endured.
It has also been observed that such a regime would be highly controversial in contested situations. Until the matter is addressed in court, however, it is difficult to ascertain which forms of legal reasoning will prevail, and consequently what types and levels of access will be available to various parties.

[19] 6 C.F.R. § 29.2(b)-(3).

4. Accompanied by a signed statement identifying the submitting person or entity, containing contact information and certifying that the information being submitted is not customarily in the public domain.[20]

It seems clear that the PCII Program's usage applies to rate cases/siting applications, required reporting, and incident reporting. Beyond merely meeting the broad mandates of the PCII Program (e.g., "security related" or the acquisition of the submitter's consent), these cases must also meet the specific requirements of the PCII Program. When the requirements[21] for acquiring PCII protection are presented, it seems clear that information submitted by a utility to a PUC—so long as the submission went through the proper steps—could receive PCII certification and, as a result, would be exempt from disclosure under federal, state, and local sunshine laws. For more detail on the proper steps, please see Appendix B.

Can states submit information to PCII for PCII protection?

State entities are permitted to submit information to PCII for protection, much as the private sector is allowed to do so, subject to the same legal structure as described above.

Is Information Submitted Voluntarily?

One may initially question whether the submission of CII to the PCII Program for use by the PUC in the aforementioned cases is, indeed, "voluntary." In the Final Rule, DHS asserts: "The definition of 'voluntary' in Section 29.2 of this rule implements section 212(7)(A) of the CII Act (6 U.S.C. 131(7) (A)), which provides that a submittal of CII is not 'voluntary' if such information is provided pursuant to the exercise of legal authority by DHS (the 'covered agency') to compel access to or submission of the information."[22] This interpretation seems to mean that information provided by utilities to the PUC, required or otherwise, would still receive PCII protection because it was not required by DHS to be submitted. In other words, because DHS is not requiring the information in rate cases/siting, required reporting, and incident reporting, the information would be considered voluntarily submitted to the PCII Program.[23]

Simultaneous Submittal of Information to PCII and a PUC

Some interested regulatory commissioners have expressed concern about CII simultaneously provided to the state PUC and to the PCII Program Office. The concern is that the information would be protected under PCII because it went through the PCII Program Office, but that it would simultaneously not be protected under PCII because another copy of the same information was submitted directly to the PUC. This situation suggests two responses:

[20] 6 C.F.R. § 29.5(a).

[21] Again, those "requirements" include: The information needs to be voluntarily submitted to the PCII Program Manager or PCII Program Manager Designee; submitted for a particular purpose, which relates to a class of protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against, and/or mitigation of terrorist threats to the homeland; the information is labeled with an express statement, such as: "This information is voluntarily submitted to the official PCII office within DHS [or within the relevant state, or state entity] in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Act of 2002"; and the submitted information is also accompanied by a statement, signed by the submitting person or an authorized person on behalf of an entity identifying the submitting person or entity, containing such contact information as is considered necessary by the PCII Program, and certifying that the information being submitted is not customarily in the public domain.

[22] 6 C.F.R. § 29, "Supplementary Information," p. 52262.

[23] This interpretation is speculative, although as sound as speculation can be based upon current understandings of priorities in the PCII Program. This paragraph describes one possible set of questions related to definitions of voluntary submittal. To the extent that there are questions about these definitions or other related issues, the PCII Program and the courts will resolve those questions based upon their particular facts.

1. Ordinarily this situation would not arise in practice. Instead, the PUC would encourage the utility to send CII to the PCII Program and to direct the PCII Program to share it with the PUC. The PUC would then receive the PCII that was exempt from disclosure under federal, state, and local sunshine laws from the PCII Program.
2. If this simultaneous submission of documents to PCII and to the PUC does occur however, the information possessed by the PUC would not be deemed PCII. The PUC, however, could then—so long as the PUC met the necessary accreditation requirements—submit the CII to the PCII Program and have it sent back to the PUC. That information would then be PCII. Although this approach is likely permissible, it would be discouraged by the PCII Program Office.

The Final Rule exempts PCII from disclosure under federal, state, and local disclosure laws and during civil litigation. Importantly, information that can be disclosed under other laws would still be subject to those laws. At the state and local level, an analysis of the effect of the Final Rule's preemption clause on state and local disclosure laws is sometimes unnecessary because some state and local disclosure laws possess a "mirror" provision whereby information that is exempt from disclosure under federal disclosure laws (such as the Federal FOIA) is also exempt from disclosure under state and local disclosure laws. Put differently, the determination of whether the PCII is disclosable under state or local law may merely hinge on the "mirror" provision and will, thus, not have to delve into the more complex considerations surrounding the disclosure of security information at the state and local level. In Maryland, for example, SG §10-615(2) says that the state custodian must deny inspection if the inspection is contrary to federal statute or regulation. These state FOIA provisions are discussed in more detail below.

It is not too difficult to determine who would prevail in a state court in the event the state did not have this "mirror" provision. This is particularly the case for a program, such as the PCII Program, which uses federal preemption to assert that PCII is not subject to disclosure under state or local laws. Through these "mirror" provisions, states automatically "accept" this preemption. The existence of the "mirror" provision makes the legal analysis far simpler; its absence will likely not change the outcome (withholding disclosure of the PCII) due to Congress' powers via federal preemption (as is exercised in the CII Act).

Conclusion to Specific Considerations for PUCs and PCII

Based upon the above analysis, it appears that PUCs could use the PCII Program for a number of purposes. It remains unclear how the PCII Program would interact with data-management needs in administrative hearings, however.

In order to use the PCII Program, the state in which the PUC is located would need to be accredited by the PCII Program, or the PUC itself would need to be accredited. In addition, PUC employees who would be handling the PCII would need to complete PCII Authorized User training. The PUC would be required by the PCII Program to handle and store the PCII in accordance with its requirements.[24] The PCII Program would also ensure that any electronic filings including potential PCII were executed in compliance with the PCII Program's handling requirements.

Importantly, the PUC could use the PCII to make judgments and file reports. Public PUC documents could either be issued with PCII information redacted, or the PUC could issue two separate reports, one with summary information that was not PCII protected and one with the PCII information; the report with the PCII information would be given PCII protection – meaning it could be disseminated among PCII-authorized users only.

[24] PCII safeguarding and handling requirements are available from the PCII Program Office in the form of the PCII Procedures Manual and include items such as whether PCII is stored in a locked room (when unattended), et cetera. See Appendices for complete description of protocol.

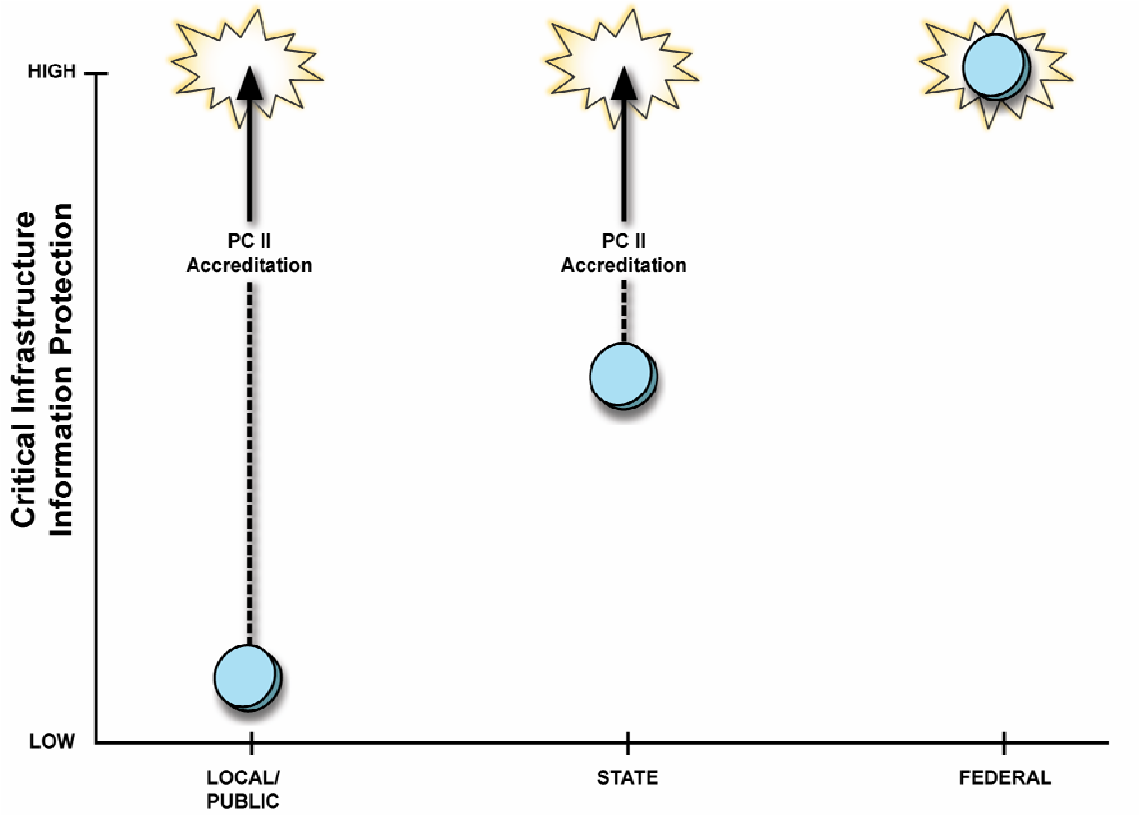


Figure V.A: Using PCII to Enhance Information-Sharing at the State and Local Level

While numerous federal regimes have offered protection from disclosure to various types of information, the PCII Program is the first to have been designed specifically for expansion to the state and local level The current approach is to attempt accreditation for an entire state; it is imperative that PUCs who want to access the PCII coverage regime incorporate their initiatives into state-based efforts, rather than attempting an entirely separate accreditation. This paper suggests that, through obtaining accreditation of a state within the PCII system, information that is sensitive but otherwise subject to uncertain legal protections can benefit from the PCII umbrella.

VI. State-Based Options for Information Protection

This section addresses state-based options for protecting CII outside of the PCII Program context.

PCII could be an important component of states' strategies to protect information, but it is only a part of the whole picture of information sharing and protection. States may also use their own protocols for protecting and sharing information and, in some cases, already use those protocols. These state protocols are important because they offer another way to protect CII for states that do not become PCII accredited, or for situations in which parties want to protect specific information without going through the PCII process.[25]

States take many different approaches to protecting information about critical infrastructure. Some have very little in the way of protocol, others have detailed protocols in place. Most state protocols for protection of information were originally designed to protect commercially sensitive information and, in many cases, state

[25] The PCII Program is broader and stronger protection for information than a protective order. That is to say, if information is classified as PCII, then it has blanket coverage, whereas a protective order only has coverage of that specific material for that trial or proceeding.

commissions have simply applied these procedures to critical infrastructure. This approach works to some degree since it at least establishes protocols. It may nonetheless be worth considering specific approaches to protect CII. Some states have specifically addressed the protection of CII. This section focuses on those states' strategies and discusses them in four categories. These are:

1. Definitions of critical infrastructure;
2. Exemptions from state Freedom of Information Act requirements;
3. Procedures for Protecting Information at the State Level, including information classification structure; and
4. Efforts that state commissions make to avoid becoming custodians of information about critical infrastructure.

The following section describes each of these in turn.

Definitions of Critical infrastructure

Many, but not all, states define critical infrastructure. A definition of critical infrastructure, whether set in statute or in rule, is useful because it helps to avoid conflict about what is or is not critical infrastructure in case of a later argument about who has access to such information. There are essentially two approaches to defining critical infrastructure. One is to develop a state-based definition, an approach that New Jersey has adopted. The other is to define critical infrastructure with reference to federal statutes, as California and a number of other states have done. Each approach is effective, although in an age of multi-state companies and many cross border transactions it can be helpful to refer to one standard definition. In addition, it can help to avoid legal problems of interpretation if different governmental entities use the same terms and define them in the same way.

New Jersey, for instance, defines critical infrastructure as follows:

> Critical infrastructure means any system or asset, including but not limited to, communications, financial, computers, transportation, military, government services, emergency services, water, waste water, and energy and public utility services, vital to this State such that the incapacity or destruction of such systems and assets or parts thereof would have an impact on the physical or economic security and public health or safety of any combination of those matters of this State.[26]

California relies on the federal definition, defining critical infrastructure by making reference to critical infrastructure information, as defined in Section 131(3) of Title 6 of the United States Code.[27] [28] U.S. code defines critical infrastructure as follows: "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would

[26] N.J.A.C. 13:1F-1.4

[27] CA, Ch 476, Section 6254, z(bb)

[28] The U.S. Code definition is: The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems - (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation. (U.S. Code Title 6, Section 132(3)).

have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[29]

Exemptions from State Freedom of Information Act Requirements

One of the first steps that many state legislatures took after September 11, 2001, was to create exemptions from FOIA requirements for CII. By 2003, most states had some kind of FOIA exemption in place and, according to a survey conducted by the National Conference of State Legislatures (NCSL), 49 states now have some kind of FOIA exemption in place for critical infrastructure information in the water sector; in most, but not all, cases exemptions applicable to the water sector also apply to the electricity and telecommunications sector.[30] [31]

Significant questions remain as to how strong these FOIA exemptions are, and as to how they translate into strong information protection protocols upon which utility commissions and utilities can rely. As a result, the strength of the FOIA exemption vary significantly from one state to another. In practice, and as described below, some states such as New Jersey end up relying on a combination of state statutory FOIA exemptions, executive orders and administrative and commission rules. It is likely that many of these FOIA exemptions on their own are still weak protection for CII.

FOIA exemptions essentially fall into three categories, according to the NCSL report:

1. Specific exemptions;
2. States that provide for exemptions with reference to federal law; and
3. States that provide for exemptions in the interests of the general health and security of the public.

Specific Exemptions

Most states provide for specific exemptions. These states list specific types of information that is exempt from disclosure such as vulnerability assessments, blueprints, or security plans. Indiana's law demonstrates this kind of exemption:

> (a) The following public records are excepted [under] this chapter and may not be disclosed by a public agency, unless access to the records is specifically required by a state or federal statute or is ordered by a court under the rules of discovery: A record or a part of a record, the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack. A record described under this subdivision includes: (A) a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism … or an act of agricultural terrorism …; (B) vulnerability assessments; (C) risk planning documents; (D) needs assessments; (E) threat assessments; (F) domestic preparedness strategies; (G) the location of community drinking water wells and surface water intakes; (H) the emergency contact information of emergency responders and volunteers; (I) infrastructure records that disclose the configuration of critical systems such as communication, electrical, ventilation, water, and wastewater systems.[32]

Alabama's law offers another example of a specific exemption, according to the draft NCSL report. Specifically, the law[33]:

> Exempts from public disclosure requirement records concerning security plans, procedures, assessments, measures, or systems as well as other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures. The exemption includes

[29] U.S. Code Title 42 Chapter 68 Subchapter IV-B § 5195c.
[30] "Protecting Water System Security Information -- 2006 Update" by Cathy Atkins, National Conference of State Legislatures, 2006. Available as of 5-24-07 at http://www.ncsl.org/programs/natres/watersecurityupd06.htm
[31] Ibid, reporting that only Minnesota has no FOIA exemption for CI.
[32] Indiana IC 5-14-3-4
[33] Ala. Code §36-12-40 (2006)

> information concerning critical infrastructure and critical energy infrastructure information when the disclosure could reasonably be expected to be detrimental to the public safety or welfare or otherwise is detrimental to the best interests of the public. When a request for such records is received, the statute provides that the public officer receiving the request for records shall notify the owner of such infrastructure in writing of the request and provide the owner an opportunity to comment on the request and on the threats to public safety or welfare that could reasonably be expected from public disclosure on the records.

The Alabama law provides an example of a FOIA exemption that on its own may not offer strong protection to CII. Although it separates exempt information from non-exempt information, it does not offer blanket protection. If someone makes a request to view the exempt information, the owner of that information must re-justify its exempt classification on each occasion.

States provide for exemptions with reference to federal law

These exemptions essentially state that anything that is exempt from disclosure under federal law is also exempt from disclosure under state law. For instance, the Maryland Public Information Act exemption has a provision that mirrors federal FOIA law, essentially providing that any items exempt from the federal FOIA are also exempt from the state FOIA. Maryland SG §10-615(2) says that the state custodian must deny inspection if the inspection is contrary to federal statute or regulation. This is relevant here because that exemption ensures that all PCII litigation occurs at the federal level and not the state level (where a judge may not be as versed in FOIA, PCII, et cetera).

Mississippi's language offers another example.

> "The provisions of this chapter shall not be construed to conflict with, amend, repeal or supersede any constitutional or statutory law or decision of a court of this state or the United States which at the time of this chapter is effective or thereafter specifically declares a public record to be confidential or privileged, or provides that a public record shall be exempt from the provisions of this chapter."[34]

States provide for exemptions in the interests of the general health and security of the public

These exemptions are broadly stated and open to greater interpretation than the specific exemptions. Arkansas code, for instance, gives the utility commission the statutory authority to issue protective orders that cover non-disclosure of confidential or proprietary information. Any information, reports, records, files, books, accounts, papers and memoranda in the commission's possession can be protected when it is in the interest of the public or the interest of the utility to withhold that information from the public.[35]

New Jersey's FOIA law exempts:

> "Emergency or security information or procedures for any buildings or facility which, if disclosed, would jeopardize security of the building or facility or persons therein; and security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software." The act places the onus on the custodian – meaning the state agency -- to prove that a denial of access is lawful.[36]

New Jersey protects information through other means as well, relying on an executive order and administrative code. Executive Order 21 of 2002 provides that the following records are not considered government records and are therefore not available for public inspection, copying or examination: "[a]ny government record where the inspection, examination or copying of that record would substantially interfere with the State's ability to protect and defend the State and its citizens against acts of sabotage or terrorism, or which, if disclosed, would materially increase the risk or consequences of potential acts of sabotage or

[34] Miss. Code Ann. § 25-61-11
[35] Ark Code Ann 23-2-316.
[36] N.J. Rev. Stat. §47:1A-1.1through 1A-6.

terrorism."[37] The Division of Law and Public Safety's Proposed Rule[38] provides that certain records or portions of records are exempt from public access. Specifically, the proposed rule "…excludes from public access under the Open Public Records Act (OPRA) records disclosing any inventory of State and local emergency resources compiled and any policies or plans compiled by a public agency pertaining to the mobilization, deployment or tactical operations involved in responding to emergencies…"[39]

Procedures for Protecting Information at the State Level

State PUCs can use several methods to secure information, ranging from the way in which they store information to specific procedures that set out whom has access to the information to document classification protocols.

Typically, commission procedures will address at least the following in their protocols for handling CII.

- Method in which that information is stored.

  For example, Pennsylvania law (HB 854) requires that CII be kept on site at the utility commission in a secure location, separate from the general records relating to the public utility, where it is available for inspection by authorized individuals.[40]

- Control over who has access to information.

  Pennsylvania's law is again illustrative, stating that only authorized individuals, as designated by the agency, may have access to CII. Typically the test for access to such information would be based on the individual's need to know the information in that person's official capacity as well as binding agreements that the individual may have signed. These agreements would place restrictions on how that information is handled; an example from Colorado is provided below. As might be expected, the more sensitive the information the fewer people have access to it. Commission staff assigned to the case would have access to information in almost all situations, although that access is often granted under specific conditions. Counsel to intervening parties will often have access to sensitive information, subject also to strict limitations that proscribe to whom they can distribute and release that information.

- Conditions under which parties are granted information.

  The conditions under which authorized people are allowed to view information can vary a great deal, depending on how sensitive the information is. For an example, see the Colorado protocol described below.

- Training requirements:

  In some cases anyone who has access to CII must undergo training and sign an access agreement summarizing their responsibilities and personal liabilities.

- Documents are viewed on company premises and not removed from the premises.

- Documents can be distributed at a meeting, but returned at the end of the meeting.

- Documents can be distributed but with a signed document stating no further distribution is allowed.

- Sanctions imposed

[37] Executive Order 21, Governor James E. McGreevey, July 8, 2002
[38] N.J.A.C 13-1F-1 et seq.
[39] N.J.A.C 13-1F-1.4(a) 11
[40] HB 854 of 2005.

States can sanction those who violate the laws that protect CII. Pennsylvania law, for example, specifies that any public official who knowingly releases CII will, upon conviction, be sentenced to pay a fine of no more than $5,000 plus court costs and shall be removed from office or agency employment.

- State commissions can require that CII only be discussed in general terms during the course of a proceeding and not released in pubic documents.

  In Iowa, the Iowa American Water Company asked for a rate increase to cover security-related expenditures. During the hearing the specific security measures were only described in general terms and the Iowa Utility Board's order stated that "The Board will not provide details on how and where security has been upgraded because public disclosure of this information could compromise the security measures. However, after reviewing the information the Board is satisfied that the increased security measures are a reasonable precaution to protect the water supply…"[41]

- Commissions can opt to discuss CII only in-camera with only certain parties present.

- State commissions can issue redacted material. This practice involves publishing and distributing a report with all sensitive information removed.

- In some cases, this might require issuing two reports, one with redacted material that is publicly released and another that is exempt from public release that contains all material.

Information-Classification Structures

Some utility commissions use classification structures to protect CII. These structures typically allow a commission to segregate highly sensitive information from less sensitive information, providing higher levels of protection to the most sensitive information. Document classification systems are not common in state PUCs, although Colorado's two-tiered classification system offers an example of how to differentiate between what the PUC calls "confidential" and "highly confidential" information. Higher levels of classification, such as "highly confidential" in the case of Colorado, imply greater protections and less public access to information. Another more extensive example taken from CIPAC (Critical Infrastructure Partnership Advisory Committee) may offer another example of an approach (see *infra*).

Colorado

In Colorado, confidential material is marked as such by the submitting party, with the approval of the commission, and distributed, with restrictions, to parties to a proceeding. Confidential information, if filed with the Commission, will be sealed by the director of the commission, segregated in the files of the commission, and withheld from inspection by any person not bound by the terms of this rule. This treatment prevails unless the confidential information is released from the restrictions of this rule either through agreement of the parties and publication by the filing party, or pursuant to order of the Commission or final order of a court having jurisdiction.

Where feasible, confidential information is marked as confidential and delivered to counsel for the parties. Where the material is too voluminous to copy and deliver to counsel, the confidential information is made available for inspection and review by counsel and experts. During the inspection, the parties may take notes on the material or request and receive copies of the documents. All notes taken and copies received of such documents are treated as trade secret or confidential information in accordance with this rule.[42]

[41] RPU-01-4

[42]CO Department of Regulatory Agencies, Public Utilities Commission, 4 Codeof Colorado Regulations CCR) 723-1 Part 1, Rules of Practice and Procedure, part1100 d,e

Highly confidential material in Colorado is less well defined. Colorado rules state "to the extent there may be information which a party believes requires extraordinary protection beyond that provided for in these rules the party shall submit a motion seeking such extraordinary protection. The motion shall state the grounds for seeking the relief, the specific relief requested, and advise all other parties of the request and the subject matter of the material at issue."[43] Based on a recent case, treatment of highly confidential material requires:

- Marking of the material as highly confidential on each page;
- Use of a different color paper in the submittal from that used to submit material not deemed as highly confidential;
- Designation, upon filing, of the parties whom the submitter would like to receive the documentation;
- A signed form that those parties receiving the information will sign;
- A restriction placed on those parties receiving the information, requiring them to keep it confidential and the information under their physical control; and
- Procedures for parties to protest classification of the information as highly confidential.[44]
- Note that, for all levels of classification, the problem of digital data is persistent. Revision of most states' classification systems to include digital formats, exchanges, and storage simply has not yet occurred.

Texas

Texas does not have a classification system beyond classifying some documents as Confidential and others as open, public record. While the PUCT does not currently have a classification in place, provisions in H.B. 9 (2003) classify information as confidential if it pertains to emergency response providers, risk or vulnerability assessments, encryption codes and security keys for communications systems, and critical infrastructure.

Information filed in the PUCT Central Records Division is only confidential if it is filed under seal. There are rules governing what is considered confidential, including PUCT §21.77. The rules currently in place allow any member of the public to view anything filed in Central Records that is not marked "Confidential." For example, maps of transmission lines, testimony for a certificate of convenience and necessity (CCN), or evidence from a rate case can be accessed by any member of the general public if it is not designated confidential. The PUCT also adheres to the Texas Public Information Act (TPIA).

Generally, competitive information that is provided during a case is under seal and can only be viewed by non-competitors. This information is usually not presented in a hearing because it is too difficult to seal a hearing record. During cross-examination in a hearing, the attorneys will usually ask general questions that will not require the use of the competitively sensitive information.

Other Models for Information Classification

States have the option to develop much more detailed and explicit information classification systems as well. Several models exist, but one model is that used for the DHS Critical Infrastructure Partnership Advisory Council (CIPAC), which may be particularly useful. This guidance uses several classifications of sensitive information, three of which are summarized below.

(1) "COMMERCIAL/PROPRIETARY SENSITIVE" applies to information such as trade secrets, or information that would harm the competitive position of a company. This information is available only to badged and credentialed Federal and State law enforcement officers, agents, and their analyst personnel as authorized by law and regulatory policy; members of the Intelligence Community as authorized by law and

[43] [43]CO Department of Regulatory Agencies, Public Utilities Commission, 4 Codeof Colorado Regulations CCR) 723-1 Part 1, Rules of Practice and Procedure, part1100 aIII.
[44] CO Public Utilities Commission DOCKET NOS. 04A-411T and 04D-440T , 2004

regulatory policy; and non-regulatory members of Federal and State government entities with an official need to know the information.

"SENSITIVE – FOR OFFICIAL USE ONLY" applies to documents such as comments that industry might submit to DHS on draft versions of sector-specific plans. Another way to describe this is Governmental Proprietary or Pre-decisional Information. This information is generally accorded limited access only to badged and credentialed Federal and State law enforcement officers, agents, and their analyst personnel as authorized by law and regulatory policy; members of the Intelligence Community as authorized by law and regulatory policy; and non-regulatory members of Federal and State government entities with an official need to know the information.

"LAW ENFORCEMENT SENSITIVE" is used for documents or information that is likely subject to retention under certain federal FOIA exemptions, including law enforcement sources, methods, means, tactics, or procedures that are not publicly known or if publicized could jeopardize of law enforcement efforts. Such information is generally accorded limited access only to badged and credentialed Federal and State law enforcement officers, agents, and their analyst personnel as authorized by law and regulatory policy; and members of the Intelligence Community as authorized by law and regulatory policy. PUC personnel may not have access to such information except in circumstances in which they have been given security clearances.

Efforts that State Commissions Make to Avoid Becoming Custodians of Information About Critical Infrastructure

Some states' commissions try to avoid becoming custodians of CII at all. By doing so, they avoid the procedural and other questions that becoming a custodian of such information implies. Three examples from Iowa, Michigan, and Texas describe this approach.

Iowa

The Iowa commission made a choice, in the wake of the September 11, 2001 attacks that it was not capable of keeping CII secure, and elected not to collect it. This situation may be somewhat unique to Iowa in that according to Iowa law, all information filed with the Iowa Homeland Security and Emergency Management Division can be deemed vital to security and shielded from the Iowa Open Records Law as a result. Most records of the Iowa Utilities Board are not exempted as a result of this law.

Michigan

Michigan's PSC has dealt with two cases in which utilities have requested recovery for security related expenses at nuclear power plants. In on case the utility submitted the request for cost recovery without detailing those expenses and the Michigan PSC granted cost recovery for those expenses.[45] In another case the PSC staff visited the utility offices and inspected paperwork that described the security-related expenses, but did not go into specific detail about how the money was spent. In neither case did the PSC take possession of critical infrastructure information, so there was no need to use protective measures.

In another situation the Michigan PSC asked the state's utilities to report on what measures they were taking to safeguard their critical infrastructure. In order to complete this report the Commission staff met with the utilities and received oral reports without taking material back to the Commission offices—again meaning that they did not become custodians of CII.

While Michigan's PSC has elected not to collect any information they may not need to retain, there remains the ability to exempt much of this information from disclosure under an exemptions provision contained in Michigan's FOIA (section 13(1)(Y)) dealing with internal and security matters.

Texas

[45] Case U-13808 of the Michigan Public Service Commission.

To protect sensitive information on critical infrastructure, the Public Utilities Commission of Texas (PUCT) currently requests that utility companies only file a summary of their emergency response plans rather than a complete copy of the plans. Members of the general public have access to these records, and according to staff at the PUCT, it is in the best interest of the companies to only file a condensed version.

Special Considerations: Data in the Digital Age

After thousands of years dealing in paper records, the past half-century has seen a shift in data creation, transmission, and storage: more than 70 percent of all records are digital. While paper-based protection protocols are well-established, both the management and mismanagement of electronic materials are less well understood. Since 1990, the legal system has struggled to understand and address digital materials appropriately. The Gramm-Leach-Bliley Act (1999) sought to force responsibility for digital security to the Board level; Sarbanes-Oxley (2002) pressed liability for leaks of digital data pertaining to individuals; the Health Insurance Portability and Accountability Act of 1996 gradually resulted in follow-on regulations that brought medical privacy rules into the digital realm. Most recently, the California Identity Theft and Fraud Act moves toward a regime of penalties for data breach, and requires notification of potentially affected parties.

As a result of these and other laws—several important cases imposing fines and penalties on large corporations for data leaks, and the growing availability of user-friendly, affordable data-security technology—the general rule is that the protections and penalties that apply to paper information also apply to digital information.

Data encryption is an effective part of a strategy for electronic data protection.

Electronic devices requiring encryption for participants in the PCII Program:

- Required: Internet, High Frequency or Other Radio Signals (cell phones)
- Not required: Wireline Telecon Networks, Faxes, E-mail (but strongly encouraged).

While in theory this is an appealing approach, applying it may present challenges. Uncertainty remains more common than comfort, in all sectors. States and localities have not all adopted or maintained a consistent approach to digital security. Outsourced records management, forwarded emails, and lax data destruction plague almost all organizations outside the intensively regulated financial-services and healthcare sectors. And cyber criminals continue to develop ever-more-sophisticated tools.

At the risk of repetition, the uncertainty surrounding digital information management provides another reason to refer to the PCII Program. Those accredited for PCII must adhere to a specific, although simple, set of digital data-management rules.[46] Violation of these rules carries specific penalties.

An approach that spells out which digital protection mechanisms apply to which devices, and details penalties for failing to observe these mechanisms, is sound. Dovetailing a state approach with the PCII Program's digital data-management rules may – as in other areas of legal concern – provide some level of direction about how to proceed, and some level of comfort to those whose data is submitted.[47]

In this realm, as in the others where PCII-style approaches are discussed, there remains, as of this writing, a fair amount of legal uncertainty. If all goes well, there will be lawsuits in the next decade about the use or abuse of the PCII Program. If there are problems or damaging disclosures, we will see greater clarification emerge in the courts. Unfortunately, there is no detour around this gray area.

[46] See Appendices for more information on the specific compliance regime for PCII.

[47] There is, at this time, no research on state-based approaches to digital data management. Surveying the states and the PUCs to determine what the range of current practices – if any – are, and digesting them to determine whether they align with recommended practice or with the PCII Program approach, would be a useful endeavor.

VII. Conclusion and Options for Consideration

This paper has attempted to demonstrate the importance of sharing information about critical information, the challenges to sharing that information, and the federal and state context for the sharing of that information. It has focused heavily on the new PCII Program because that program offers a new and potentially effective method for states, local government, the federal government, and private industry to share information about critical infrastructure. There are a number of questions about the PCII Program remaining because it is so new; however, it appears to offer a new and effective path to trusted information sharing.

The document has also outlined state level information sharing protocols, discussing specific methods for gathering, storing, and protecting hard copy and electronic information. This, too, is an evolving area, particularly because many information protection protocols up until this point have been heavily focused on protecting commercial information rather than security-sensitive CII.

This paper offers a set of next steps for states to consider. The most compelling – that is, the steps most likely to generate a measurable improvement in the ease of dealing with CII – are threefold. States and state PUCs can:

1. Adopt PCII into the state, explicitly making the PUC an authorized user
    - By securing state PCII accreditation, the state – and by extension the state PUC – have access to the strong information protection protocols of the PCII program. One key to the success of this for PUCs is to make sure that the PUC is well integrated into the state's accreditation procedures.
2. Promote the consistent use of the term and definition of CII
    - By using a single term, preferably a term that is recognized around the country such as CII, states maximize the uniformity of likely legal recognition granted to their procedures regarding CII. Uniformity minimizes uncertainty, which is a primary concern of industry.
3. Establish a confidential hearing process for CII matters, if one does not yet exist.
4. Establish a procedure for sensitive information that may be needed by a PUC to discharge its responsibilities and which may not be covered by PCII. This could include:
    a. Defining who can gain access to the information and how it can be controlled; and
    b. Establishing protocols for data storage, transmittal, and handling.

A number of other adaptations to accommodate the emerging role of CII in regulated utilities would support these steps. These include:

- Distinguishing legally between commercially sensitive information (e.g., proprietary data, trade secrets) and information that is sensitive because it pertains to security
    - This issue is particularly important in the states that have information sharing protocols that are based primarily or exclusively on their concerns about sharing commercial-proprietary information. Protocols for CII should reflect the need to protect a different class of information, with a focus on information classification, labeling, and management structures.
    - States that do not distinguish between commercially sensitive information and information protected for security reasons (CII) risk challenges in the legal system on grounds of void-for-vagueness and overbreadth.

- Promoting FOIA laws that mirror Federal FOIA, thus providing protection to documents that are already protected under Federal FOIA
    - Mirror provisions in FOIA laws simplify the applicability of information protection programs, such as the PCII Program.
- Conducting work within NARUC to develop language describing recommended standards for information protection that states can consider for adoption, as well as sample roadmaps for how to move forward; and providing educational outreach to states – both PUCs and other stakeholders, such as Governors' offices and Mayors' offices – about how these roadmaps can work in their state. Such a standard might address items such as information, classification systems, lockable file cabinets, encryption and other digital-protection protocols, et cetera, that states can use to protect CII. Consider applicability of the DHS CIPAC information classification guidance to this effort
- Affirmatively support DHS' initiative to create a new state-focused body to take on this challenge and promulgate discussion and consensus surrounding how to move forward, including sample language for these options

In sum, this paper has offered an overview of the range of options that states already pursue for keeping Critical Infrastructure Information protected. In addition, it offers for consideration a new option: leveraging the emerging PCII program structure to facilitate the end goals of utility commissions and industry alike.

VIII. APPENDICES

Appendix A: Situations in Which Utility Commissions Address Critical Infrastructure Information - Specific Examples

State commissions address critical infrastructure information issues in four primary contexts: rate cases, siting applications, reports and investigations and in their advisory capacity. Not every state commission is involved in every one of these activities. This appendix describes each of these situations in more detail.

a. Rate Cases

Commissions conduct proceedings according to their rules that consider and approve the rates that utilities charge their customers. The rates that utilities charge are based on their costs in categories such as telecommunications switching equipment, water pumping, land acquisition, computer equipment, power plants, and the security systems to keep all of such critical infrastructure safe. Utilities need to be guaranteed a reasonable chance of rate recovery for their security related costs, assuming they were prudently incurred, but some utilities have said that they are concerned about presenting detailed information to their regulatory commission for fear that the information could be released and end up in the hands of people who could damage the utility network. The practical application of protective orders and CII policies has so far been relatively uncommon for security costs, and more common for commercially sensitive information. For example:

In Texas through Docket No. 32907, Application of Entergy Gulf States, Inc. for Determination of Hurricane Reconstruction Costs, the Company proposed that its reconstruction costs should be fully recovered. This application, which was filed on July 5, 2006, was approved on December 1, 2006. Throughout the process, any financial information such as depreciation and capital cost information was filed confidentially. Only staff members who are assigned to this case would be allowed access to this information; other parties were not permitted to view this information nor was it publicly available.

b. Siting Cases

Some commissions issue siting certificates and certificates of need for new power plants or other major utility equipment. Although, in general, siting applications do not require detailed information about the security systems for specific facilities, the applications might include information about the need for the new facilities. New facilities might be required to shore up a weakness in an electric utility's power delivery system, for example. Information about these system weaknesses would be useful to the commission, and might be requested by other parties intervening in the case. Utilities might be reluctant to provide such information without giving it some type of protected status.

c. Utility and commission reports

Utilities commissions are frequently asked to make reports to the state legislature. In other cases utilities are often required to provide reports to the utility commission; one common type of such a report is the Integrated Resource Plan, prepared in more than 20 states. Such reports often rely on CII as background, presenting that information in summarized form.

For example, the Pennsylvania Public Utilities Commission required that the utilities under its jurisdiction self-certify as to the security of their physical and cyber system. The Commission ordered that the reports detailing the self-certification be kept at the Commission's premises, but under an automatic protective order, thus restricting the people who would be able to view the reports.[48]

[48] Physical and Cyber Security Program Self-Certification Pennsylvania: Requirements for Public Utilities; Doc. No. M-00031717.

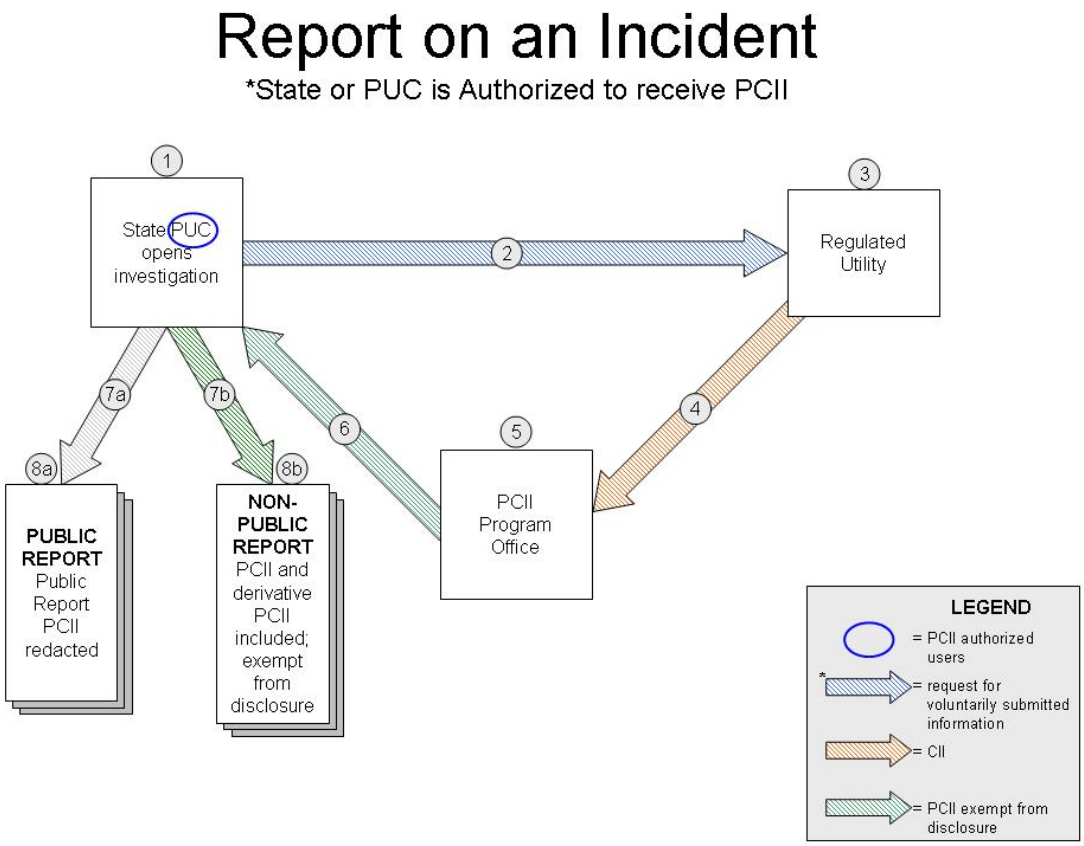
In another example, the Colorado Public Utilities Commission conducted a report on the causes of a blackout affecting 370,000 customers in February of 2006.[49] In this case, the utility met with the Commission staff and committed to file a report on the causes of the service interruption. The company filed two versions of the report, one labeled as highly confidential and another public version with the commercially- and security-sensitive information removed.

d. Some Commissions Act as Advisors to Governors, or participate in state homeland security committees

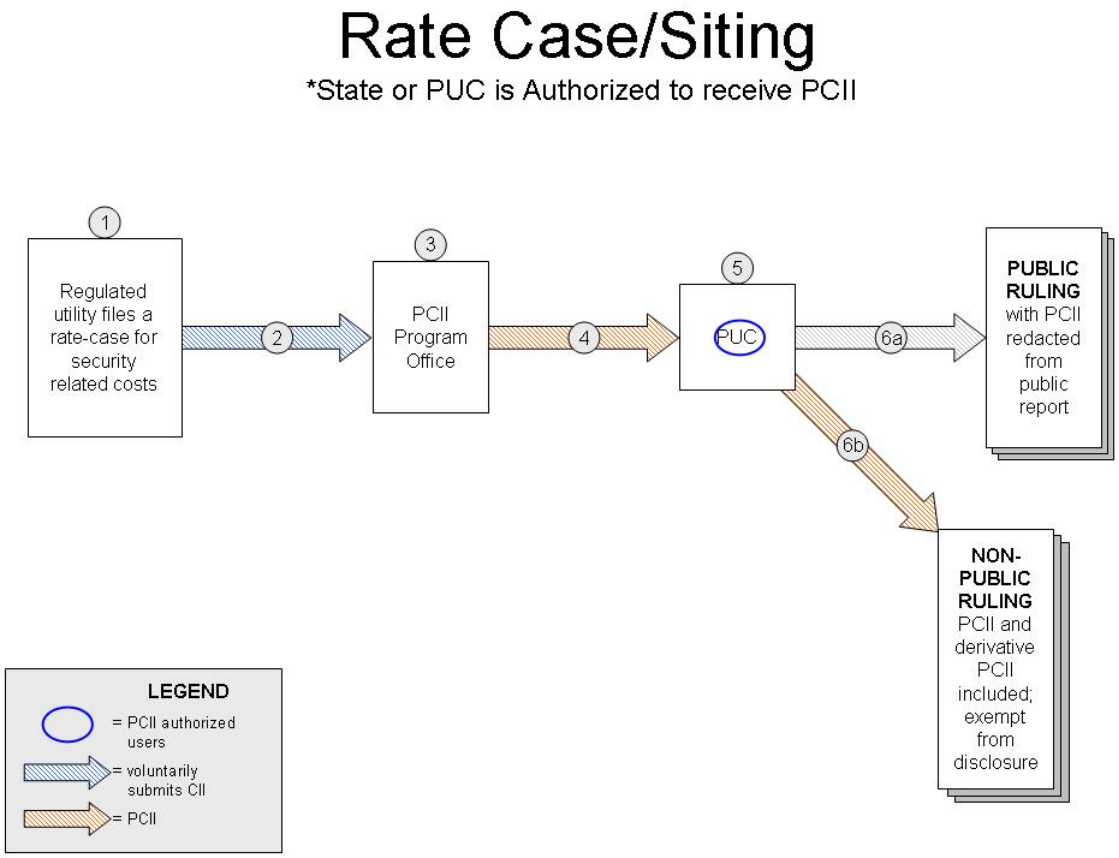
In some states, the public service commission staff advise the governor on energy security matters, or they may be the government expert in case of an energy emergency, as is the case in Colorado. In Michigan, the Public Service Commission (MPSC) staff have been working with the Michigan State Police's Emergency Management and Homeland Security Division with regard to the protection of energy and telecommunication critical infrastructure. In this role—because state public utility commissions, including Michigan's, are responsible for a reliable supply of energy and the reliability of telecommunication systems—the MPSC staff has collected some information on critical energy and telecommunication facilities that is considered sensitive and which is exempt from disclosure under Section 13(1)(y) of Michigan's FOIA. Note, though, that this activity takes place under the duties of the advisor role, not the regulatory role. Access to homeland security sensitive material is restricted to a limited number of personnel and it is held in a secure manner. In addition, some information has been obtained under non-disclosure agreements between the State of Michigan and the private sector. The legal basis that has allowed for a non-disclosure agreement to be signed is among the state's FOIA exemptions.

[49] Docket No. 061-118EG Before the Public Utilities Commission of the State of Colorado in the Matter of the Investigation of the Report of Events that Let to Controlled Outages February 18, 2006 – Public Service Company of Colorado. Mailed Date: July 13, 200 Adopted Date: July 7, 2006

Appendix B: Graphic Illustrating the PCII Program's Applicability to the Relationship Between PUCs and Regulated Utilities

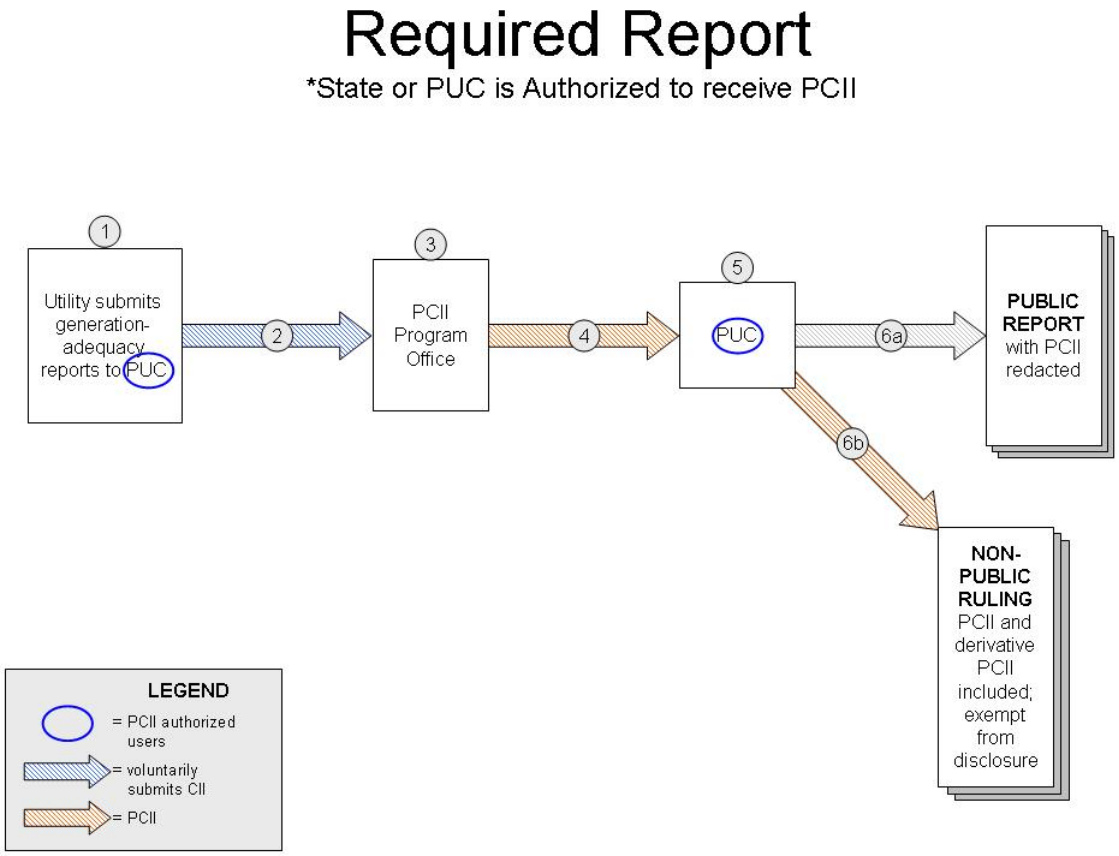


a. Report on an incident: In this case, a PUC—an authorized PCII user (either via state accreditation or entity-specific accreditation)—opens an investigation into an incident such as a blackout. It would submit a request for voluntarily-submitted CII to the regulated utility. If the regulated utility consents, it would send the CII to the PCII Program Office at DHS and the CII would be certified as PCII. The PCII would, in turn, be sent to the PUC and that information—and product derived therefrom—would be exempt from disclosure under federal, state, and local disclosure laws and during civil litigation. Upon receipt of the PCII by the PUC, it could file a public report that redacted any PCII or its derivative product; it could also issue a non-public report to PCII-authorized users with the PCII and its derivative product included. Notwithstanding the existence of the public report, the PCII in the non-public report would be exempt from disclosure under federal, state, and local disclosure laws as well as during civil litigation by the Critical Infrastructure Information Act of 2002.



b. Rate Case/Siting: In this case, a regulated utility is seeking to increase its rates due to investments made for security-related enhancements. In order to provide the necessary information, the regulated utility wants proper assurances that the submitted security-related information will not be disclosed under applicable disclosure laws. Under the scenario described in the flowchart above, the regulated utility would voluntarily send the security-related information (CII) to the PCII Program Office. According to discussions between SRA and the PCII Program Office in December 2006, the state PUC can be PCII-certified and have a direct relationship with the PCII office; information thus can come directly to the PUC as opposed to being sent through another state office. The PCII Program Office—in less than a day—would validate the CII as PCII and send it to the PUC for rate-case judgment. Other interveners would not have access to this PCII information unless they were also PCII-authorized. Upon receipt of the PCII by the PUC, it could file a public ruling that redacted any PCII or its derivative product; it could also issue a non-public ruling to PCII-authorized users with the PCII and its derivative product included. Notwithstanding the existence of the public ruling, the PCII in the non-public ruling would be exempt from disclosure under federal, state, and local disclosure laws as well as during civil litigation by the Critical Infrastructure Information Act of 2002.

In some states, this approach may be problematic because it places too many restrictions on which information can be distributed to non-PCII-authorized parties to the case. This PCII approach is more restrictive than an administrative order, for example, that typically allows information to be distributed to parties that have agreed to abide by specific information handling protocols (see section, above, that addresses state information management protocols). States will need to consider how this PCII approach fits with their own administrative procedures. If appropriate, states may consider whether it is necessary to make changes to their administrative procedures that allow rate case rulings on security related expenditures even when the PCII information is unavailable to most parties to the case.



c. Required Report: In this case, the utility is required to submit a report to the PUC, such as a generation-adequacy report. Upon receipt of the report, the PUC would submit the report to the PCII Program Office. The PCII Program Office would validate the CII in the report as PCII and send it back to the PUC. The PUC could then file a public report that redacted any PCII or its derivative product; it could also issue a non-public report to PCII-authorized users with the PCII and its derivative product included. Notwithstanding the existence of the public report, the PCII in the non-public report would be exempt from disclosure under federal, state, and local disclosure laws as well as during civil litigation by the Critical Infrastructure Information Act of 2002.

Appendix C: Requirements for State Compliance with PCII

The CII Act limits the purposes for which state, local and tribal governments may use PCII and how state, local and tribal governments may share PCII. PCII may not be used by those governments for purposes other than protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act, and an agency of those governments may not further disclose the information without the consent of the submitter.

In general, before federal, state, or local government entities may access and store PCII, they must have executed a Memorandum of Agreement (MOA) with the PCII Program and have met the requirements of the PCII Accreditation Program. The construction of the PCII Accreditation Program's requirements has taken a great deal of time, but now appears to be solidified and user-friendly.

The accreditation process was established to provide oversight and to ensure that each entity (such as a state) and user (such as a state official) has a clear understanding of how to initiate and manage their entities' program and adequate policies, procedures, secure systems, and databases for handling, using, sharing, and safeguarding PCII. The PCII Program's Operations Branch is responsible for managing the process. The following are the key steps in the accreditation process:

1. After a government entity, such as a state, determines its need to access PCII data, the entity requests an application for PCII accreditation from the PCII Program Office and nominates a PCII officer and deputy. Any nonfederal government employee who is nominated to be a PCII officer or deputy must sign a nondisclosure form. The application requests points of contact, entity-mailing address, initial identification of PCII Officer and Deputy, proposed use of PCII, et cetera. Once the application is received, the steps below can be completed in any order. The PCII Program Office, however, recommends that the PCII Officer be familiar with the PCII Program requirements and policies that, in turn, help to facilitate the completion of the self-inspection plan.
2. The PCII Program Office appoints the nominated PCII Officer and deputy for the candidate entity (such as a state) after they complete a three-day training course and pass a certification examination. The PCII Officer and Deputy are responsible for the management and oversight of the PCII Program within the State.
3. A senior official with the authority to represent the candidate entity (such as a state homeland security director) enters into an MOA with DHS. The MOA constitutes an entity wide obligation and an executive-level commitment to achieving and maintaining PCII accreditation. In addition, it sets for the responsibilities and obligations of the PCII Officer and deputy as well as the requirements for handling, using, sharing, and safeguarding PCII throughout the federal, state, or local entity.
4. The PCII Officer develops a self-inspection plan that outlines the methods by which oversight will be performed on the use of PCII within the PCII Offier's organization. The PCII Program Office reviews the self-inspection plan and works with the accreditation candidate's PCII Officer to address any needs for further development activities. The Self-Inspection Plan provides the guidelines by which PCII Officers will perform their oversight responsibilities. Examples of information that the PCII Officer may ask while performing oversight may include:
    a. How the State safeguards and handles PCII;
    b. Who was PCII data shared with and via what mechanism?
    c. Importantly, the PCII Program Office will provide a template off on which the State can simply sign.
5. After the above requirements are fulfilled, the PCII Program Office will issue an interim accreditation notice and the initial accreditation process is complete.

6. After a probationary period, the PCII Program Office accredits the government entity. The PCII Officer must submit an annual report to the PCII Program Office to keep the office appraised of any developments in the participating entity's PCII program. A fully-accredited entity must be reaccredited every three years. In addition, the Program Office may also elect to conduct a site visit of an accredited entity at any time to ensure that the minimum requirements are continually being met or to respond to requests for consultation or guidance from the entity.
7. In order for an accredited entity to maintain its accreditation, it must demonstrate compliance with PCII safeguarding and handling requirements. This is demonstrated by the PCII Officer providing the results of its auditing and oversight to the PCII Program Office in the form of an annual report.
8. Importantly, individuals within the State who need access to PCII are required to complete PCII-authorized user training (this training is accomplished via an online training that can be emailed to the individuals who need it) as well as a non-disclosure agreement for non-Federal employees.

Appendix D: Further Detail on the Colorado incident

The blackout incident referenced in the main text above created a chain of events that illustrate the dynamics in the exchange of sensitive information between utilities and utility commissions. In this case, a Commission order addressed a number of issues affecting how the PUC would treat the sensitive information coming out of this study.

- The company requested that access to the Highly Confidential Version be restricted to the Commissioners, the Staff, consultants working with the Staff on Staff's investigation in the Docket, the Office of Consumer Counsel (OCC), and the attorneys representing each of the those parties.
- The company also requested that all persons other than the Commissioners be required to execute Non-Disclosure Agreements provided to the Company prior to obtaining access to the Highly Confidential Information. It maintained that the security of the Company's gas and electric operations and/or the strength of the Company's bargaining position with key suppliers could be adversely and significantly affected by public disclosure of this information.
- The company also requested that anyone from Staff or OCC that accesses the Highly Confidential information sign a Company provided non-disclosure agreement.
- The company also requested that should the Commission open another docket related to follow-up matters from this docket, that the documents classified as highly confidential in this docket should also be classified as highly confidential in the following docket. The company stated that it was willing to consider whether to reclassify those documents as confidential at a later time.
- The Commission ruled that only the specific parties to the case, identified above, should be allowed to see the highly confidential documents. It however saw no reason to require those parties to sign an additional non-disclosure document. It also stated that the company would need to file a second request for the documents to remain confidential in a future docket.

Appendix E: Frequently Asked Questions for Electronic Submission of Critical Infrastructure Information Regarding the PCII Program

1. *What safeguarding procedures has the PCII Program Office put in place to ensure secure transmission of CII?*

   Submitted files are encrypted in transit to prevent access to anyone except the PCII Program Office. All files are checked for viruses or malicious code before being stored in a stand-alone database maintained in a secure location.

2. *How will submitters know the PCII Program Office has received its submission?*

   A confirmation e-mail will be sent by the PCII Program Office and include a confirmation number verifying receipt of the submission. Once the submission is validated, the PCII Program Office will provide a tracking number that can be used to reference the submission when additional information is provided or other actions are required.

3. *At what point does the PCII Program Office protect electronic submissions from disclosure?*

   Electronic submissions are protected from public disclosure immediately upon receipt and throughout the validation process. If a submission meets the qualifications for protection under the CII Act, the submission retains protection. If a final determination is made that the submitted information does not qualify for PCII protection, the PCII Program Office will either return the information to the submitter in accordance with the submitting person or entity's written preference or destroy the submission in accordance with the Federal Records Act and Department of Homeland Security regulations.

4. *How long will it take the PCII Program Office to validate a submission to determine if it qualifies for protection under the CII Act?*

   The PCII Program Office will make a validation determination as quickly as possible. Several factors affect how quickly the information can be validated, such as:

   ♦ *Submission Completeness:* At times, the Program Office will need additional information from a submitter in order to complete the validation determination. In such cases, validation depends directly on how quickly the submitter responds to the request. If the submitter does not remedy the deficiency within 30 days of the request, the PCII Program Office may either cure the deficiency or inform the submitter that the submission does not qualify for PCII protection. In the latter case, the PCII Program Office will either return the information to the submitter in accordance with the submitting person or entity's written preference or destroy the submission in accordance with the Federal Records Act and Department of Homeland Security regulations.

   ♦ *Volume of Submissions Received:* Although the overall volume of submissions cannot be predicted, the Program Office has measures in place to expedite the approval process so validation can be completed as quickly as possible.

5. *Can submitted CII be withdrawn?*

   Yes. A submitter may withdraw a submission at any time before a final determination has been made as to whether or not the information qualifies for PCII protection. The PCII Program Office will either return the information to the submitter in accordance with the submitting person or entity's written preference or destroy the submission in accordance with the Federal Records Act and Department of Homeland Security regulations. The submitter is not required to provide a reason for this request.

6. *What happens if connectivity is lost or the computer system crashes during the submission process?*

   If the connection fails, or the computer system crashes at any time during the submission process, the information submitted will be lost. This is also the case if the submitter hits 'Cancel' before completing the submission process. The submitter must start the submission process from the beginning.

7. *How should information be submitted that cannot be sent electronically?*

   Information that cannot be sent electronically can be sent directly to the Program Office via registered mail, U.S. mail, courier delivery, or facsimile transmission. Information should be sent to:

   PCII Program Office
   Department of Homeland Security
   245 Murray Lane, SW, Building 410
   Washington, DC 20528-0001