State Protection of Critical Energy Infrastructure Information (CEII)

JESSICA RACKLEY | NATIONAL GOVERNORS ASSOCIATION
jrackley@nga.org | 202-624-7789

Summary

States are developing rules to better facilitate the exchange of sensitive information needed to protect critical energy infrastructure from cyber and other threats. Owners of critical energy infrastructure information (CEII) can mitigate physical and cyber risk by sharing vulnerability, threat, location or design information with government and industry as this information is important for energy planning, emergency response and outage restoration. However, to facilitate information sharing, asset owners must be able to trust that their sensitive information is securely managed, stored and shielded from public disclosure. Consequently, more than half of the states have established laws that exempt CEII from being released as part of Freedom of Information Act (FOIA) and other public disclosure requests.

CEII DEFINITION

The Federal Energy Regulatory Commission (FERC) has established regulations to govern how CEII from the bulk-power system is managed. Many states look to FERC's definition as a model.

"*CEII is engineering, vulnerability, or design information about proposed or existing critical infrastructure (physical or virtual) that relates details about the production, generation, transmission, or distribution of energy; could be useful to a person planning an attack; and gives strategic information beyond the location of critical infrastructure."*

The U.S. Department of Energy (DOE) also issued a Notice of Proposed Rulemaking in October 2018 to address CEII.

Background

This policy scan explores state laws that protect CEII from public disclosure, addresses court rulings protecting sensitive data for other infrastructure types and explores how states are protecting shared critical data from cyberattacks and cyber theft.

Thirty-one states have open government law exemptions that cover CEII.[1] The breakout is as follows and shown in the map below:

- Twenty-eight states have adopted statutory exemptions from open government laws for critical infrastructure information (CII, defined as systems and assets, whether physical or virtual, so vital that their incapacity or destruction would debilitate social or economic security;[2] CEII is a subset of CII).
- Three other states, **Hawaii**, **Minnesota** and **Washington**, do not explicitly exempt CEII, but language from court cases, opinion letters or general statutory language is interpreted to contain this exemption. Only a few states list a specific state agency and/or authority that is exempted from open disclosure requirements (e.g., **Iowa**).

States define critical energy information differently. For example, **Missouri**, **Nebraska** and **North Carolina's** laws exempt disclosure of information about "infrastructure" while other state statutes use the phrase "energy infrastructure."

How states manage CEII, such as labeling and storing this data, is important to prevent data leaks that could expose businesses and critical infrastructure to cyber vulnerabilities. Often state agencies such as utility regulators determine procedures for protecting CEII from being obtained by outside parties that may be a threat to critical energy assets.

NATIONAL GOVERNORS ASSOCIATION

State Protection of Critical Energy Infrastructure Information (CEII)

Examples of Statutory Exemptions of Energy Information

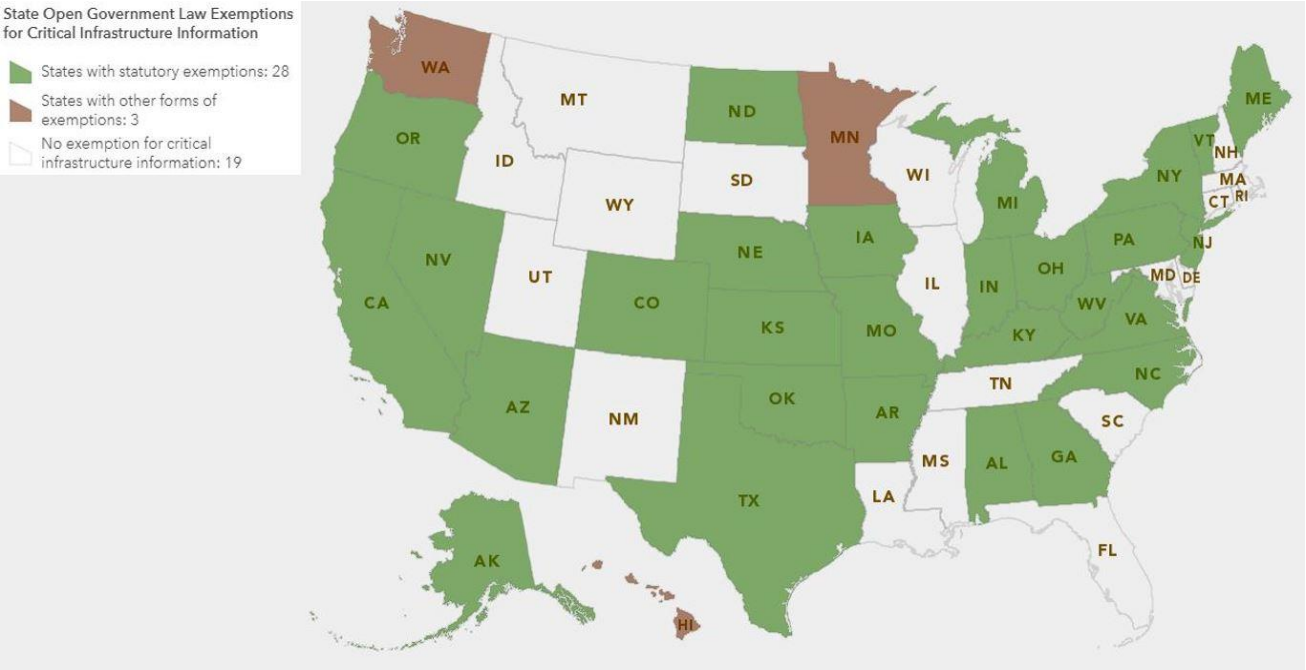
The state statutory provisions listed below demonstrate the diverse ways of protecting CEII information.

Arkansas
Ark. Code § 25-19-105 exempts CEII from mandatory disclosure and includes language referencing those protections listed under federal law such as the Critical Infrastructure Information Act of 2002, which prohibits the disclosure of certain information submitted to the U.S. Department of Homeland Security; and rules of the Federal Energy Regulatory Commission addressing CEII. The code also addresses the importance of protecting the security for any public water system or municipally owned utility system and includes protection "plans and related information for generation, transmission, and distribution systems."[3]

Iowa
Iowa lists specific state agencies from which records are confidential, such as the state utilities board, and includes categories of protected energy-related infrastructure. Code §22.7 (71) lists those records "held by the utilities board of the department of commerce or the department of homeland security and emergency management for purposes relating to the safeguarding of telecommunications, electric, water, sanitary sewage, storm water drainage, energy, hazardous liquid, natural gas, or other critical infrastructure systems."

Minnesota
Minnesota does not explicitly exempt CEII, however it does make some energy data nonpublic. Minn. Stat. §13.68 Subdivision 1 defines nonpublic data as "Energy and financial data, statistics, and information furnished to the commissioner of commerce by a coal supplier or petroleum supplier, or information on individual business customers of a public utility."

Pennsylvania
Pennsylvania has detailed language on CEII exemptions in 65 Pa. Stat. §67.708 (b).[4]



The map was developed with Esri's GIS software, data from the National Conference of State Legislatures, and state outreach. Information for the territories was unavailable.

Pennsylvania's exemption covers records that create a "reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system." The statute addresses the need to protect against a "terrorist act," and defines as critical and protected "risk analysis; threat assessments; consequences assessments; antiterrorism protective measures and plans; counterterrorism measures and plans; and security and response needs assessments." Records that also contain locational or configuration information for critical systems including public utility systems, electrical, water, wastewater, sewage and gas systems are protected.

Pennsylvania also includes details on how CEII information should be stored and who has access to the information. The law requires that CEII be kept on site at the Public Utilities Commission (PUC) in a secure location that is separate from general records (Enacted into law as Act 156 of 2006). Pennsylvania law also states that only authorized individuals, as identified by the PUC, may have access to CEII.[5]

State Court Rulings Related to Protecting Critical Infrastructure Information (CII) [6]

In recent years, many states have amended their public disclosure laws to exempt information about critical infrastructure. State courts have upheld these exemptions but also ruled that they should remain narrowly tailored.[7] Based on past court cases, if the requested information reveals the nonpublic location of critical infrastructure, courts have typically upheld a state's decision not to disclose the information.[8]

California
Under a California Public Utilities Commission (CPUC) filing, Pacific Gas and Electric Company, Southern California Edison and San Diego Gas & Electric Company sought to redact customer-identifiable energy use information and critical energy infrastructure information pursuant to the June 8, 2018 *Administrative Law Judge's Ruling … Confidential Treatment and Redaction of Distribution System Planning Data Ordered by Decisions 17-09-026 And 18-02-004* ("ALJ Ruling"). The three investor-owned utilities (IOUs) requested that the CPUC accept their individual, amended 2018 Grid Needs Assessment reports with this redacted distribution system CEII data. The CPUC issued a ruling on these CEII concerns in July 2018. The CPUC found that the IOUs failed to articulate uniform and specific criteria for identifying CEII that would merit redaction, and the CPUC adopted uniform criteria for identifying data that should be classified as CEII outlined in this ruling. The CPUC states that it will be up to each IOU "to show that every data set it wishes to redact fits within the criteria."[9]

Washington
As noted earlier, Washington's CII exemption is not set by statute, but determined through a court ruling, which is now applied to similar requests in the state. In 2007, the Washington Court of Appeals interpreted a statute to exempt CII from its Public Records Act. This court case involved an information request seeking data on natural gas pipeline infrastructure. The court ruled that the Washington Utilities and Transportation Commission (WUTC) was not required to disclose this data after more than 20 natural gas industry organizations stated that the pipeline system is part of CII in the state and that destruction of this system would have dire outcomes.[10]

Cybersecurity Exemptions Focused on Critical Infrastructure or Utilities

The state statutory provisions listed below demonstrate the diverse ways states exempt the

disclosure of certain data to prevent cybersecurity threats.

Connecticut
Since 2002, procedures submitted by Connecticut water companies for "sabotage prevention and response" have been exempt from disclosure under the state FOIA statute.[11] In June 2017, the state expanded that protection to records filed by a water company with any public agency that contain, among others: cybersecurity plans and measures, supervisory control and data acquisition systems, information and communications systems, vulnerability assessments, internal security audits, security training, emergency contingency plans and emergency preparedness plans, network topology maps; and "any other record if … disclosure may create a safety risk."[12]

Florida
In the past two years, Florida added four cybersecurity exemptions, one of which applies to records controlled by local public utilities.[13] The state now shields records related to "technology, processes, or practices" designed to protect a utility's systems from attack, as well as information concerning "existing or proposed IT systems or industrial control technology systems" but only if disclosure would "facilitate" a data breach or an attack that could "adversely impact the safe and reliable operation of the systems and the utility."[14]

Idaho
Idaho's cybersecurity exemption covers records held by any public agency that are "related to proposed or existing critical infrastructure" if disclosure "is reasonably likely to jeopardize the safety of persons, property or the public safety."[15] For purposes of this exemption, critical infrastructure means any system, "whether physical or virtual" and including electrical, computer or telecommunications systems, whose disruption "would have a debilitating impact" on economic security, public health, safety or any combination of those matters."[16]

Kansas
In 2013, Kansas passed a law protecting public utility records concerning information about "cybersecurity threats, attacks, or general attempts to attack utility operations."[17] Interestingly, this exemption applies only if the records have been provided to certain government bodies, including any organization with a role in safeguarding "telecommunications, electric, potable water, waste water disposal or treatment, motor fuel or natural gas energy supply systems."[18]

New Jersey
New Jersey enacted the Domestic Security Preparedness Act after the events of Sept. 11, 2001, which addresses security and preparedness in the state and exempts public access to certain types of records, including critical utility information. "No record held, maintained or kept on file by the [New Jersey Domestic Security Preparedness Task Force ("Task Force")] or planning group shall be deemed to be a public record under the provisions of [the Open Public Records Act, N.J.SA] or the common law concerning the access to public records." N.J.SA App. A:9-74a. Pursuant to Executive Order No. 5 (Corzine), the task force is now part of the New Jersey Office of Homeland Security and Preparedness ("NJOHSP").

The New Jersey Board of Public Utilities (BPU) has subsequently issued several orders to "mitigate cyber risks to critical systems of electric, natural gas, and water/wastewater utilities" and issued requirements for reporting cyber incidents. The BPU March 18, 2016 order *In the Matter of Utility Cyber Security Program Requirements in Docket No. AO16030196* requires energy sector companies to report cyber incidents to the New Jersey Office of Homeland Security and Preparedness (NJOHSP) and to the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC).

Looking Ahead

As the electric grid continues integrating more information and communication technologies, and as states look to partner more closely with utilities on energy assurance and resiliency, the sensitivity of information being shared and threats from increased connectivity will grow. States need to have rules in place and regularly update these rules as threats evolve to protect the public in the case of an emergency.

Additional State Resources

Council of State Governments (CSG), *State Official's Guide to Critical Infrastructure Protection*, 2003.
Federal Energy Regulatory Commission (FERC), *Critical Energy/Electric Infrastructure Information (CEII)*, 2018.

National Association of Regulatory Utility Commissioners (NARUC), *Information Sharing Practices in Regulated Critical Infrastructure States Analysis and Recommendations*, 2007.

National Conference of State Legislatures (NCSL), *Open Government Laws and Critical Energy Infrastructure*, 2018.

This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000817.

[1] This number is based on NGA research and NCSL. *Open Government Laws and Critical Energy Infrastructure*. January 30, 2018.
[2] Public Law 107–56: USA PATRIOT Act of 2001 (Date: 10/26/01).
[3] Arkansas. § 25-19-105. https://cdn.ymaws.com/www.arkansaspress.org/resource/resmgr/files/FOIHandbook_18thEd.pdf.
[4] 65 Pa. Stat. §67.708 (b).
[5] NARUC. *Information Sharing Practices in Regulated Critical Infrastructure States, Analysis and Recommendations*. 2007. Act 156 of 2006. https://www.legis.state.pa.us/cfdocs/legis/li/uconsCheck.cfm?yr=2006&sessInd=0&act=156.
[6] This section and subsequent ones describe critical infrastructure information (CII) more broadly and are not focused solely on energy infrastructure.
[7] *Santa Clara v. Superior Court*, 89 Cal.Rptr 374, 388 (2009).
[8] *Virginia Dept. of Corrections v. Surovell*, 290 Va. 255, 263 (Va., 2015); *see also, Crawford v. New York City Dept. of Information Technology*, 982 N.Y.S.2d 725 (2014).
[9] Cal. Pub. Util. Comm. ("CPUC"), Dkt. 14-08-013, Administrative Law Judge's Ruling Ordering Pacific Gas

and Electric Company, Southern California Edison Company, and San Diego Gas and Electric Company to File Separate Motions for Confidential Treatment and Redaction of Distribution System Planning Data Ordered by Decisions 17-09-026 and 18-02-004 ("ALJ Ruling"), July 24, 2018.

[10] Northwest Gas Association v. Washington Utilities and Transp. Commission (2007) 141 Wash. App. 98, 168 P.3d 443.

[11] Codified at Conn. Gen. Stat. § 25-32d(c).

[12] 2017 Bill Text CT H.B. 7221, codified at Conn. Gen. Stat. § 25-32d.

[13] Codified at Fla. Stat. § 119.0713(5)).

[14] Fla. Stat. § 119.0713(5).

[15] Idaho Code § 74-105(4)(b).

[16] *Id*.

[17] K.S.A. § 45-221(a)(54).

[18] *See* K.S.A. § 45-221(a)(54).