NARUC

National Association of Regulatory Utility Commissioners

Compendium of Cyber Incident Notification Requirements for Critical Infrastructure Utilities by State

Hyleah O'Quinn

July 2022

Disclaimer

This material is based upon work supported by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response under Award Number DE-CR0000009.

Acknowledgments

The author would like to thank the following individuals and organizations for their contributions, review, and comments to inform the contents of this compendium:

- Advanced Energy Economy
- Members of NARUC's Committee on Critical Infrastructure and Staff Subcommittee on Critical Infrastructure
- **Ashton Raffety**, Argonne National Labs
- **Lynn P. Costantini**, NARUC
- **Brandi Martin**, **Jason Pazirandeh**, and **Cynthia Hsu**, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response

Introduction

Cyber attacks targeting critical infrastructure in the United States are on the rise and pose serious risks to the economy and health and safety of its citizens. Experts suggest a sound cyber risk mitigation strategy includes constant monitoring for signs of cyber intrusions and rapid reporting of incidents so that other critical infrastructure operators may benefit from early warnings. Reporting incidents to Public Utility Commissions (PUCs) and other state agencies who have roles in energy emergency planning and incident response and recovery is essential for them to maintain situational awareness and provide necessary support to ensure rapid restoration of utility services, should disruptions occur. Until recently, however, most cyber incident reporting for critical infrastructure owners and operators was voluntary.[1] Most states have laws that require private businesses, including energy utilities, to notify individuals of security breaches of information involving personally identifiable information (PII), such as social security numbers.[2] However, few states have mandatory requirements to report cybersecurity incidents involving critical infrastructure. This compendium identifies those states and details the requirements each has for utilities to report cyber incidents. Documenting this information in a single place makes it easier to compare existing state-level requirements. It also provides a starting point for other states interested in pursuing similar action.

Research for this compendium relied on a variety of proprietary and public sources. Findings were compared against a database of PII reporting requirements maintained by the National Conference of State Legislatures, and duplicates were removed. The remaining entries focused on state-specific, non-PII cyber incident reporting requirements for utilities. As a last step, relevant states' PUC staff verified details pertaining to their state's requirements. This comprehensive process culminated in the list of 10 states confirmed as having requirements for utilities to report cyber incidents affecting critical infrastructure to a state-appointed party.

What this compendium includes:

- Non-PII-only cybersecurity incident reporting requirements applicable to critical infrastructure utilities (energy, water, telecommunications, etc.) issued by PUCs, state legislatures, or other state agencies.

What this compendium does not include:

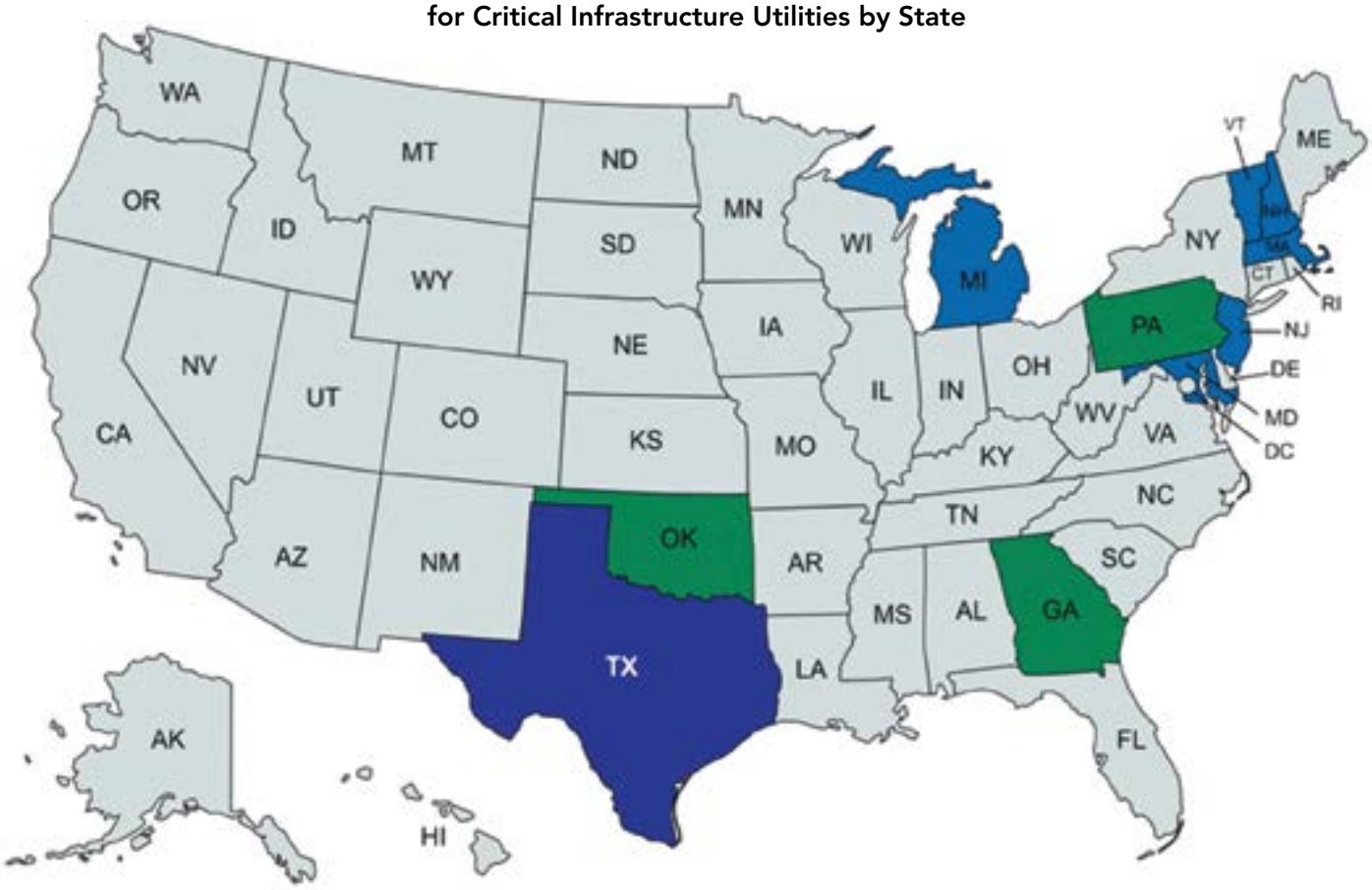
- State reporting requirements pertaining to PII data breaches, as documented by the National Conference of State Legislatures.
- Utility service outage reporting requirements, often required by states regardless of the cause. This compendium does not include general service outage reporting rules unless those rules specifically reference cyber incidents as a cause.

Details of each state's reporting requirements follow. Content for each entry is excerpted from the prevailing statute or order; no attempt was made to qualitatively interpret or provide explanatory context. Entries are in alphabetical order.

1 Bulk electric system owners and operators are required to report certain cyber incidents to the Electricity Information Sharing and Analysis Center (E-ISAC), per CIP-008-6, R4. See https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf. In July 2021, U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA) instituted mandatory cyber incident reporting requirements for gas pipelines (https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators). In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law, but implementation details are still under development.

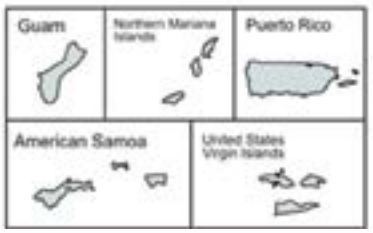
2 https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Cyber Incident Notification Requirements for Critical Infrastructure Utilities by State



Requirement Issued by:

- Public Utilty Commission
- State Government
- Certified 501 (c) (4) non profit corporation governed by a board of directors and subject to oversight by the Public Utilty Commission and the State Legislature



Georgia	
Requirement Issued By	Georgia State Code
Year Issued	2021
Utilities Required to Comply	"Utility" means any publicly, privately, or cooperatively owned line, facility, or system for producing, transmitting, or distributing power, electricity, light, heat, or gas.
Notification Required If	Any cyber attack incident, data breach, or identified use of malware on a utility computer or network as such information is required to be reported to the U.S. Government or any agency thereof.
When Is Notification Required	Within two hours of making the report to the U.S. Government or any agency thereof.
Who Must the Utility Notify	Director of Emergency Management and Homeland Security, or his or her designee
How Should Notification Occur	Subject to approval by the Governor, the Director of Emergency Management and Homeland Security will promulgate rules and regulations specifying the reporting mechanism.
Exceptions	If information is prohibited under any federal law, rule, or regulation from being disseminated, the utility shall provide such information upon the expiration or lifting of such prohibition.
Source	Georgia House Bill 156 (2021)

Maryland	
Requirement Issued By	Maryland Public Service Commission
Year Issued	2019
Utilities Required to Comply	Investor-owned utilities (IOUs), cooperatives, municipalities, gas, and water
Notification Required If	A cybersecurity breach impacts information technology (IT), operational technology (OT), or a smart grid system. A "security breach" is defined as any unauthorized act that has been confirmed to result in access to, acquisition, control, destruction, disclosure, or modification of a utility's IT systems, OT systems, or smart grid systems.
When Is Notification Required	Within one business day of confirmation of a security breach.
Who Must the Utility Notify	Maryland Public Service Commission's Chief Engineer (or designated alternate). As appropriate, also report to U.S. Department of Homeland Security (DHS), Maryland Fusion Center, and Maryland Attorney General.
How Should Notification Occur	Verbally
Exceptions	Not required if contrary to law or the recommendation of law enforcement to avoid compromising an investigation.
Source	Pursuant to Order No. 89015

Massachusetts	
Requirement Issued By	Massachusetts Department of Public Utilities (MA DPU)
Year Issued	2015
Utilities Required to Comply	Electric IOUs and natural gas companies
Notification Required If	**For Electric and Gas**—As soon as practicable following the determination that a cyber attack or physical attack has resulted in any electric outage event or gas interruption event. **For Electric Only**—As soon as practicable following a reportable cybersecurity incident, as outlined by North American Electric Reliability Corporation (NERC) CIP 008-3. **For Gas Only**—Following a malicious act or suspicious event that compromises, or was an attempt to compromise, the electronic security perimeter or physical security perimeter or, disrupts, or was an attempt to disrupt, the operations of a gas distribution company's cyber system. **For Electric and Gas**—A company shall submit a final post-event report to the MA DPU within 72 hours of the incident and may update that report with any additional supplemental information no later than 10 days following an incident.
When Is Notification Required	See time specifications for each type of event above.
Who Must the Utility Notify	Designated representative within the MA DPU
How Should Notification Occur	Not specified
Exceptions	Not specified
Source	MA DPU Memorandum[3]

3 Memo not publicly available.

Michigan	
Requirement Issued By	Michigan Public Service Commission
Year Issued	2019 (Electric) and 2020 (Natural Gas)
Utilities Required to Comply	Electric and gas IOUs and cooperatives
Notification Required If	A person intentionally interrupted the production, transmission, or distribution of natural gas or electricity. A person extorted money or other things of value from the utility through a cybersecurity attack. A person caused a denial of service in excess of 12 hours. A security breach, as defined by section 3(b) of the Identity Theft Protection Act, 2004 PA 452, MCL 445.63(b), prior to public and customer notification. At the utility discretion.
When Is Notification Required	As soon as reasonably practicable and prior to any public notification.
Who Must the Utility Notify	Designated member of the commission staff and the Michigan Fusion Center
How Should Notification Occur	Verbally
Exceptions	Not required if prohibited by law or court order, or instructed otherwise by official law enforcement personnel.
Source	Admin Code R.460.3205 (Electric) and Admin Code R.460.2324 (Gas)

New Hampshire	
Requirement Issued By	New Hampshire Public Utility Commission
Year Issued	2005 (Gas) and 2014 (Electric)
Utilities Required to Comply	**Gas**—Privately-owned natural gas utilities **Electric**—Electric IOUs and the New Hampshire Electric Cooperative, Inc.
Notification Required If	**Gas**—A breach of security or other threat that jeopardizes the operation of a utility's major facilities. **Electric**—Security breaches against a utility's "critical cyber assets." "Critical cyber assets" means those electronic data, communications, and computer network systems without which the utility could not provide safe reliable service to its customers.
When Is Notification Required	**Gas**—Immediately upon an event by phone. **Electric**—A soon as possible, but no later than two hours after becoming aware of an accident or event that involved a breach of security or threat against the utility's facilities. • In addition, on the 15th day of the month following the last day of each quarter, each utility shall file Form E- 37, pursuant to PUC 308.17, reporting all material breaches of security as defined within their cybersecurity plan.
Who Must the Utility Notify	**Gas**—The LPG operator or landfill gas operator shall notify the Division of Enforcement within the New Hampshire Department of Energy. **Electric**—The utility shall notify the Division of Enforcement within the New Hampshire Department of Energy.
How Should Notification Occur	**Gas**—by telephone. **Electric**—by telephone.
Exceptions	Not specified
Source	https://www.energy.nh.gov/enforcement/physical-cyber-security

New Jersey	
Requirement Issued By	New Jersey Board of Public Utilities (NJ BPU)
Year Issued	2016
Utilities Required to Comply	Electric IOUs, natural gas, water/wastewater utilities
Notification Required If	Utilities shall report cyber events relating to industrial control systems (ICSs), as set forth below: • A person, including any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity that accessed the ICS without authorization or exceeded authorized access. For purposes of this order, "exceeds authorized access" means a person who accesses the ICS with authorization and uses such access to obtain or alter information in the ICS that the person is not entitled to obtain or alter. • Unauthorized programs, information, code, or commands discovered on an ICS. • A person extorted any money or other thing of value by threatening to cause damage to your ICS. For purposes of this order, damage includes any impairment to the integrity or availability of date, a program, a system, or information. • Utilities shall report unusual cyber activity that has the potential to compromise critical systems and for which controls are ineffective.
When Is Notification Required	Reports must be submitted to Reliability and Security Division staff through the NJ Cybersecurity and Communications Integration Cell (NJCCIC) and in accordance with the prevailing rules, requirements, and submittal forms and formats designated by NJCCIC. Pursuant to N.J.A.C. 14:3–6.7, reports shall be made within six hours of the detection of an incident. In addition: • Utilities shall copy Reliability and Security Division staff on notifications to law enforcement agencies of the State of New Jersey regarding information breaches involving the PII of customers to the extent such notifications are required by the laws of the State of New Jersey, including, but not limited to, N.J.S.A. 56:8–163.mj.
Who Must the Utility Notify	Designated staff within the NJ BPU's Reliability and Security Division through the NJCCIC.
How Should Notification Occur	Via reports, email, and in accordance with prevailing rules, requirements, and submittal forms and formats designated by the NJCCIC.
Exceptions	Not specified
Source	Docket No. AO16030196[4] and New Jersey Department of Environmental Protection Division of Water Supply and Geoscience

4 This 2016 ruling supersedes a similar 2011 NJ BPU ruling.

Oklahoma	
Requirement Issued By	Oklahoma Administrative Code
Year Issued	2019 (Water), 2019 (Gas), and 2020 (Electric)
Utilities Required to Comply	**Natural Gas Utility**—means a natural gas utility as defined in 17 O.S. § 151 et seq., and that includes all utility affiliate assets which the commission has determined to be included in ratebase. **Electric**—means any person, firm, partnership, or corporation furnishing electric service to the public in Oklahoma and subject to the regulatory jurisdiction of the commission. **Water**—includes any corporation, association, company, individual, and the trustees, lessees, or receivers, successors or assigns of any of them (but shall not include a city, town, or other body politic) that now or hereafter may own, operate, or manage any plant or equipment, or any part thereof, directly or indirectly, for public use, for the transmission and distribution of water by pipeline.
Notification Required If	A cybersecurity or infrastructure event that affects customers.
When Is Notification Required	Immediately
Who Must the Utility Notify	Public Utility Division (PUD) of the Oklahoma Corporation Commission Director or designee.
How Should Notification Occur	Not specified
Exceptions	Not specified
Source	Water (OK Admin Code 165:65-9-2) Natural Gas (OK Admin Code 165:45-21-7) Electric (OK Admin Code 165:35-33-7)

Pennsylvania	
Requirement Issued By	Pennsylvania State Code
Year Issued	2005
Utilities Required to Comply	Jurisdictional utility (see § 27.10, § 29.43, § 31.10, § 33.103, § 57.47, § 59.48, § 61.28, § 63.36, or § 65.19).
Notification Required If	Abnormal operating conditions exist. "Abnormal operating conditions" is defined as a condition possibly showing a malfunction of a component or deviation from normal operations that may: (i) indicate a condition exceeding design limits or (ii) result in a hazard to person, property, or the environment.
When Is Notification Required	Not specified
Who Must the Utility Notify	Appropriate emergency services and emergency preparedness support agencies and organizations.
How Should Notification Occur	Not specified
Exceptions	Does not apply to an entity regulated by the Federal Railroad Safety Act and the Hazardous Materials Transportation Act.
Source	PA Code Ch. 101

Texas	
Requirement Issued By	Electric Reliability Council of Texas (ERCOT)[5]
Year Issued	2019
Utilities Required to Comply	ERCOT Market Participants[6]
Notification Required If	A malicious or suspicious act that compromises or disrupts a computer network or system, which could jeopardize the reliability or integrity of the ERCOT system or ERCOT market operations. These notification requirements extend to malicious or suspicious acts that compromise or disrupt the computer network or system of a market participant's agent that transacts with ERCOT.
When Is Notification Required	Immediately upon discovery of a cybersecurity incident.
Who Must the Utility Notify	ERCOT
How Should Notification Occur	Market participants shall submit a Notice of Cybersecurity Incident to NCSI@ercot.com. If, as a result of the cybersecurity incident, a market participant is unable to securely send the Notice of Cybersecurity Incident to ERCOT, the market participants shall call the ERCOT Help Desk at (512) 248-6800 and/or its Client Service Representative to request a secure means for sending the Notice to ERCOT.
Exceptions	Not specified
Source	NPRR928 and NPRR993

Vermont	
Requirement Issued By	Vermont Public Utility Commission
Year Issued	2019
Utilities Required to Comply	Electric utilities (except national grid) and energy efficiency utilities
Notification Required If	A cybersecurity attack results in the release of confidential customer information, a compromise of grid reliability, or required reporting to another entity.
When Is Notification Required	Promptly
Who Must the Utility Notify	Commissioner of the Department of Public Service
How Should Notification Occur	Not specified
Exceptions	Not specified
Source	Case No. 7307

5 ERCOT is a membership-based 501(c)(4) nonprofit corporation, governed by a board of directors and subject to oversight by the Public Utility Commission of Texas and the Texas Legislature. Its members include consumers, cooperatives, generators, power marketers, retail electric providers, IOUs, transmission and distribution providers, and municipally owned electric utilities. See more about ERCOT: https://www.ercot.com/about.

6 ERCOT Market Participants, https://www.ercot.com/committees/mktparticipants.

Frequently Asked Questions

1. Do federal agencies currently require cyber incident reporting for utilities?

Yes. The U.S. Department of Energy (DOE) requires Balancing Authorities (BA), Reliability Coordinators (RC), some Generating Entities, and Electric Utilities to file DOE-417 reports. Filing is mandatory whenever an electrical incident or disturbance is sufficiently large enough to cross defined reporting thresholds, regardless of cause. Timing of initial reports and status updates vary depending on the nature of the situation. Reporting coverage for the Form DOE-417 includes all 50 States, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and the U.S. Trust Territories. DOE provides a summary of incident reports, but details of the incident are not publicly available.

U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA) also requires owner/operators of TSA-designated critical pipelines and liquified natural gas (LNG) facilities to file cyber incident reports with DHS. These reports are confidential.

2. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 will require utilities to report "covered cyber incidents" and ransomware to the DHS. Will states still require incident reporting?

Yes. It is important to note that not all utilities will be required to report "covered cyber incidents" and ransomware events to DHS. Only utilities that DHS defines as "owners and operators of critical infrastructure" through a formal rulemaking process will be subject to this law, which may or may not include utilities within your state. It is unclear whether PUCs will be privy to which utilities DHS eventually defines as owners and operators of critical infrastructure for reporting purposes. It is also unclear if reports made pursuant to this law will be available to states.

3. Why would a commission institute cyber incident reporting requirements?

Cyber incident notifications are invaluable for PUCs, especially those with ESF-12 responsibilities, to effect rapid information sharing with key stakeholders and to help implement appropriate response actions. Over time, PUCs will gain a better understanding of the cybersecurity risk environment in which their jurisdictional utilities operate and are better prepared to assist utilities to plan for and respond to emerging cybersecurity threats. Before instituting rules, it is important to have a candid discussion with your jurisdictional utilities about their cybersecurity programs and whether they are subject to other cybersecurity incident reporting requirements. If so, you may ask them to include you as a report recipient, rather than creating new requirements.

PUCs that are contemplating new cybersecurity incident notification requirements may want to consider aligning their efforts with federal requirements or those issued by other states to ensure consistency, which promotes timely reporting.

4. Do alternatives to requiring utilities to report cyber incidents exist?

Rather than instituting formal cybersecurity incident reporting requirements, some PUCs rely on informal, trusted lines of communication between commission staff and utilities to stay informed. Other commissions may participate in information sharing forums such as the Multistate Information Sharing and Analysis Center or their state fusion centers to stay abreast of cybersecurity threats and incidents. Because these resources provide anonymized information, they are helpful to maintain situational awareness of the evolving cybersecurity threat landscape and provide opportunities for more detailed discussions with utilities about risk and mitigation strategies.

5. Are there are other resources that could inform PUCs about energy utilities' cybersecurity practices?

Yes! NARUC has developed a Cybersecurity Manual specifically tailored for PUCS as a comprehensive suite of cybersecurity tools filled with information on cybersecurity risk management and preparedness. There are five components of the manual:

1. Cybersecurity Strate0gy Development Guidelines
2. Cybersecurity Preparedness: Question for Utilities
3. Cybersecurity Preparedness Evaluation Tool
4. Cyber Tabletop Exercise Guide
5. Cybersecurity Glossary

These tools are designed to be used together; however, they can be used individually to fit specific commission needs. The NARUC Cybersecurity Manual can be found here.

In addition, the DOE offers utility-centric resources such as the Cybersecurity Capability Maturity Model (C2M2), a tool for evaluating and improving cybersecurity through implementation and management of practices associated with IT and OT. The tool can be found here.

The National Institute of Standards and Technology (NIST) offers a host of tools including the Framework for Improving Critical Infrastructure Cybersecurity. The framework focuses on cybersecurity risk as a part of the organization's risk management processes, designed to apply principles and best practices to improve security and resilience. The framework can be found here.

Last, Public Utilities Fortnightly, in collaboration with the National Conference of State Legislatures and DOE, developed an educational video to explore the state's role within cybersecurity in the power sector. This video features dialogue from state legislatures, PUCs, DOE, and IOU companies. The video can be found here.

NARUC
National Association of Regulatory Utility Commissioners

1101 Vermont Ave, NW • Suite 200 • Washington, DC 20005
www.naruc.org • (202) 898-2200