Cybersecurity for Critical Infrastructure

IPPSR Legislative Staff Training
September 10, 2021

Dan Scripps, Chair
Michigan Public Service Commission

MPSC
Michigan Public Service Commission

Outline of presentation

- About the MPSC
- MPSC Cybersecurity Activities to Date
- 2019 Statewide Energy Assessment – recommendations and implementation
- Safeguarding Critical Energy Infrastructure Information (CEII)
- COVID-19 Critical Infrastructure Task Force

About the MPSC

- Established in 1873 as the Michigan Railroad Commission; Michigan Public Service Commission established in 1939
- Consists of three commissioners, appointed by the Governor (with advice and consent of the State Senate) to serve six year terms
- Chairperson designated by the Governor
- Exists as an autonomous entity located within LARA
- MPSC has jurisdiction over electric and natural gas utilities and telecommunications providers, as well as authority over the siting of oil pipelines and operation of natural gas pipelines
- Staff of 180 individuals with expertise in accounting, auditing, cybersecurity, emergency planning, energy markets, engineering, finance, and law
- Annual budget of approx. $30M, funded through Public Utility Assessments (PUA) and federal funds
  - Typically no GF/GP

The mission of the MPSC is to serve the public by ensuring safe, reliable, and accessible energy and telecommunications services at reasonable rates.

MPSC
Michigan Public Service Commission

Our vision is to be a best-in-class commission by:

- *Making well-informed decisions at every level of the organization*
- *Meaningfully engaging the public*
- *Enabling innovation for the future*

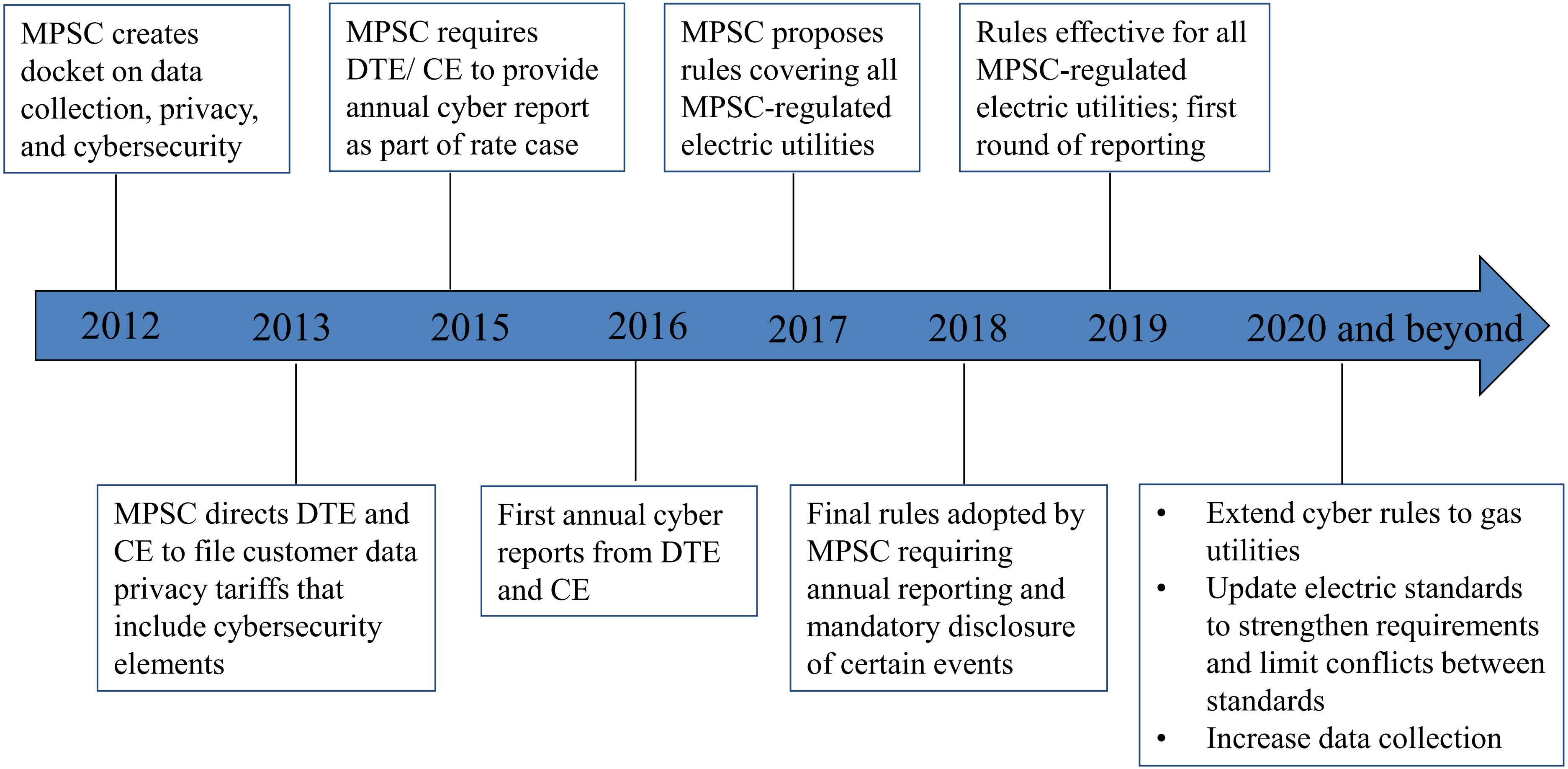
Katherine Peretick

Tremaine Phillips

Dan Scripps

Cybersecurity activities to date

Timeline of MPSC's Cybersecurity rules



2012

MPSC creates docket on data collection, privacy, and cybersecurity

2013

MPSC directs DTE and CE to file customer data privacy tariffs that include cybersecurity elements

2015

MPSC requires DTE/ CE to provide annual cyber report as part of rate case

2016

First annual cyber reports from DTE and CE

2017

MPSC proposes rules covering all MPSC-regulated electric utilities

2018

Final rules adopted by MPSC requiring annual reporting and mandatory disclosure of certain events

2019

Rules effective for all MPSC-regulated electric utilities; first round of reporting

2020 and beyond

- Extend cyber rules to gas utilities
- Update electric standards to strengthen requirements and limit conflicts between standards
- Increase data collection

Overview of cybersecurity rules

Effective: January 2019

Scope: Investor-owned and cooperative electric utilities

Frequency: At least once per year

Required Reporting Thresholds:

- Interrupted production, transmission, or distribution of electricity
- Extortion
- Denial of service of more than 12 hours
- Data breach (as defined in Michigan law)
- Anything else utility deems to be “notable, unusual, or significant”

MPSC cyber rules, cont.

Required Plan Elements:

- Overview of plan describing approach to cybersecurity awareness and protection
- Description of training efforts, and participation in emergency preparedness exercises in last year
- Diagram of cybersecurity organization, including names and contact information for both primary and secondary contacts
- Description of communication plan for events that result in loss of service, financial harm, or data breach
- Summary of events above, including parties notified and remedial actions undertaken
- Description of risk assessment tools and methods
- General information about emergency response plans
- *For investor-owned utilities only*: overview of major cybersecurity investments in previous year and plans and rationale for anticipated major cybersecurity investments in next calendar year

Lessons learned to date

- Highlights
  - Awareness and interest are generally good
  - Strong focus on phishing and security awareness
  - More plans and procedures than anticipated
  - Utility size generally correlated to strength of systems
  - Sector collaborative efforts are healthy
- Areas for Improvement
  - Openness/ transparency highly variable; need to develop trust
  - Many utilities reliant on single IT vendor
  - Need for increased, better organized data collection
  - Inconsistent assessment practices
  - Growing IT/ OT environment complexity

Calendar Year 2019 reported incidents

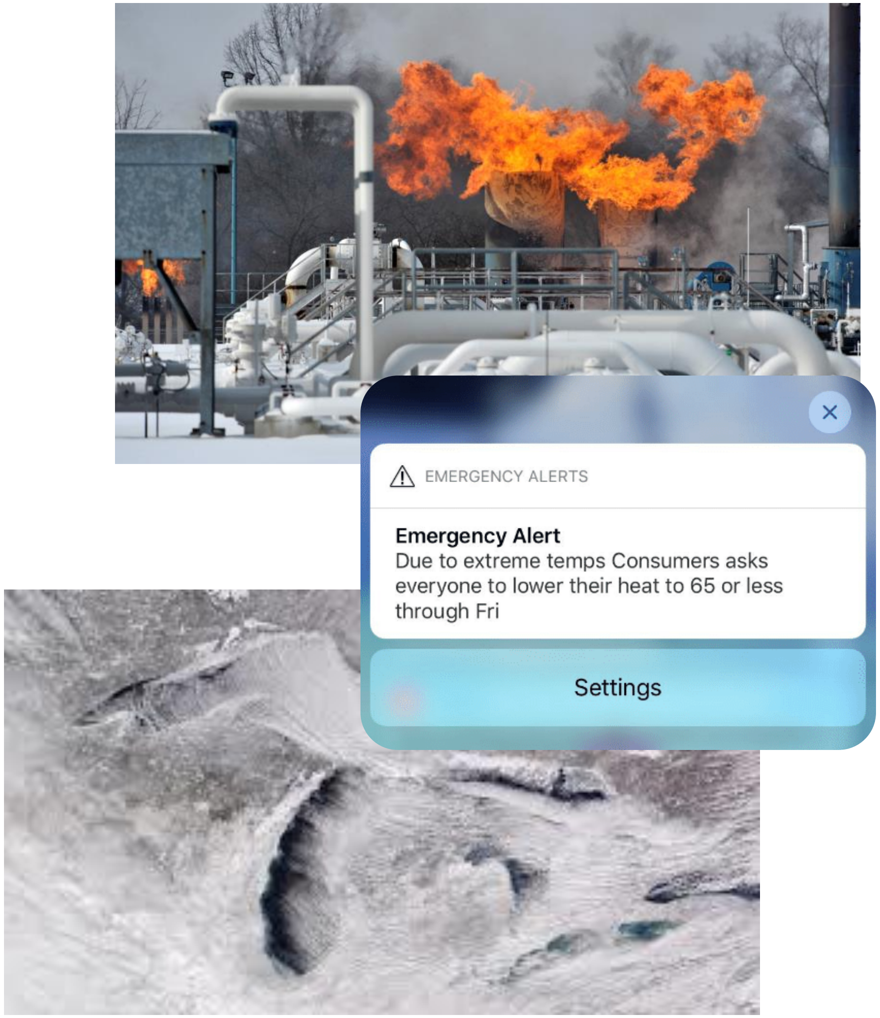
- Three incidents reported
- Two attributed to internal IT errors
- One incident by malicious actor
  - Motivated by financial gain
  - No linkages to Operational Technology (OT) systems or assets

Major Trends in Michigan

- Visibility over obscurity
- Centralization, often at enterprise level
- Automation
- Outsourcing

2019 Statewide Energy Assessment – Origins and Scope

- Following a January 2019 polar vortex that triggered overlapping energy emergencies, Michigan Governor Gretchen Whitmer requested the MPSC review the supply, engineering, and deliverability of natural gas, electricity, and propane
- The MPSC investigated six areas in Statewide Energy Assessment:
  - Electricity
  - Natural Gas
  - Propane
  - Cybersecurity
  - Physical Security
  - Emergency Preparedness
- Final Assessment released in September 2019 includes 37 recommendations under MPSC's jurisdiction and 15 observations to the Legislature, RTOs, and others



EMERGENCY ALERTS

Emergency Alert
Due to extreme temps Consumers asks everyone to lower their heat to 65 or less through Fri

SEA cyber recommendations

Rulemakings and Standards

S-1 Include cybersecurity standards and reporting for natural gas distribution systems under MPSC jurisdiction through proposed amendments to the Gas Technical Standards (Complete)

S-2 Continue to evaluate existing Commission rules and utility data privacy tariffs for opportunities to enhance the protection of customer data and the cybersecurity of electric distribution infrastructure (Ongoing)

S-3 Electric and Natural Gas conduct annual self-assessments of cyber capabilities (In Progress)

S-6 Categorize physical and cyber incident types and severities and make clear internal and external notifications that will take place (In Progress)

S-8 Utilities run simulated phishing campaigns at least quarterly and include all employee levels (In Progress)

- Cybersecurity standards and reporting updates made to the Technical Standards for Gas Service
- Staff report issued 12/15/20 in Case No. U-20630 includes proposed baseline cybersecurity requirements and simulated phishing campaigns in the Technical Standards for Electric Service. Request for Rulemaking (RFR) submitted.
- Customer Education and Participation workgroup to review data privacy tariffs

SEA cyber recommendations

Reporting, Metrics, and Oversight

S-4 Utilities pursue the close coordination of OT, IT, and physical security operations, and centralize security functions (Ongoing)

S-5 Utilities work to develop and track metrics to assess cybersecurity performance (Ongoing)

S-7 Regularly audit operational technology environments for internet-facing systems (Ongoing)

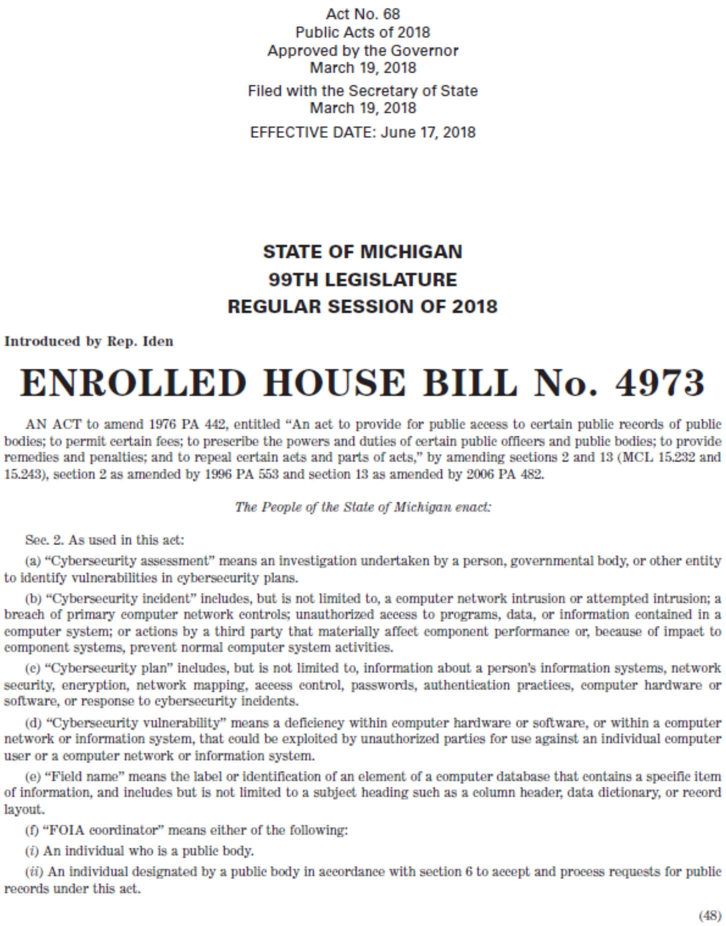
S-9 Utilities require multifactor authentication to remotely access OT assets (Ongoing)

S-10 Encourage utilities to adopt best practices in mitigating threats from phishing and other IT threats, perform cost-benefit analysis on security controls, and implement additional controls (Ongoing)

- Implemented annual cybersecurity reporting – can be done in written format or through a verbal update
- Staff also continues to engage with utilities to monitor progress and ensure continuous improvement
- Staff working with utilities to ensure the inclusion of cost-benefit information for proposed security investments in rate case proceedings
- Staff working with larger utilities on additional cybersecurity and IT data streams and metrics for incorporation in multi-year IT and Security plans

Protecting Critical Energy Infrastructure Information

- Need to protect sensitive information raised as significant issue in both Energy Assessment and annual cybersecurity reporting
- Steps taken to address this issue:
  - ➢ Legislation enacted in 2018 amends Michigan's Freedom of Information Act to exempt records of measures designed to protect the confidentiality of certain information systems, as well as cybersecurity plans, assessments, or vulnerabilities
  - ➢ Annual utility cybersecurity reports can be done either orally or in writing
  - ➢ Informational survey results will be aggregated to protect confidentiality
  - ➢ Assessment called for strengthening protections for Critical Energy Infrastructure Information (CEII)



Act No. 68
Public Acts of 2018
Approved by the Governor
March 19, 2018

Filed with the Secretary of State
March 19, 2018

EFFECTIVE DATE: June 17, 2018

STATE OF MICHIGAN
99TH LEGISLATURE
REGULAR SESSION OF 2018

Introduced by Rep. Iden

ENROLLED HOUSE BILL No. 4973

AN ACT to amend 1976 PA 442, entitled "An act to provide for public access to certain public records of public bodies; to permit certain fees; to prescribe the powers and duties of certain public officers and public bodies; to provide remedies and penalties; and to repeal certain acts and parts of acts," by amending sections 2 and 13 (MCL 15.232 and 15.243), section 2 as amended by 1996 PA 553 and section 13 as amended by 2006 PA 482.

The People of the State of Michigan enact:

Sec. 2. As used in this act:

(a) "Cybersecurity assessment" means an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans.

(b) "Cybersecurity incident" includes, but is not limited to, a computer network intrusion or attempted intrusion; a breach of primary computer network controls; unauthorized access to programs, data, or information contained in a computer system; or actions by a third party that materially affect component performance or, because of impact to component systems, prevent normal computer system activities.

(c) "Cybersecurity plan" includes, but is not limited to, information about a person's information systems, network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware or software, or response to cybersecurity incidents.

(d) "Cybersecurity vulnerability" means a deficiency within computer hardware or software, or within a computer network or information system, that could be exploited by unauthorized parties for use against an individual computer user or a computer network or information system.

(e) "Field name" means the label or identification of an element of a computer database that contains a specific item of information, and includes but is not limited to a subject heading such as a column header, data dictionary, or record layout.

(f) "FOIA coordinator" means either of the following:

(*i*) An individual who is a public body.

(*ii*) An individual designated by a public body in accordance with section 6 to accept and process requests for public records under this act.

(48)

COVID-19
Critical Infrastructure Task Force

- During early months of COVID-19 pandemic, MPSC convened department/ agency emergency management coordinators (EMCs) across state government with responsibility for critical infrastructure sectors to ensure continuity of service
  - Also held weekly calls that included external stakeholders from the private sector and local units of government
  - This built on and was in addition to existing sector-specific calls organized by a number of state agencies
- Future plans are to reconvene this group around similar shared critical infrastructure priorities, including cybersecurity
- This network can also assist in developing strategies for leveraging any available federal funding targeted at cybersecurity for critical infrastructure sectors in the future