**MISSOURI PUBLIC SERVICE COMMISSION**

**STAFF REPORT**

# A WORKING CASE TO ADDRESS SECURITY PRACTICES FOR PROTECTING ESSENTIAL UTILITY INFRASTRUCTURE

**FILE NO. AW-2015-0206**

**August 19, 2019**

**STAFF REPORT**
**A WORKING CASE TO ADDRESS SECURITY PRACTICES**
**FOR PROTECTING ESSENTIAL UTILITY INFRASTRUCTURE**
**FILE NO. AW-2015-0206**

## 1 Executive Summary

Utility services and infrastructure are essential to the economy of Missouri. Nearly all Missouri citizens receive some form of utility service from a company regulated by the Missouri Public Service Commission (PSC or Commission). The PSC is charged with ensuring the delivery of safe, adequate, and reliable utility services at just and reasonable rates.

The Commission's statutory authority has a direct relationship to the cyber and physical security, reliability, and resiliency of all utility systems in Missouri. For example, a utility taking a sound physical and cybersecurity posture[1,2] will enhance its ability to provide reliable service. Any established standards developed and/or monitored by the Commission should not create an overly burdensome requirement that would thwart an efficient regulatory process.

The infrastructure that provides these essential utility services is referred to as Critical Infrastructure. Critical Infrastructure (CI) is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3] Critical Infrastructure is segmented into 16 interdependent sectors with Energy at the core of the interdependence.

CI systems are incorporating what is referred to as 'Smart Devices' which have the potential to assist CI operators in maximizing efficiencies while at the same time minimizing interruptions. These systems also have the potential to allow the customers of these services to have greater control over the use and cost of these essential services. These systems also come with an increased potential for misuse and disruption. It is imperative that these new systems be as secure, reliable and resilient as possible.

As the regulatory agency for the utilities providing these services it is incumbent upon the Commission to become more knowledgeable and proactive when it comes to understanding the conditions and the challenges that these new systems present. Ultimately the role of the Commission from a security standpoint should be considered in a tertiary manner, namely what to do:

- Before an incident – "left of boom" – understanding of the security posture of the utilities and the currently active threats. Developing, maintaining, and exercising response plans.

[1] The cybersecurity posture of an organization refers to its overall cybersecurity strength. This expresses the relative security of your Information Technology (IT) and Operational Technology (OT) assets, particularly as it relates to the internet and the vulnerability to outside threats.
[2] The physical security posture of an organization refers to the overall strength of the security protecting the organizations' physical assets, particularly as it relates to outside threats.
[3] United States. (2001). The USA PATRIOT Act: Preserving life and liberty: uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism. Washington, D.C.: U.S. Dept. of Justice.

- During an incident – "boom" – active emergency response and an understanding of the actions that are being taken by each utility. Monitoring the situation on the ground as it relates to utilities and to assist in the rapid restoration of services.
- After an incident – "right of boom" – resilience and recovery planning and actions[4].

After much work by the Commission and Commission Staff with input from other stakeholders, the following Staff recommendations are being made in the interest of enhancing the security, reliability, and resiliency of Missouri utilities.

The Staff recommendations are as follows:

- Reporting:
  1) Require each Missouri utility to identify, provide, and actively update contact information for both cyber and physical security points of contact. Points of contact should be personnel actively engaged with both cyber and physical security issues and not a member of the utilities' counsel or involved with regulatory liaison activities.
  2) Require formal[5] disclosure of plans specifically related to emergency response.
  3) Require periodic Commission briefings on current security posture and related activities.
  4) Require timely informal disclosure of both cyber and physical security incidents and any related response(s) and effect(s).
  5) Specifically address supply chain risk management during periodic Commission briefings.
  6) Investigate CI information storage within the Department of Public Safety (DPS), State Emergency Management Agency (SEMA), or the Missouri Information and Analysis Center (MIAC).
  7) Monitor governmental and industry efforts to develop cyber security reporting metrics. Implement a reporting mechanism for such metrics should the development efforts produce useful results.

- Emergency Communications:
  8) Transition cellular communication accounts to FirstNet for those areas that participate in emergency response and/or other emergency and safety related activities.
  9) Commissioners and select Staff members individually investigate transitioning personal phones used for communications during security related activities to FirstNet if prioritized emergency communications is warranted.

- Information Sharing:
  10) Encourage utilities to actively participate in the Intelligence Liaison Officer (ILO) program to receive pertinent threat information and provide information on suspicious activities that they may encounter in conducting everyday operations.
  11) Proactively inform Missouri utilities about the Sensitive Compartmented Information

[4] Popularized in military circles during the months and years after 9/11, the phrase "left of boom" refers to the moments before an attack – a period when you still have time to prepare and avert a crisis. "Right of boom", by contrast, includes the chaotic moments after the attack. http://nectoday.com/left-of-boom-defeating-the-threat-among-us/

[5] See section 4.3.2 within this report for information on 'formal' and 'informal' reporting.

Facility (SCIF) capabilities at the MIAC and the timing of any classified briefings that are taking place for cleared personnel.

12) Actively participate in the organization and development of a Utility Information Exchange Group and encourage all Missouri utilities to participate.
13) Actively participate in the improvement of information sharing between the public and private sectors by encouraging the involvement of investor-owned utilities, cooperative utilities, and municipal utilities where possible.

- Organization Development:
  14) Partner with SEMA and develop a proposal to expand the types of volunteers involved with the Missouri Structural Assessment and Visual Evaluation (SAVE) Coalition as well as the types of evaluations that could be carried out by such members with a focus on structures associated with critical infrastructure and volunteers with knowledge of such structures.
  15) Investigate the activities and partnerships necessary to create a Civilian Cyber Corps volunteer organization possibly in connection with the SAVE Coalition.

- Mapping:
  16) While Staff has no specific recommendations on adoption at this time, the use of Geographic Information System (GIS) technology does allow for ease of maintenance and production of maps and mapping services such as the identification and publication of certificated areas granted through the Certificate of Convenience and Necessity (CCN) process.
  17) Periodical review, by the Commission, of software options concerning GIS mapping technology.

- Preparedness and Exercises:
  18) Continue to actively participate in upcoming statewide emergency response exercises and when possible, participate in other local, regional, national drills and exercises.
  19) Train at least three Staff members on the emergency response Incident Command System Operations to the minimum level of ISC-400.
  20) Periodically update Commission General Procedures GP-7 and GP-7.5, as necessary.

- Resource Availability:
  21) Encourage all utility owners and operators to engage the Department of Homeland Security (DHS) and the Missouri National Guard Cyber Team and leverage their respective resources.

## 2 Critical Infrastructure

The USA PATRIOT Act defines Critical Infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The 'Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience' advances a national policy to

strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 segmented critical infrastructure into 16 *interdependent* sectors.

Utilities regulated by the PSC fall primarily into three sectors: (1) the Energy Sector (2) the Water and Wastewater Sector and to a limited extent, (3) the Communication Sector. Although there are significant interdependencies between all CI sectors, it is generally accepted (but frequently argued) that all other sectors have a primary dependence upon energy, and more specifically, electricity. Figure 1 represents the interdependencies between all of the CI sectors.

The Energy Sector is in the center with direct interdependencies with each of the Communication, Transportation, and Water sectors. The second level of interdependencies is indicated by the middle (red) cluster and the connections to the remainder of the Critical Infrastructure sectors. While much of the the following discussion and analysis focuses on modern society's central dependency on the electric utility, the positons and conclusions are applicable to all utilities.

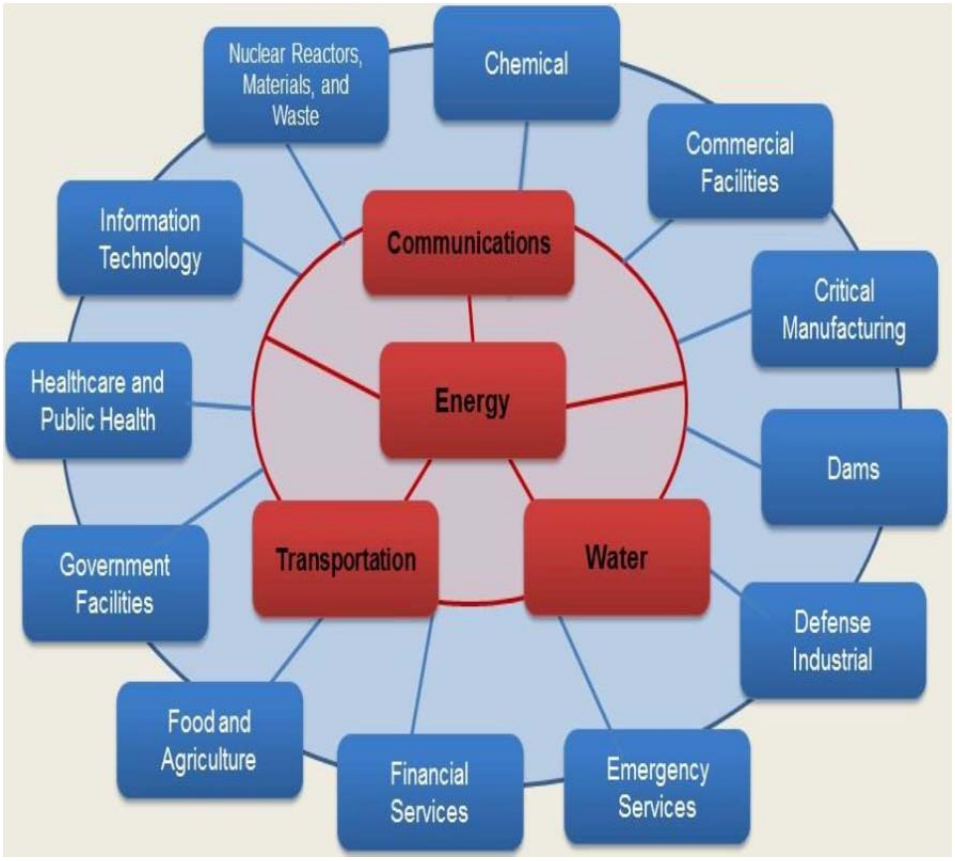


**Figure 1: Sector Interdependencies, Department of Energy and Department of Homeland Security, Energy Sector Specific Plan, page 19, 2015.[6]**

[6] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

## 3 Smart Utility Systems

It has been postulated by the United States Department of Energy's National Renewable Energy Laboratory (NREL) that the combined electrical generation, transmission, and distribution systems are the single largest and most complex technological system ever built[7]. It has also been argued by the Congressional Research Service that newly introduced technological advances, via what has been collectively referred to as the "Smart Grid", has created vulnerabilities that may increase the chances of a successful cyberattack[8]. Given these changes occurring in the energy sector, it appears to Staff that there may be a need for additional security oversight, or at a minimum, a better understanding of the efforts which are being undertaken to protect the energy sector from increased vulnerabilities.

The first official definition of "Smart Grid" originated within the Energy Independence and Security Act of 2007 (EISA-2007). The "Smart Grid" has the primary goal of "optimizing resources and system control through the increased use of automated digital control mechanisms, two way data flow, and customer usage data." The EISA-2007 also stated that the Smart Grid will provide for the integration of:

- renewable and other distributed resources
- demand side resources
- energy efficient resources
- peak shaving storage resources
- smart appliances
- transportation electrification

Since EISA-2007, ***all*** utility systems have become more complex with the introduction, and in some cases the widespread adoption of many of the technologies identified in EISA-2007. This technological advancement has been driven by US policy on the smart grid in 42 U.S.C. §§ 17381–17386 (2007).[9] Although all utilities have become more technologically advanced and dependent, and therefore technologically vulnerable, the electric power utility has undoubtedly been affected by this change more than any other.

The electric power industry is increasingly incorporating both Information Technology (IT) and Operational Technology (OT) systems into its existing infrastructure as part of a nationwide effort, commonly referred to as Smart Systems, aimed at improving reliability, resiliency and efficiency. This communication process also facilitates the use of distributed energy resources such as wind and solar in the case of the electric power industry. Smart technologies can include a myriad of technologies that can enable two-way communication between customers and electric utilities such as:

- Advanced Metering Equipment
    - Automated Meter Reading (AMR)
    - Advanced Metering Infrastructure (AMI)

[7] https://www.nrel.gov/continuum/analysis/ergis.html
[8] The Smart Grid: Status and Outlook, Richard J. Campbell, Specialist in Energy Policy, April 10, 2018
[9] https://www.govinfo.gov/app/details/USCODE-2011-title42/USCODE-2011-title42-chap152-subchapIX/summary

- Supervisory control and data acquisition (SCADA) based Operational Technologies (OT)
    - Improving efficiency (power factor control)
    - Load Control (limiting peak power )
    - Continuous condition monitoring (both normal and abnormal conditions)
    - Trend and alarm monitoring (problem identification)
    - Historical data and data viewing from remote locations (system monitoring)
    - Reliability and Resilience (response to service interruptions)
- Information Technologies (IT)
    - Quasi-real time usage data (Demand Response)
    - Customer based energy efficiency decision making (Green Button[10])
    - In-house and third party billing and payment processing

If every one of these technologies were incorporated into an electric utility system, the system could be referred to as a Smart Grid. More importantly, if any subset of these technologies is implemented into a distribution system, the system could still be referred to as a Smart Grid. Therefore, any discussion of the "Smart Grid" creates a great need to be very clear on which set of technologies are being discussed and which are not. A clear understanding by all parties discussing a "Smart Grid" will alleviate later confusion and disagreements about any conclusions and/or agreements which were made during such conversations.

However limited or inclusive a definition of 'Smart Grid' is considered, there is widespread agreement that the information smart technologies provide system operators can create benefits such as fewer and shorter outages. There is also widespread agreement that the information smart technologies provide customers can create benefits such as reduced consumption and energy costs, and increased efficiencies. Smart technology-provided information can also be used to inform decision making on product and/or equipment selection and replacement; thereby increasing investments for both the system operator and the customer.

While an increase in the use and availability of smart systems will increase the availability of actionable information for both system operators and customers, that same growth will create vulnerabilities for the foreseeable future[11]. The net result of greater access and information exchange within the system creates more opportunities for threats to the utility system and therefore increases the need for enhanced security.

## 4 PSC Role and Security at Missouri Utilities

Cybersecurity of interconnected utility systems involves not only the physical distribution and transmission systems, substations and offices, but also equipment and systems that communicate, store and act on data. Cybersecurity encompasses utility-owned systems and aspects of customer and third-party components that interact with the grid such as the advanced metering systems.

[10] The Green Button initiative is an industry-led effort that responds to a 2012 White House call-to-action to provide utility customers with easy and secure access to their energy usage information in a consumer-friendly and computer-friendly format. http://www.greenbuttondata.org/

[11] Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector Mission Support Center Analysis Report, Idaho National Laboratory, August 2016, Office of Scientific and Technical Information Document #1337873

And more than simply being a function of hardware, cybersecurity is critically important as a function of software, data and the networks that transfer data and use that data to keep the system operating.

Cybersecurity vulnerabilities exist wherever computer systems and data exist. With the advent of smart technologies, which layer software on top of utility operations and computer systems, threats become increasingly likely and relevant. The aims and implications of cybersecurity violations vary widely. Gaining system control, the ability to remotely modify and operate the system or its characteristics as a vehicle for attack, is but one threat. Data theft, or "exfiltration," is also a known and on-going problem. Cybersecurity must protect against inadvertent sources of data loss, such as user errors, hardware failure, software bugs, operator errors or just plain negligence. Natural disasters also present a major threat.

The Commission finds itself at a critical juncture for infrastructure protection as utility systems transition from a previously isolated environment to a complexly interconnected one. With such a dynamic and broad landscape to consider, both cyber and physical security cannot be a stagnant prescription. It should evolve as technology, threats and vulnerabilities evolve, introducing the building blocks that stand the test of time while still being flexible enough to meet changing security requirements.

The Commission is charged with the duty of assuring that utility companies provide safe and adequate service at just and reasonable rates. Because cyber and physical security threats challenge the reliability, resiliency and safety of utility systems, and because utility spending to address security vulnerabilities can impact the bills that customers pay, the Commission must explore, understand, and ensure the integrity of each utility's internal physical and cybersecurity practices. It was with this goal in mind that the Commission opened this working docket.

The Department of Energy (DOE) has stated that because of a rapidly changing technology landscape, effective cybersecurity requires continuous and comprehensive assessment of threats, identification of system vulnerabilities, strengthening and sharing of recognized security practices, and analysis of the impact of cyber events on the infrastructure. Timely bi-directional sharing of cyber threat information between the energy sector and government helps to determine the severity, scope, and nature of threats and helps to rapidly develop mitigations.

The following graphic represents the "Sliding Scale of Cyber Security". It presents the continuum of possible types of cyber defensive positions that an entity can undertake. Any one entity can take any position on this scale at any time subject to the threat being posed; hence the "sliding scale".

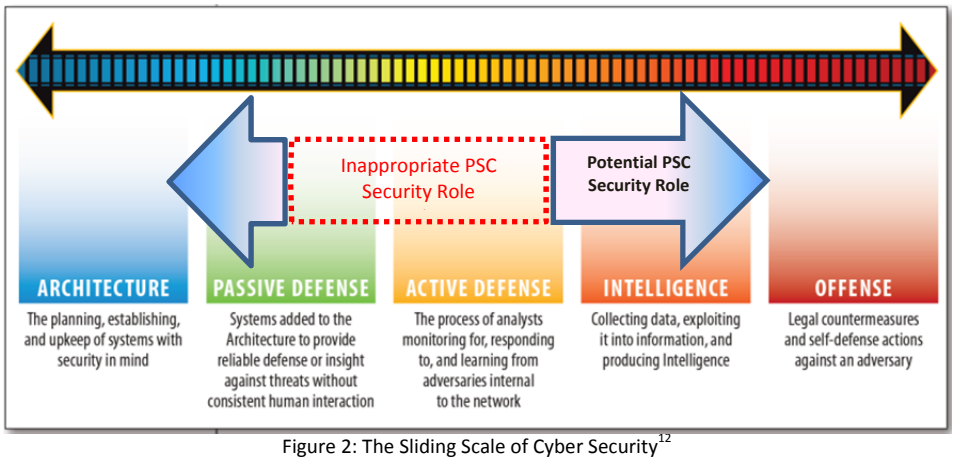

Figure 2: The Sliding Scale of Cyber Security[12]

The blue arrows overlaid on the Sliding Scale of Cyber Security indicate the areas in which Staff considers it appropriate for the PSC to proactively participate in the cyber defense of Missouri utilities. These four areas are (in no particular order):

(1) Architecture: Reviewing the future plans of each utility as they relate to cyber and physical security and how they relate to the anticipated threat landscape.
(2) Passive Defense: Understanding the current security posture of each utility and the relationship of that posture to industry best practices.
(3) Active Defense: Monitoring the currently active global threats against utilities and communicating those threats to the utilities through an information sharing process.
(4) Intelligence: Through the cooperation of the personnel and the use of assets at the MIAC as well as national intelligence resources, assist in developing a critical infrastructure analytical product for use by all Missouri utilities.

PSC engagement does not, and should not, include participation in the myriad of daily business activities in which utilities engage. The activities involved in managing and actively protecting utility systems on a daily basis is the responsibility of each individual utility. Additionally, the areas Staff identified for engagement are not uniquely the realm of the PSC. Staff fully understands and expects the utilities will and do actively engage in these areas as well.

### 4.1 2015 Workshop and Staff Report

The Commission issued an order opening this case in March 4, 2015. A workshop was held on March 23, 2015, to discuss issues related to cybersecurity and physical infrastructure security. Stakeholders provided comments over the next few months culminating with a Staff report filed on October 23, 2015. A brief summary of the 2015 Staff recommendations are as follows:

1) Since utilities are actively engaged in [physical and cyber] security, Staff does not recommend the Commission promulgate rules related to cybersecurity or infrastructure

[12] Robert M Lee, Sans Institute, 2015, https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

security.

2) With existing processes in place to report incidents or events that result in injury, death, significant infrastructure damage, or which may result in significant attention (i.e., make sure the Commission is aware of an incident before it learns about it through the news), Staff recommends that natural gas and electric utilities continue to communicate such incidents to the Commission on an informal basis. Additionally, Staff recommends:
   i) This process be expanded for all non-telecommunications utilities to include verbal reporting of cybersecurity or infrastructure security events or breaches that affect many customers, involve the release of customer proprietary information, or which pose a threat to the general public.
      - Reports to be provided to a Staff member directly involved with emergency management functions.
      - Staff will verbally inform the Chairman/Commissioners as deemed appropriate.
      - While written records will not be retained regarding individual contacts, the information may result in Staff or the Commission requesting an investigation into any potential issues.
   ii) Telecommunications:
   Due to limited jurisdiction over telecommunications providers, Staff recommends the Commission encourage telecommunications providers to interact with Staff in the event there are cybersecurity or infrastructure security events or breaches that affect many customers, the release of customer proprietary information or which pose a threat to the general public.

### 4.2 2017 Workshop

During 2017 the Commission again expressed that it was necessary to look at the status of security at Missouri regulated utilities and the utilities' relationship with SEMA, the Missouri Highway Patrol (MSHP), and their respective intelligence resources for the protection of CI in Missouri. Shortly thereafter, the position of Critical Infrastructure Security Engineer (CISE) was created at the PSC and a Staff member was appointed to fill that position. The charge for the CISE was to investigate the current state of security at Missouri utilities, become integrated within the state fusion center - the MIAC, and understand and coordinate with SEMA since the PSC is the lead agency for the Emergency Support Function (ESF) for energy related emergency response (ESF-12).

Staff held a workshop to investigate the state of utility security, the role of the PSC within the realm of utility security, and to determine what the path forward might look like from the perspective of the utilities and other interested parties. Many comments were received, which are all available in detail on the PSC's Electronic Filing Information System (EFIS). The workshop was intended to be a baseline for Staff to better understand the current security-related issues and what to focus on going forward. The following is a high-level summary of the workshop topics and some excerpts of responses from the workshop.

- **Is there a need for a legislative proposal to safeguard critical infrastructure security information?**
  - Information sharing is a key element to any successful security program.

- Exemptions to the Freedom of Information Act (FOIA) and Missouri's Sunshine Law are needed to protect critical infrastructure and threats to intelligence information from disclosure.
- In-person communication is the preferred method for sharing information with the Commission.
- Minimum encryption/file-protections standards for information should be considered.
- Third parties disclosure of usage information for marketing purposes should not be allowed.

- **How can the PSC assist in the deconfliction of federal and state responsibilities?**
  - State regulatory action in an area with robust federal regulations may create conflicting requirements.
  - State understanding of the sector-specific federal requirements and their interactions would assist in containment and recovery in the event of an incident.
  - Utilities should make use of available state and federal protective initiatives.

- **Is there a need for cyber and physical security performance measures and metrics?**
  - A "one-size-fits-all" approach to measures might not work for utilities with unique characteristics.
  - Some federal work is being done on a baseline set of measures and metrics.
  - NERC CIP[13] standard audits already take place on a regular basis.
  - Measures could be used to determine areas that need focus.
  - Separate definitions and processes for event or incident reporting are recommended.
  - Consistency across all sectors is a key ingredient to reporting requirements. As such, a cross sector working group would be useful to accomplish consistent reporting requirements.

- **Is there a need for a functional listing of utility security personnel?**
  - Some utilities have expressed a willingness to supply such information.
  - Must have privacy and access control(s) for personnel confidentiality.

- **Should the PSC develop a formal group for cyber related information exchange and/or monitoring between utilities?**
  - Sharing information on these issues with the PSC needs to be confidential.
  - These types of information sharing groups already exist at a federal level – redundancy is not helpful.
  - Many avenues of sharing already exist, maybe the best route would be to make sure those are known and used by all utilities.
  - Fusion centers[14] already provide this to a certain extent.

[13] North American Electric Reliability Corporation Critical Infrastructure Protection Standards - a set of requirements designed to secure the assets required for operating North America's bulk electric system

- Sharing between utilities might be a great avenue to permit utilities to learn from each other.

- **Should a formal cyber related mutual aid and assistance plan be developed?**
  - This already exists at the Edison Electric Institute (EEI) for electric industry but requires significant investment.
  - The EEI program is being expanded with the American Gas Association to include gas utilities.
  - Might be difficult to implement due to the variations in system makeup.
  - This already exists for water utilities.

- **Should the PSC support monitoring intelligence feeds and pushing out intelligence products for events related to Missouri?**
  - Cyber [15]is not defined by state borders.
  - Defining Missouri-focused issues is difficult.
  - Products already exist from the federal level.
  - Fusion centers already produce and distribute products with a Missouri focus.

- **Should cyber related risks be contemplated while reworking ESF12 emergency response plans?**
  - Emergency response plans could highlight the portion of the plans related to cyber response to assist in identifying actions in the event of a cyber event.
  - Emergency response plans at the ESF level should not include cyber risks as a specific issue as these are already included in company response plans and from the ESF level, the reason for an outage is immaterial to the response.
  - Cyber risks should be included to ensure the availability of support resources if an event were to occur.

- **Should all Missouri utilities submit updated emergency response plans on a recurring basis?**
  - General plans can be shared with little concern. More detailed response plans can be highly sensitive and sharing of such plans can be more problematic.
  - The Missouri Department of Public Safety (DPS) or the Missouri State Highway Patrol (MSHP) may be better positioned to provide assessments of these types of plans and that venue may be better as a path of sharing information.
  - The question for consideration is what level of detail should be included in a plan required to be shared?
  - Who will be responsible for the protection of the information contained in the plans, and who will be responsible for the aggregation of the plans to determine the sufficiency of resources in the case of a large event?
  - Without a guarantee of a FOIA exemption, there is a concern for public disclosure of CI information.

---

[14] Fusion centers operate as focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, tribal, territorial, and private sector partners.

[15] Relating to or characteristic of the culture of computers, information technology, and operational technology

- Any plan submissions should be limited to general topics of response. Details should not be included with any submission of emergency response plans.
- It is difficult to take a position on such a requirement as the underlying knowledge of the business interests supporting such a requirement is unknown.

As can be ascertained from the included selection of comments received from the workshop, there is no universal opinion as to the best direction that the Commission should take regarding security issues at Missouri utilities. That being said, no stakeholder suggested that the Commission take no actions concerning utility security.

### 4.3 2019 Staff Recommendations

Historically, the relationship between the Commission and the security activities at Missouri utilities was largely an informal one. The following Staff recommendations include actions that, in Staff's opinion, can be taken by the Commission without opposition such as more active involvement of Staff in emergency response exercises. However, other more complex recommendations on issues such as cyber and physical security event reporting will require further effort including more detailed stakeholder interactions and agreements and may ultimately face opposition to implementation. Each recommendation contains a short description and/or rationale with the associated **Staff Recommendation in bold**.

#### 4.3.1 Testing of Utility Infrastructure Security

Some commissions such as the Illinois Commerce Commission require disclosure of specific information to evaluate the state of utility physical and cyber security. Other commissions perform intrusion testing[16] of utility facilities and/or penetration testing[17] of utility cyber systems.

In the opinion of Staff, the Commission is not currently positioned to perform either of these types of testing. Additionally, there are other readily available resources for these types of testing at little to no cost. For example, the DHS will perform penetration testing for utilities as a part of its function and engagement with critical infrastructure owners. The Missouri National Guard Cyber Team can also assist with testing on an as needed and as available basis. The Cyber Team also offers some cyber security training for private infrastructure owners as well as public employees to help organizations secure their systems. **Staff recommends that all utility owners and operators engage the DHS and the Missouri National Guard Cyber Team and leverage these resources which can be utilized at little to no cost.**

[16] Intrusion testing is an authorized attempt to gain physical access to facilities by methods or locations not normally authorized i.e. bypassing security through fraud or stealth. The intrusion test is performed to identify both vulnerabilities, such as the potential for unauthorized access, as well as strengths in the system to allow for a risk assessment to be completed.

[17] A penetration test is an authorized simulated cyber-attack on a computer system performed to evaluate the security of the system.

### 4.3.2 Security Information Disclosure and Exchange

The primary reasons for utility security-related interactions is to enable Staff to transfer actionable information between utilities, enhance the Commissions' situational awareness, and prepare emergency response plans. For the purposes of these recommendations, formal disclosure will be in written form and presented to Commission Staff for review. Informal disclosure will be done verbally with Commission Staff and would be the basis for further discussion and/or review of incident response, additional security measures and/or posture changes. Therefore, Staff recommends:

(1) **As more specifically described in the subsections below, Staff proposes the Commission requires utilities to share plans formally with Staff specifically related to emergency response and disclose informally current security posture and other security related utility activities. Additionally, Staff proposes the Commission require informal disclosure, to Staff, of both cyber and physical security incidents and any related response(s) and effect(s). Timing of disclosures should be done on a regular basis with the possibility of a Commission briefing by utility personnel and/or Staff as requested or as an incident situation warrants.**

a. The emergency response plans shared with Staff will allow for the identification of any potential overlap of utility expectations from state responders and/or resources. If such overlaps exist they should be addressed within each respective emergency response plan.
b. All shared emergency response plans should be to a level of detail sufficient to enable PSC personnel to evaluate potential overlaps but not to such a fine detail to over burden a utility with unnecessary work related to information sharing with the Commission when small plan details change.
c. The informal disclosure concerning ongoing security activities and posture would provide Staff with better situational awareness and enhance communication between the disclosing utility, the Commission, Commission Staff, and other utilities which may be affected by the security related issue.

(2) **Continuation of informal briefings between utility security personnel and Staff for better situational awareness and ease of communication in the event of an issue at a Missouri utility.**

### 4.3.3 Supply Chain Risk Management

Supply Chain Risk Management (SCRM)[18] is a threat vector that is now coming to the forefront of the threat landscape. The disclosure by DHS concerning significant attempted intrusions into critical infrastructure systems originated with an attack on a utility vendor**. Staff therefore recommends that as part of an informal disclosure process, utility plans for addressing supply chain risk management be specifically addressed with Staff.**

[18] Supply-chain risk management (SCRM) is a process to assess the risks and uncertainties associated with logistics-related activities and/or resource suppliers within your supply chain.

### 4.3.4 Cyber and Physical Security Points of Contact

Utilities should actively update security related personnel contact information. This will help to ensure that contact information will lead Staff to personnel that can discuss security issues directly and not through intermediaries. If personnel changes occur, new contact information should be reported without delay. Even without personnel changes a proactive process of updating contact information will assist in limiting natural inertia to assume security personnel contact information is fresh.

**Therefore, Staff recommends that each Missouri utility be required to identify and provide, to Staff, contact information for both a cyber and physical security point of contact that would be actively updated when personnel changes occur or at a minimum be updated twice a year. These points of contact should be required to be personnel actively engaged with both cyber and physical security issues and not a member of the utilities' counsel or regulatory liaison activities**.

### 4.3.5 First Responder Network Authority (FirstNet)

FirstNet[19] is a nationwide system of user tiered prioritization for cellular communications. Funded by the National Telecommunications and Information Administration (NTIA) as an interoperable first responder network, the system overlays and enhances the existing AT&T cellular network.

FirstNet users are segmented into tiers with first responders having the highest priority, emergency response and governmental entities having a second tier position and ordinary commercial cellular communication in the third and lowest tier. The idea behind FirstNet is to minimize first responder communication issues during emergency situations where communication volume is high and may exceed the capacity of the system. The system still allows lower tier communications to occur as capacity becomes available.

FirstNet is now operational in Missouri having been implemented over the past few years. The Missouri Statewide Interoperability Center (MOSWIN) and the Office of Administration Information Technology Services Division (OA-ITSD) are currently switching state agencies to FirstNet services. The program was tested and proven effective during previous flooding events.

Although the PSC is not a first response agency, there are emergency response and other safety related functions within the PSC that would allow membership as a second tier organization. **Staff, therefore, recommends transitioning cellular communication accounts to FirstNet for those employees that participate in emergency response and/or other emergency and safety related activities.**

Personnel that utilize privately owned phones related to emergency and/or safety related activities are also able to join FirstNet. There may be cost and/or account changes for those employees who choose to join FirstNet. **Staff, therefore, also recommends Staff members individually investigate transitioning personal phones used for communications during**

[19] www.firstnet.com

**security related activities to FirstNet if prioritized emergency communications is warranted.**

### 4.3.6 Structural Assessment and Visual Evaluation (SAVE) Coalition Enhancement(s)

The SAVE[20] Coalition is a group of volunteer engineers, architects, building inspectors and other trained professionals that assists SEMA with building damage inspections. SAVE volunteers have been trained to move quickly after a disaster to determine which buildings are safe to use, which are marginal, and which should be evacuated. The SAVE Coalition was established by Section 44.023 RSMo during the 1990s.

While this Coalition is currently focused on structural assessments of buildings and other vertical structures, it could be argued that there is a ready built process for the development of a resource for the evaluation of other critical infrastructure in the event of a natural or man-made disaster. The structure and membership system required for developing an organization that has experience in observing and evaluating the physical condition of critical infrastructure already exists within the SAVE Coalition. Expansion of this program to include other types of infrastructure would need to be developed in cooperation with SEMA and may require a legislative effort to amend Section 44.023, RSMo. **Staff recommends the PSC work with SEMA and develop a proposal to expand the types of volunteers that could join the SAVE Coalition as well as expand the types of evaluations that could be carried out by such members. This expansion would focus on structures associated with utility critical infrastructure and those volunteers with knowledge of such structures.**

The State of Michigan created an organization similar to SAVE but focused on cyber security. The Michigan Civilian Cyber Corps, established by statue, is utilized as an asset for private sector organizations that need assistance in the event of a cyber security incident. The organization is not intended to be an organization's primary source of cyber security but as a supplement in the event of an emergency. The Missouri SAVE coalition could be used as a model for such an organization in Missouri but the creation of such an organization would appear to require legislative action as cyber security activities fall well outside the physical structure-focused activities of the SAVE coalition. **Staff also recommends the Commission work with SEMA to investigate the activities and partnerships necessary to create such a volunteer organization.**

### 4.3.7 Missouri Information and Analysis Center (MIAC) Engagement

The current partnership with the Missouri Information and Analysis Center has been successful. The MIAC has integrated the Commission liaison position and has made the necessary intelligence assets available for use by the CISE. A question raised during the 2017 workshop concerned the possibility of the creation of a Missouri-centric intelligence feed. **Staff recommends against the development of a Missouri-centric cyber intelligence feed as the nature of the cyber threat does not confine itself to state borders. As for a Missouri-centric physical security intelligence feed, that type of product is already available through the MIAC.**

[20] sema.dps.mo.gov/programs/SAVEcoalition.php

The MIAC also has available a Sensitive Compartmented Information Facility (SCIF) for the dissemination of classified materials to those parties with a right and a need to know. Secure briefings take place at the MIAC and are regularly conducted within the SCIF. **Staff recommends the Commission's MIAC liaison proactively inform Missouri utilities about the capabilities at the SCIF and timing of any classified briefing that are taking place for cleared personnel.**

### 4.3.8 Intelligence Liaison Officer (ILO) Program

The MIAC also has an effort referred to as the Intelligence Liaison Officer (ILO) program. The ILO program recruits, vets, and trains private and public sector partners with which to share intelligence information. The program also encourages reporting by members when encountering suspicious situations during their normal activities. While many utilities currently have ILOs within their organization, **Staff recommends the Commission encourage the utilities to actively participate in the MIAC ILO program to receive pertinent threat information and provide information on suspicious activities that they may encounter in conducting everyday operations.**

### 4.3.9 Utility Group Focused Information Sharing Organization

The MIAC and the Missouri National Guard have received inquiries from members of the Central Electric Power Cooperative to develop an information sharing group with other Missouri utilities. There has also been positive feedback from some investor-owned utilities to participate in such a statewide group. While this type of Missouri-centric industry group should be organized and developed by the utility industry, the PSC should encourage and support this effort in whatever capacity possible. **Staff, therefore, suggests that the PSC actively participate in the organization and development of such an industry group and encourage all Missouri utilities to participate.**

### 4.3.10 Interaction with the Missouri State Emergency Management Agency (SEMA)

As the ESF-12 lead state agency, SEMA has recommended that there are two to three members of the agency that are trained in the Incident Command System (ICS) at the ICS300/400 level so they can actively participate at the Emergency Operations Center (EOC) in the event of an emergency. **Staff recommends that at least three members of the Staff be identified and trained to the ISC400 level.**

SEMA has also requested a Continuity of Operations (COO) document from each lead agency. This work is currently underway, but in the process of developing this document using the information contained within the Commission's general procedures, GP-7 and GP-7.5[22], it appeared that those documents require updating. **Staff will review GP-7 and GP-7.5, and update as necessary.**

[22] GP-7: Emergency Response Procedures and GP-7.5: Emergency Support Function Procedures

### 4.3.11 Utilities Information and Mapping

The information available in the PSC-internal "Utilities Information & Maps" binder, which is used by certain Commission personnel at the EOC, has not been updated recently. Further, the process for updating the maps contained in the binder is laborious and time consuming given that it was originally created within a drafting software application. Modern mapping is done through a Geographic Information System (GIS) and is displayed through a layered system. For example, the state boundary can be overlaid with the county borders easily as the layers have been built to be readily used. GIS layers for critical infrastructure are available and are continually updated by federal, state, and infrastructure owners. **Staff has no specific recommendations at this time, but recommends the Commission periodically review GIS related software options.**

### 4.3.12 Emergency Response Exercise Participation

**As the lead state ESF12 agency, the PSC should continue to actively participate in upcoming emergency response exercises, and in particular any New Madrid Earthquake[23] exercises. When possible, participation in other local, regional, and national drills and exercises should also be pursued.**

### 4.3.13 Cyber and Physical Security Measures and Metrics

The possibility of developing measures and metrics for utilities to formally report to the PSC has an attractive nature as such measures and metrics would allow for the evaluation of the status and/or improvement of the security situation at any particular utility. Unfortunately this is a very difficult task. Every utility has different security postures and processes in place and finding a small set of measures that would encompass all situations is problematic at best. There are efforts at the federal level attempting to define metrics for this purpose but the results of these efforts have not been completed**. Staff recommends these efforts be monitored, and if they produce useful results, the implementation of a reporting mechanism for such metrics be evaluated at that time.**

## 5 Summary and Conclusion

Even though the Commission is not required to actively participate in the day-to-day defense of utility critical infrastructure, the Commission does have the responsibility to ensure Missourians receive safe and reliable utility services at just and reasonable rates, by:

(1) Understanding what actions utilities are taking in the effort to secure their infrastructure and reviewing whether those actions are reasonably within industry standards.
(2) Understanding what security incidents are occurring, if there's a pattern to those incidents, and if those incidents can be better managed with improved utility

[23] FEMA Shaken Fury 2019 Exercise Scenario. https://www.fema.gov/media-library/assets/images/175766. Staff participated in the June 2019 New Madrid exercise.

security posture.

(3) Informing all Missouri utilities of any persistent incidents which may have been identified through the analysis of reported incidents.

(4) Responding to incidents in the state that may have affected utility services as the lead agency for EFS-12 through emergency operations at SEMA.