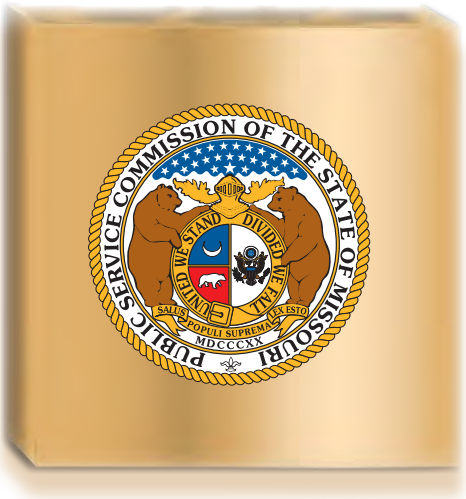
KEEPING YOUR UTILITY SERVICES SAFE & SECURE



— **Michael Rush**, PSC Critical Infrastructure Security Engineer

The Missouri Public Service Commission (PSC) has undertaken the task of addressing the state of physical and cyber security for essential utility assets and services within Missouri. The creation of a new position dedicated to Critical Infrastructure (CI) security was the first step toward evaluating and improving the protection of these essential systems, data, and other assets in Missouri.

The National Institute of Standards and Technologies (NIST) has issued guidelines on a more focused approach to security. The guidelines focus on risk management using continuous monitoring and real-time security assessments. The core of these guidelines is a framework whereby the most critical assets are identified; procedures are developed to protect those critical assets; resources are applied to detect security threats and respond in a timely manner; and preplanned recovery efforts are developed if a threat were to successfully interrupt or disable the asset. These guidelines are applicable to both physical and cyber security. While some Missouri utilities already utilize this approach, the Commission is dedicated to ensuring all regulated Missouri utilities employ a similar approach to protecting the states utility assets and services.

WHAT ARE PHYSICAL & CYBER SECURITY?

Physical security naturally involves cameras and other surveillance systems, guarded entrances, fences and other barriers to physical entry into a facility. However, physical security also includes securing facilities and equipment from physical harm due to weather, vandalism, energetic attacks, or electromagnetic disturbances. Physical security is an all-inclusive topic, which uses an all hazards approach to threats which can cause any type of physical harm to facilities and/or equipment.

In the world of computers, security *means* cyber security. Cyber security is generally defined as the technologies, processes, and practices designed to protect networks, computers, software and data from attack, damage, or unauthorized access. Making sure that things are protected in the cyber world includes securing the applications that operate the system, the information needed to operate the systems, user and

customer information, and the restoration of those systems and/or data in the event of damage or loss.

One of the largest issues in addressing cyber security is the rapid changes in technology which lead to evolving security threats. A traditional approach to security that singularly focuses on the protection of individual components is no longer a viable methodology. Therefore, it is necessary to use a layered approach because the layered approach will require each attack to penetrate each successive layer of a system. This allows the entity protecting the system to secure a layer to a threat, while simultaneously protecting the many system components that reside under that layer. The protecting entity can also rank the current set of threats by reviewing the depth to which the attacks were successful.

An often overlooked and critical part of both physical and cyber security is the idea of resilience. Resilience is defined as the ability to adapt to changing conditions and withstand and/or recover rapidly from disruptions. Unfortunately, security measures will not withstand all threats. In the event that a natural disaster or successful attack against critical infrastructure occurs, the ability to rapidly restore services is an extremely important aspect of security.

WHAT IS CRITICAL INFRASTRUCTURE?

Critical Infrastructure (CI) provides essential services necessary to serve the economy, security, and health. Each of us recognize it as the power we use at home and at work, the water we drink, the roads and bridges on which we drive, the stores at which we shop, the hospitals and emergency services we rely on when in need, and the communication systems we use to stay in touch with doctors, schools, family and friends. The Department of Homeland Security (DHS) has identified 16 CI sectors vital to the health and welfare of the nation and its citizens. Among these sectors are

energy, dams, nuclear facilities, water and wastewater systems, transportation services, commercial facilities, healthcare, emergency services, communications and information technology.

WHAT DOES THE PSC CRITICAL INFRASTRUCTURE ENGINEER DO?

The Critical Infrastructure Security Engineer (CISE) is responsible for engaging both regulated and non-regulated utilities and encouraging compliance to NIST guidelines on physical and cyber security.

The CISE will work with utilities, law enforcement agencies, and the Missouri State Highway Patrol's Missouri Information Analysis Center (MIAC) to review the current state of physical and cyber security of utilities in Missouri and the threat landscape those security measures must face. The CISE will also make suggestions about improving CI security as well as collect, analyze, and disseminate security related information to utilities throughout the state in partnership with the MIAC.

Utilities regulated by the PSC are granted certificates to solely operate in a specific area in exchange for Commission oversight on costs, investments and rates. The Commission develops rules in accordance with state statutes to ensure safe and reliable utility services at just and reasonable rates. In today's computerized environment, 'safe and reliable' services require strong cyber and physical security measures. Physical or cyber penetrations or disruptions can lead to loss of critical services or loss of customer data to unauthorized persons.

While the Commission does not have direct regulatory oversight of all utilities in the State, the Commission does regulate the operational safety of the state's rural electric cooperatives and municipally owned natural gas utilities. The Commission has a good working relationship with the non-regulated utilities and is exploring methods to coordinate with regulated and non-regulated utilities on security issues.

WHAT IS THE PSC'S RELATIONSHIP WITH THE MIAC AND SEMA?

The Missouri Information Analysis Center (MIAC) is a public safety partnership between local, state and federal agencies, as well as private sector members.

The purpose of the MIAC is to gather, analyze, and disseminate information in a timely and effective manner. Reports of suspicious activities inside and outside of Missouri are analyzed to determine their effect on the safety of Missouri citizens and infrastructure. The MIAC is a two-way communication link between partner organizations to enhance the safety and security of our community. The CISE will be working directly with the MIAC and will be the bridge between the information available at the MIAC and Missouri utilities.

The PSC also works with the State Emergency Management Agency (SEMA) to carry out the mission to protect the lives and property of all Missourians. SEMA responds to both natural disasters and those caused by man. It is also responsible for developing State Emergency Operations Plans and putting those plans into action when a disaster strikes. Coordination of local, state and federal agencies during a disaster is the backbone of these emergency plans. SEMA has various Emergency Support Functions (ESFs) that coordinate efforts to respond to emergencies and natural disasters. The PSC actively participates in the ESFs for energy, communications and to a lesser degree, water and sewer. In this role, the PSC serves as a liaison between the utilities and SEMA, answers questions and works with the utilities on such things as response and restoration times, and addressing utility needs of critical functions such as those required by hospitals. The PSC also participates in periodic mock emergency exercises.

WHAT IS THE ROAD FORWARD FOR THE PSC AND CRITICAL INFRASTRUCTURE SECURITY?

The PSC is committed to its mission of ensuring safe and reliable utility services at just and reasonable rates to Missourians. The CISE will be enhancing the safety component of the Commission's mission by helping Missouri utilities improve both their physical and cyber security. Through the new relationship with the MIAC, the CISE will be enabling dissemination of pertinent security information to Missouri utilities thereby enhancing reliability. Along with the continuing relationship with SEMA, these are positive steps to furthering safe and reliable service to Missouri citizens.