Prepared Statement of Mark A. Gabriel, Administrator and CEO of Western Area Power Administration, for the Security Investments for Energy Infrastructure Technical Conference Cyber and Physical Security, Best Practices, and Industry and Government Engagement panel March 28, 2019

Good morning. My name is Mark A. Gabriel, and I am the Administrator and CEO of Western Area Power Administration. WAPA, a power marketing administration within the Department of Energy, is responsible for marketing and delivering federal hydropower and related services to nearly 700 preference power customers across a 1.3 million square-mile territory encompassing all or parts of 15 central and western states. WAPA owns, operates and maintains $4.3 billion in transmission assets, including more than 100,000 structures along 17,305 miles of transmission lines, 322 substations, 291 high-voltage transformers and four control centers and SCADA systems.

As one largest transmission owners and operators in the nation, one of WAPA's most significant challenges is appropriately protecting its extensive assets while containing costs. To that end, WAPA has been innovative and collaborative in seeking solutions to effectively and affordably protect its assets from cyber and physical threats.

WAPA's security and reliability programs have been validated through the results and recommendations of audits by DOE, Western Electricity Coordinating Council, Midwest Reliability Organization and industry peer groups. The professional staff at WAPA takes personal responsibility in doing what is right and safe for grid operations and security, as well as in meeting the spirit of compliance.

We have completed more than 345 physical security assessments since 2014, and 316 remediation items were implemented in fiscal year 2018. We are scheduled to complete risk assessments for all our assets in 2019. Since September 2017, we have completed 12 security projects through a $25-million contract designed to remediate risk at our facilities.

Our Office of Security and Emergency Management is implementing new baseline security standards across the enterprise to better align resources to asset criticality. By proportionately assigning resources to our most critical assets instead of a "one-size-fits-all" approach, we expect to realize more than $1 million in savings over the next several years while providing the most effective protection to our extensive assets.

In 2018, cybersecurity tools identified more than 10,000 individual cases of suspicious activity on our system. More than 97 percent of these were investigated and resolved within two days. In an average day, WAPA's firewalls are pinged nearly 200,000 times by suspicious or potentially damaging events. Aggressive education and training programs have strengthened employees' ability to recognize and defend against phishing, the primary technique used by hackers to access secure systems.

As our security posture and awareness have matured, we have discovered interdependencies between our Cyber Security, Physical Security and Asset Planning and Management programs.

By looking at grid security holistically, wherein each effort complements and strengthens the others, we can more efficiently and cost-effectively defend our infrastructure from attacks.

We are not undertaking security efforts alone. Due to the connectedness of the bulk electric system, we all play critical roles in defending the grid. To share best practices, information on current threats and lessons learned, WAPA convenes stakeholders, security experts, customers and other utilities to bolster the knowledge and awareness of the collective industry. Our 2018 Technology and Security Symposium looked at threats and leading practices broadly, while a smaller meeting focused on the convergence of operation and information technology to better promote the resilience of certain grid components.

WAPA participates in numerous forums to improve its cybersecurity posture, including nine associated with DOE agencies that focus on addressing different cybersecurity vulnerabilities. Finally, we take part in government and industry exercises, such as GridEx, to test our response and recovery capabilities.

We are streamlining certain procurement actions to shorten our recovery time in case of an event, especially in regard to large power transformers. Our goal is the cut the lead time for transformer acquisition in half. This effort will support lifecycle replacements and periodic system additions and allow WAPA to more quickly recover from a high-impact, low-frequency event.

Another area of concern is supply chain security. Many electric components are purchased outside the U.S. because they are no longer made in this country or are manufactured by so few companies that a security breach at one organization could have significant detrimental effects across the industry. We appreciate the focus of FERC, NERC and the Administration on this area to develop bulwarks against vulnerabilities introduced in the supply chain, and we also participate in supply chain risk management for control systems environments.

These measures are absolutely imperative. We have no option but to make these investments in monitoring, hardening and reconstitution activities. We must all work together to identify leading practices, most efficient deployment of security resources and, when possible, share in the costs of safeguarding the electric grid.