UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Commission Notice of Inquiry	**)**	
Virtualization and Cloud Computing	**)**	**Docket No. RM20-8-000**
Service; Comment Request	**)**	

COMMENTS OF GRIDBRIGHT, INC.

GridBright, Inc. ("GridBright")[1] respectfully submits these comments in response to the Federal Energy Regulatory Commission's ("FERC" or Commission") Notice of Inquiry request for comments on Virtualization and Cloud Computing Services ("Notice").[2]

GridBright supports the Commission's examination of this important and emerging area of computing support for the utility industry and its intent to establish a record for potential modifications to the CIP Reliability Standards. Through GridBright's commercial services and two ARPA-E research projects,[3] we have worked with industry, academia, research, and regulatory value chain participants specifically in the areas of the Notice's focus. That experience informs our perspective, insights, and the following comments. Our comments are structured in themes that may cross one or more of the four areas of inquiry requested by the Commission.

[1]GridBright Inc., (www.GridBright.com) specializes in electric grid integration. Its services and solutions span the full electric value chain safely interconnecting renewable and distributed energy resources to the grid, implementing and integrating modern computer applications for grid operations and planning, and providing the secure exchange of grid data among grid value chain participants.

[2]FERC Notice of Inquiry; Comment Request, 85 Fed Reg 11363 (February 27, 2020), Docket No. RM20-8-000.

I. COMMENTS

A. Five years of DOE sponsored research informs these comments

GridBright, over the course of the last five years, has been engaged in research under two ARPA-E projects (collectively "research projects") specifically focused on cloud-based data exchanges. Through these projects, GridBright investigators have encountered many, if not all, the points of inquiry of this Notice.

The first project, now complete, established the BetterGrids repository[4]. The repository is a free library of curated, non-sensitive grid models shared voluntarily by grid researchers. It includes synthetic and anonymized grid models that are created under the ARPA-E GRID DATA Program and uses a rigorous curation process to ensure data quality. AI tools for semantic and natural language searching allow researchers to find their desired test data easily. BetterGrids is used by thousands of grid researchers in 45 countries and has been in production since 2017. Most users are in universities, research institutes, consulting companies, software companies, national labs, and utilities.

GridBright has released the repository software as open-source software and has founded a dedicated non-profit, tax-exempt corporation, BetterGrids Foundation, that governs the Repository Users Group. Volunteers from 50+ organizations, including universities, utilities, ISOs, and consulting companies, are engaged.

The second project was initiated in 2019 when DOE ARPA-E awarded GridBright a contract (DOE Award# DE-AR0001030) to develop the Secure Grid Data Exchange (SGDX). SGDX is a service that is a user-friendly but secure cloud-based approach for sharing sensitive

[4] www.BetterGrids.org

grid infrastructure data. It is based on off-the-shelf open-source distributed-computing technologies and leverages GridBright's prior DOE-funded work building cloud-based grid data exchange solutions.

Secure, compliant, and efficient data exchange is foundational for managing the communication, coordination, and collaboration required to handle accelerating demands on utilities to integrate renewable and distributed energy resources. Such data exchange is also necessary to ensure resilience in the face of increasingly frequent and extended detrimental natural events, and to meet deepening demand for exchange of highly correlated, contextual and timely information between an expanding set of new energy ecosystem actors.

SGDX aims to provide electric value chain participants the capability to exchange sensitive grid and operational data at the highest level of cybersecurity, comply with federal, state, and industry regulations for exchange of grid and customer data, scale services on-demand providing efficient operations in both standard and "extreme" circumstances, standardize data exchange processes for new energy grid operations and market transactions, and automate the workflow of the data exchange process.

The benefits of the SGDX are simplified and standardized grid communications that reduce cyber-security exposures, improve resiliency, and maximize compliance. It eliminates the need for expensive private communications networks and outdated point-to-point systems, and improved operational efficiency of the modern grid value chain with more DERs and fewer CO2 emissions.

GridBright's SGDX partners include Midcontinent Independent System Operator (MISO), Mid-Carolina Electric Cooperative, Inc., and the BetterGrids Foundation. Through BetterGrids, we have engaged over 50 organizations with an interest in enhancing access to grid

data to benefit electric grid operations and research. We have also conducted structured interviews with over 40 representative electricity value chain participants from utilities, ISOs, independent power producers, regulators, technology vendors, academia, national labs, and consultants on requirements for the secure exchange of grid data.

B. Cloud computing services can be leveraged to improve grid operations

Grid operations are becoming increasingly 'federated' as the energy industry value chain disaggregates. As outlined in the NIST Smart Grid Conceptual Model,[5] an ever-expanding set of new actors (retailers, aggregators, and independent energy producers) are emerging. Increasingly, distributed applications using sensors, and controls on the grid edge require cross-domain secure interactions to manage energy balance, voltage, and frequency will comprise the grid of the future. Secure inter-entity communication is fundamental to reliable grid operations, especially in a world of increasingly sophisticated cyber-threats from hackers and state-actors that could disrupt or spoof information flows. Well documented attacks worked by sending damaging control instructions to operating equipment while sending false telemetry data back to monitoring systems.

In our research projects, we have found that many of these inter-entity communications *already* take place over the 'cloud' – including both public networks and virtual private networks. But in most cases, the cloud is treated as a dangerous no-mans-land, and significant investments are required to protect and limit the flow of sensitive information to/from the cloud and mission-critical reliability operations in the security perimeter.

[5] http://dx.doi.org/10.6028/NIST.SP.1108r3

GridBright's SGDX research has identified cloud technologies and services that can *improve* inter-entity communications security, resiliency, and efficiency. Example solutions fall into three broad classes.

i. Solutions to improve the protection of sensitive grid and personal information

A class of solutions to help automate data classification, mask particularly sensitive data values, ensure end-to-end data encryption, certify data accuracy, prevent data loss and enhance audit traceability of information flows beyond the security perimeter. Such Digital Rights Management (DRM) and Data Loss Prevention (DLP) technology have existed for more than 15 years to protect against the unauthorized use or modification of digital media like music, movies, books, and designs. Major vendors like Apple, Microsoft, Google, Adobe, and Autodesk all have off-the-shelf DRM solutions because the creative industry ultimately demanded better content protection technology. Similarly, this technology could be used to protect and track the sharing or leakage of CEII (Critical Energy Infrastructure Information) and PII (Personally Identifiable Information) to enhance CIP compliance and address emerging privacy regulations both within and outside organization walls. It will require the utility industry to agree on digital encryption and tracking standards so that vendors can confidently make investments in DRM technical support.

ii. Solutions to deliver information between entities securely and reliably

A class of solutions to help guarantee the availability of critical operations data while protecting mission-critical computing assets from both external and internal cyber-threats. An example of such technology is Content Delivery Networks (CDN) that have existed for more than 20 years to optimize website performance by routing cloud traffic to the closest available content server. Since then, CDN technology has evolved from solving a simple efficiency issue

to become an essential part of website security and resiliency, helping companies better defend against sophisticated hacker attacks and scale elastically to meet traffic spikes. Vendors like Akamai, Cloudflare, Microsoft, Google, and Amazon all provide turnkey CDN services. Despite being used by almost all major websites across many industries, they are not widely adopted by the utility industry. CDN services could be developed to address utility needs to protect critical assets and dynamically scale communications during emergency situations.

iii. Solutions to reduce the cost and complexity of CIP compliance

A class of solutions to lower the barriers for smaller entities to use enterprise-class security software and monitoring services to ensure safe CIP compliant communications. Services from Managed Security Service Providers (MSSP) are a relatively new breed of cloud-based vendors that allow companies to outsource some of their network and communications security operations. MSSP vendors combine best-in-class security technologies with 24/7 operations centers into a set of turnkey services that can monitor and defend external communications. By sharing threat visibility, expertise, and response team across many clients, they provide very advanced and time-sensitive services at a fraction of the cost of on-premise software investments and staff. MSSP type services could allow smaller utilities and other entities to operate secure virtual private communications networks with high levels of CIP compliance and technical sophistication at a more accessible price point.

All these example solution classes help address the identified need to enhance bulk electric system reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for responsible entities to manage their mission-critical systems at higher levels of cyber-security.

C. Cloud Computing does not presently fit well within CIP standards

GridBright research projects have identified an overall gap in the CIP standards that is the predicate for this Notice, namely not clarifying how entities can use the cloud and cloud-based third-party services safely. The current standards do not adequately contemplate the use of cloud beyond a communications medium and are very oriented to the requirements for on-premise systems to protect the security perimeter against the risks of the cloud. It is thus difficult for organizations to even consider using cloud services for any mission-critical computing or sharing CEII information. They are reticent to deviate from the perceived 'safe harbor' of mature on-premise technical approaches that align with the current standards.

Furthermore, while CIP standards outline the *requirements* for security, they provide very little technical guidance on *implementation*, leaving open the opportunity for inconsistent interpretation across entities. This is especially true in the electric distribution space. The increasing shift towards Distributed Energy Resources (DER) makes distribution network operations a critical part of the BES grid reliability equation. Today, many distribution utilities use NERC CIP standards as a guideline, in the absence of equivalent cyber-security standards for distribution operations. But because CIP doesn't directly speak to non-BES distribution network assets or processes, utilities are left to themselves to interpret. This leads to a sub-optimal situation where some entities are overly conservative (limiting information sharing and stunting ecosystem growth) while other entities consider themselves exempt (creating weak links in the value chain). An anecdotal scenario is a utility that refuses to accept telemetry data from an 'untrusted' customer-owned solar inverter, but ironically accepts that same type of data from a 'trusted' solar aggregator who is not CIP compliant.

There are many well documented jurisdictional concerns in the distribution space. But there is also an established Judicial record[6] dating back to FERC Order 888 that embodies the same questions of BES concerns regarding distribution interrelationships. Although this record addresses jurisdiction in commercial and regulatory arenas vs. the highly technical area of cloud computing and security, that may provide a foundation for potentially more prescriptive guidance at the non-BES distribution level of the grid.

D. The issue is broader than CIP

The U.S. electric industry is a highly regulated sector spanning multiple Federal, state, and in some instances, municipal regulatory jurisdictions. Accordingly, there are unique nuances of the utility regulatory business model which directly impact and inform how cloud technology will be adopted.

Cloud adoption within utility industry is historically muted relative to other sectors driven by security concerns (the focus of this Notice), direct implications of the financial regulatory framework for utilities (i.e., the capital versus expense issue), and the historical statutory definition of what a capital asset is versus what it might be in the future particularly regarding digital assets.

A direct analogy to the cloud adoption issue outlined above is the utilization of software as a service (SaaS) option for utility and new ecosystem functions and activities. SaaS is intrinsically based on cloud technologies and is quickly becoming the predominant computing infrastructure pattern across all sectors of the economy. This circumstance is supported in the record of the Commission's June 27, 2019, Reliability Technical Conference, and the March 28, 2019, Commission/Department of Energy (DOE) Security Investments for Energy Infrastructure

[6] New York v. FERC, 535 U.S. 1 (2002)

Technical Conference. Some estimates have the use of SaaS by all industries to exceed 75% in 2020.

Contributing to the risk of ignoring this clear trend is the fact that the continued regulatory handling of the situation may place the industry in a backward position relative to both the technical sophistication and relative cost of implementation and management of technology.

As the SaaS regulatory issues go hand-in-hand with the cloud, they will undoubtedly proceed in unison until resolution. However, many utilities are not waiting for further clarification and have begun to utilize the cloud in areas that are economically and commercially viable.

For instance, many utilities use turnkey cloud-based e-mail monitoring services for anti-virus and anti-leak protection. Through a simple DNS redirect, these services can both block unsafe attachments from entering the company and prevent CEII classified data from leaving the company. Utilities are also increasingly asking for NERC CIP, ISO 9000, and AICPA SOC Type-2 audit reports when procuring outsourced services. Supply chain risk analysis and monitoring services are becoming more popular. PII focused regulations like GDPR (European Union), or CCPA (California) are creating a further need for compliance-related services from consultants and auditors.

Based on GridBright research projects, we can envision the eventual emergence of third-party compliance services focused exclusively on the unique issues for electric distribution companies seeking to use cloud-based information services. The services could help evaluate the strength and thoroughness of compliance preparations, security policies, user access controls, and risk management procedures. They could also help utilities assess, monitor, and periodically

audit their cloud vendors and business counterparties for cyber risks and policy compliance. Today there is relatively little independent verification that vendors follow cyber-security best-practices regardless of what they may attest during the procurement process.

Market design, and the regulation and policy that supports it, is also a crucial enabler and, ultimately, a driver for the expanded use of the cloud for both operational and market purposes. In many circles, the regulatory hurdle is considered the gate to enabling the implementations of systems and processes that will rely fundamentally on cloud-based technology. In almost every state in the United States, some level of grid market modernization action concerning policies and standards have been undertaken. These actions span policy expansions specific deployments, planning, and market access studies, business model and rate reform, and financial incentives.

By promulgating modifications to CIP reliability standards, the Commission may indeed facilitate broader adoption of cloud computing by not only resolving CIP issues but in addition to fostering their solution of financial and technical issues raised by cloud computing in other regulatory venues.

II. CONCLUSION

GridBright respectfully requests the Commission to give due consideration to the foregoing comments regarding Virtualization and Cloud Computing Services

Respectfully submitted,

/s/ Ali Vojdani
Ali Vojdani
Stephen J. Callahan
Travis Rouillard
GridBright, Inc.
PO Box 830
Alamo, CA 94507
925-899-9025