STATE OF VERMONT
PUBLIC UTILITY COMMISSION

Case No. 20-____-PET

Petition of Green Mountain Power for approval	)
of its Climate Plan pursuant to the Multi-Year	)
Regulation Plan proceeding May 24, 2019 Final	)
Order and 30 V.S.A. § 218d	)

PREFILED DIRECT TESTIMONY OF
MARK DINCECCO
ON BEHALF OF GREEN MOUNTAIN POWER

January 30, 2020

Summary of Testimony

Mr. Dincecco's testimony explains the Information Technology and Communications projects that GMP intends to pursue for customers as a part of the Climate Plan. He describes what these projects entail, what criteria GMP will utilize to select projects, and why they are important as GMP and its customers face more severe weather threats from climate change.

TABLE OF CONTENTS

EXHIBIT LIST

PREFILED DIRECT TESTIMONY OF

MARK DINCECCO

ON BEHALF OF GREEN MOUNTAIN POWER

Introduction

Q1. Please state your name, address, and occupation.

A1. My name is Mark Dincecco. I am employed by Green Mountain Power ("GMP") as its Chief Technology Executive.

Q2. Please describe your educational and business background.

A2. I have been employed by GMP since 2010 as the leader of the company's Information Technology and Operations Technology functions. I have previously worked as a technology and IT security executive at Burton Snowboards, Ben & Jerry's Homemade, Inc., and the United States Environmental Protection Agency. I graduated from Norwich University in 2004 with a Master's of Science in Information Security.

Q3. Have you previously testified before the Public Utility Commission ("Commission" or "PUC")?

A3. No.

Q4. What is the purpose of your testimony in this case?

A4. My testimony explains the Technology and Communications projects that we are recommending as a part of the Climate Plan ("CP" or the "Plan"). I describe what these projects entail, why they are important for our customers, and how the criteria we will use to choose them differs from our typical IT and Communications project planning.

GMP wants to innovate and leverage technology through these new, recommended IT projects to provide virtual, cloud-based platforms, and network infrastructures for mission-critical applications (such as Supervisory Control and Data Acquisition or "SCADA," Outage Management, Advanced Metering, and Call Center Management), so that our digital operations can literally weather a storm while maintaining grid control, communications, and customer-facing services. We also want to expand communications capabilities for our field crews, our customers, and first responders during extreme events.

This new resiliency model for our digital operations is required for safety, reliability, and customer communication as we work to address and combat the impacts of climate change. It will take time and effort to develop these capabilities, including the commitment to add these new capabilities while continuing to focus significant attention on maintaining our cybersecurity posture. But I believe that taking on the planning necessary to complete this work is critical for our customers as I reflect upon how climate change-driven storms can affect our digital and communications systems.

Q5. How does the work you describe for the Climate Plan relate to the other IT risks GMP faces?

A5. Climate change is now another manmade risk, like cyber threats, that we must find ways to mitigate in every area of our operations that will be affected by it. While most of the projects described in my testimony below relate specifically to resiliency work designed to address risks from extreme storms, I do believe that resiliency work will also affect and overlap in part with our cybersecurity work when, for example, we create a new failover system in response to climate risk that also may be utilized, in certain circumstances, if we experience a cyberattack. However, it is important to understand that GMP has many strategies in place at this time to combat such attacks, and that work will and must continue one way or the other, apart from the resiliency work we propose here.

Q6. For background, can you describe in general terms the IT systems and processes GMP has in place to protect its infrastructure and its customers?

A6. GMP uses a combination of physical and logical defense mechanisms throughout its information infrastructure in order to protect its computing hardware, databases, networks, control systems, and other applications. This includes the robust use of firewalls, intrusion and malware prevention and detection applications, threat-hunting software, encryption tools, and the use of "air-gapping" or the physical isolation of critical applications from each other, so that, if breached, the compromise of one system cannot lead to an attack on another. Our implementation of these protective measures is governed by industry best practices like those published by the National Institute of Standards and Technology ("NIST") as well as adherence to established cybersecurity frameworks such as the SANS Institute's Center for Internet Security ("CIS") Top 20 CIS Controls, which provides a framework that prioritizes cybersecurity risk mitigation activities based on best practices. As an additional measure, GMP also provides recurring, online cybersecurity training to all of its employees on a monthly basis as a means of raising awareness of cyber threats, and in turn, using the human capacity of those individuals to be on the watch for potential threats or unusual behavior.

Q7. Philosophically, how does your approach to cybersecurity inform the way you look at the opportunities to increase IT and communications resiliency in the CP?

A7. GMP's management of its cybersecurity infrastructure relies upon an overarching philosophy of isolating key systems from one another and the provisioning of alternate means of providing system operation and continuity in the event of a compromise. Similarly, as it relates to resiliency of many of these same systems in the face of weather-related threats associated with climate change, our Plan proposes focusing on ensuring that critical operational systems and applications can be designed to temporarily sustain a loss of functionality but be brought back into service quickly in another location or in the cloud. The loss of one system or circuit should not result in a catastrophic and cascading loss of the entire system itself. To reach this level of resiliency, we believe that it will be critical for GMP to innovate and take on the task of building these solutions, as the industry itself, and most of our major software and service providers, do not yet provide adequate recovery solutions for the utility industry. Extending this notion further, it becomes even more critical that the synergistic relationship between cyber prevention and recovery methodologies for climate resiliency begin to be developed in tandem, to account for the unsettling possibility that an adversary could opportunistically use the occasion of a storm to attack the system itself.

I. Overview of IT and Communications Projects for the CP

Q8. Please provide an overview of the types of IT and Communications projects GMP recommends for customers as a part of the Climate Plan.

A8. These projects primarily fall within three categories. First, we are recommending projects that will improve the resiliency and durability of communications infrastructures that manage and provide telemetry for grid operations. Second, we recommend IT projects focused on increasing the uninterrupted functionality and durability of key application infrastructures and devices necessary to serve our customers, including: our Outage Management System,[1] Supervisory Control and Data Acquisition (SCADA),[2] and Geographical Information System (GIS).[3] Finally, we recommend projects that will enhance our communication and coordination efforts with municipalities, first responders, and customers during severe weather events. This will improve and enhance the ways GMP is able to deliver information into the hands of our stakeholders and customers, allowing them to have the critical information they need, when they need it, and with greater detail. Timely and accurate information is vitally important during severe weather events, and is especially critical for safety, as we continue to see an increase in storms due to climate change.

---

[1] Our Outage Management System refers to the software system that records and aggregates residential and circuit-level outages and is used by us to help manage and prioritize the restoration of service to our customers.

[2] SCADA is used by system operators to operate remotely-located devices, open and close circuits, and otherwise manage and receive telemetry from the grid.

[3] We use GIS for mapping the latitudinal and longitudinal coordinates of poles, transformers, substation equipment, meters, and other grid assets, which helps customers because in the event of an outage, we can quickly ascertain the location of the outage as well as the potential source of the outage, which facilitates faster overall service restoration.

Q9. How do these projects differ in terms of selection criteria and prioritization, compared to typical IT planning that you undertake every year as a part of GMP's Multi-Year Regulation Plan ("Regulation Plan")?

A9. Typically, GMP's IT capital project selection process is based upon upkeep and upgrades—responding to changes in enterprise technologies or business processes, assessing the impacts of those changes, and determining how those enhancements and improvements could be implemented to provide improvements in the cost-effectiveness and quality of service for our customers, reduce operating costs, improve business processes for efficiency, or provide better functionality to enhance and improve the customer experience. These projects are also often initiated in order to upgrade systems and applications that have reached the end of their supportable and useful life, or that must be replaced in order to provide more contemporary or compatible technologies or functionality.

In the face of climate change, business as usual will no longer work. So, under the CP, recommended IT projects are focused on providing better levels of redundancy and resiliency to key operational systems that can, in their current configuration, more easily succumb to the impacts associated with extreme weather-related events, or the durability and availability of which would be critical to customer restorations during extreme events. As an example, a CP project could be undertaken to make sure that portions of the GIS system can be extended in a resilient way to the cloud, so that during an interruption in IT availability during a severe outage situation, critical premise and other data could continue to be provided to the outage management system to help line crews manage and restore customer outages. This targeted project planning goes beyond the upkeep and upgrading we typically undertake to proactively harden technology systems to withstand physical damage from storms.

Q10. How does GMP propose to improve and enhance the availability and durability of its critical operations and communications networks?

A10. Presently, GMP uses a combination of leased, wireless, company-owned, and VELCO-owned communications infrastructures to provide transport and control capabilities between GMP facilities; grid devices (for example, intelligent devices that are used to control distributed energy resources or sectionalize portions of the grid to back-feed customer power in the event of an outage, devices that control water flow at hydroelectric stations, or devices that deactivate lines in the event of a car/pole accident to ensure safety and protect lives); radio systems used by field crews to communicate; and data centers (the physical facilities in which GMP's servers, data networking, and storage devices are located). These networks, along with their underlying switching and routing components, have been significantly enhanced in recent years to provide more efficient execution of daily operational tasks but have not been specifically designed to handle the types and potential severity of interruptions that we expect to experience as a result of more climate-driven severe weather events where storms are more severe and last longer. Additional work—beyond business as usual—is needed to ensure the ongoing operation of these systems in the event that partial or entire portions of the network and/or their backend systems are interrupted. By taking proactive steps to bolster application and communication redundancy, it will be possible during severe events to maintain a high level of visibility into our grid, our generating plants, and our meter-mesh network (meaning our communications with our customer's premises), as well as ensure that the communication systems and applications used by control center, field, and office employees remain useful and viable for restoration management activities. This is key to being able to continue to operate safely and effectively during outage restoration efforts, provide information and services to customers, and continue operating our generating facilities.

To this end, in order to facilitate the ongoing ability to better secure our minimally-viable restoration services during a significant outage event, and without interruption, we are recommending a number of system-wide resiliency improvements, which are outlined in **Exhibit GMP-MD-1**. To accomplish these important improvements, we are recommending enhancements to wireless communications, cellular services, radio systems, fiber optic networks, SCADA control systems, and outage management applications. In each of these areas, it is our belief that creating levels of failover redundancy, in conjunction with developing the ability to operate key systems from geographically dispersed locations throughout the state, provides the best opportunity to avoid interruptions in functionality in the first place, while at the same time ensuring assessment and triage activities could be conducted even in the event of a loss of a portion of the system or its controls.

Q11. Can you define some of the terms you just used to provide a better understanding of the projects you expect to pursue?

A11. Yes. Minimal-viability is a term of art in my profession meaning the minimum level of functionality a system or application requires or should be preserved in order to operate. For GMP, it means the level of operation needed to serve our customers effectively.

Failover is another term of art that refers to a backup system that takes over when the primary system is offline. A minimally-viable failover system is one that would contain the basic functions necessary to meet customer needs in the event a primary system went offline. In other words, the failover system would not have every bell and whistle contained in the primary system that aids normal operations, but instead would have the minimum capabilities required to serve customers.

We can use another technical phrase—outage management system—to provide an example. An outage management system, holistically, is the combination of functions and applications that allow GMP to have visibility into outages when they occur and then manage and coordinate restoration efforts among field personnel and the control center. GMP's outage management system includes visibility to the state of AMI meters at our customers' premises; our circuits, transformers, and generating equipment; and the database utilized by our field and control center personnel to track outages and restorations. A minimally-viable failover for the outage management system would include the capability to maintain telemetry on the state of transmission, distribution, and generation devices, as well as customer meters and other devices situated on the AMI network, including gatekeepers (the devices that meters speak to) and repeaters (devices that boost messages from meters back to the gatekeepers from very remote locations). It would not have to incorporate more advanced elements of our primary system, such as remote-disconnect or the processing of register reads for billing, in order to continue to serve our needs and customers' during periods of extreme weather if our primary system were knocked offline.

Q12. What other projects do you expect to include in your work based upon this Plan?

A12. There are a number of projects that I expect to develop and implement over time in response to our resiliency planning. These include:

- Establishing carrier-redundancy for internet services in order to provide the best opportunity to maintain internal, external, and other critical communication paths during a severe event (including call center and control room-specific telephone, pre-recorded information through IVR, live web chat, and cloud-based communications tools);
- Adding satellite phones at key locations so GMP teams can continue to communicate as a last resort pathway to ensure and guarantee emergency communications capabilities in the event of a total loss of carrier, radio, or internet-based communications facilities;
- Establishing cellular backup functionality for key grid-side and SCADA devices, so that control and operation may be maintained in the face of the loss of VELCO or carrier networks (this may include adding GMP-installed fiber and communications devices);

- Upgrading Remote Terminal Unit ("RTU") devices located at substations and plants so that grid devices may be managed from either of GMP's two main control centers or another GMP facility. This is important because, at this time, neither GMP control room can fully control the grid assets that are directly connected to the other (or opposite) control room. Replacing these devices, which are largely analog and of 1980's vintage, will allow full "digital" control of grid assets from either control room location, which adds resiliency to both our grid operations as well as the location of our workforce for performing such functions;
- Extending and creating multiple path redundancy options for optical fiber to key substations and plants to elevate the likelihood of surviving a fiber cut; and
- Developing IP-based radio solutions as a failover mechanism in the event of radio system loss.

Focusing on layering multiple communication backup methodologies is critical throughout all of this work because the sources, dispersion, and severity of catastrophic communications losses anticipated as a result of climate change will likely force GMP operations personnel to need the capability to operate from alternate locations and via best available communications paths in order to continue to deliver service to customers. Ensuring that there are multiple paths and varied methods of doing this, that can survive a range of weather outcomes while permitting personnel to easily access data and control systems, is critical to system durability and restoration efforts.

Q13. How might these capabilities also help the communities our customers live in?

A13. Mr. Otley and Mr. Castonguay comment on this in more detail. For my part, I note that as GMP enhances its own communications and backup capabilities through the use of fiber installations and wireless devices, there is also the possibility of helping communities with subpar communications systems. Our field crew has the most difficulty communicating with each other and with our control center in the places where Vermont's broadband system is weakest. As we look at our resiliency zone work and consider ways in which GMP can help advance the state's broadband goals cost-effectively, we expect that the projects we undertake to enhance IT and communications under the Plan may be useful not only to GMP's own systems and crews but also to our customers, first responders, and the communities in which we operate where broadband access and coverage are lacking.

Q14. What new types of application and/or data center redundancies are you proposing to be included as part of the Climate Plan proposal?

A14. All key GMP operational and storm applications and data sources presently used by GMP to monitor and manage the grid and provide restoration services are currently housed in one of two physical data centers located within the State. Preparing for the impacts of climate-driven weather events mandates that a number of these critical systems be identified, developed, and tested to operate on an as-needed basis from the cloud, using the functionalities and potential services of a virtualized data center, in the event that these locations, or the communications networks between them, are lost. Developing this type of redundancy helps customers because it ensures that the loss of one or both physical data centers, or control rooms, would not result in a complete loss of communication and management of the system. Customer outages and restoration activities could still be undertaken (albeit with a reduced set of functionality, as described above) without having to resort to manual processes that, given the ongoing digitization of the grid and metering infrastructures during the last decade, would prove difficult to manage if not outright ineffective.

Q15. Why do you believe cloud-based services are a critical need to provide backup to physical locations to best serve customers?

A15. We will serve our customers better if we have the ability to temporarily provide basic assessment, control, restoration, and communication capabilities from the cloud, while also being able to access customer data and services, independent from GMP's physical locations, which could be cut off or damaged during a severe event. The last resort for operating our restoration efforts under catastrophic conditions is to revert back to fully manual procedures, and we recognize that in this day and age that is very unlikely to be adequate or effective. While we would be able to continue our restoration efforts while in this mode, the efficiency and effectiveness of our operations would be significantly compromised and our restoration efforts will take longer which negatively impacts our customers. The customer impacts and tradeoffs of not creating this type of failover resiliency is concerning, which is why establishing these basic systems for virtual operation offers the best and least expensive approach to ensuring the continuity of customer services during severe weather impacts.

The location of physical servers and applications becomes less critical when cloud services can be leveraged on an as-needed basis and deactivated when no longer required. That said, GMP will need to maintain some basic readiness capabilities including VPNs, firewalls, authentication mechanisms, data replication tools, and other services on an ongoing basis, and will continue to need to test those systems regularly to ensure their availability during an event. These emergency systems would be separately hosted from GMP's non-emergency systems served in the cloud, but would likely share common data sources and network connectivity methods as needed.

Q16. Can you describe the IT projects intended to further coordinate restoration efforts with Vermont municipalities, first responder personnel, and customers as part of the CP?

A16. Right now, as described in Mr. Otley's testimony, it is GMP's model to proactively disseminate information during restoration events in many ways, including customer email lists, text alerts, traditional media, social media where we engage directly with customers, and customer outreach via telephone to communicate about critical storm, safety, and restoration work. This approach has served customers well, but we need to do more work to harden this area of our operations because during a very serious incident or storm, some of these services could be lost or impacted. We know that customers appreciate and consider our communication around storms to be key. We believe that to proactively make sure there is no interruption in this critical information flow we need to create a web-based storm platform—a one-stop location for stakeholders and customers to learn about storm preparedness, register for and receive updates about their location and communities, and communicate directly with GMP staff during events.

We also propose to improve our capabilities to provide communication to key, non-customer stakeholders such as first responders, state and municipal government leaders, and media, among others. Our proposal is to work over the next three years to investigate and design a way to create either an additional level within the GMP website or a separate site that is specifically designed to provide information to first responders, municipalities, contract crews, regulators, elected officials, and others—much like what is done with the statewide outage website, vtoutages.com, now—which, as part of this initiative, could also potentially be rolled into this storm platform. We have heard from other utilities and state partners how helpful it would be to have available additional layers of data during these events. Our vision is to create a one-stop destination to be in contact with key GMP storm managers and external stakeholders who can receive an extra level of information regarding restoration activities. Our thinking is that many of these functions, like outage and restoration alerting to customers, could be automated, and that additional levels of detail within outage maps, regarding estimation of restoration times, deployment of crews, critical customer and commercial customer details, etc., could be accessed through the portal. Our investigation will include the best way to fund the project—through GMP contribution, and potentially other funding sources such as grants, if there are other partners beyond our customers who would benefit from the work.

We also plan to pursue a separate project to help with getting important information to our crews, especially about severe storm damage, through an app that would allow customers, first responders, and others to photograph and geolocate the source of broken poles, downed wires, and other events, in order to not only help crews get a quicker understanding of what is happening on the ground but also to assist in the prioritization of response and the right combination of crews and gear to provide restoration. This immediate aggregation of critical damage in this time of increased frequency and severity of storms will help customers through better storm response and is the technological step that we feel must be made to keep pace with technology and respond to what customers expect for communication tools.

II. Criteria and Preliminary Project List

Q17. What criteria will you employ to determine where to utilize these technologies?

A17. The criteria we will use to select which technologies and services to deploy in support of the CP will be determined by identifying which assessment, recovery, and information assets *must* be accessible during severe events in order for triage activities to take place in the event of a total loss of one or more of GMP's existing data centers, control centers, network operation centers, field assets, or key services (for example, Interactive Voice Response services, which manage inbound call routing based on the caller's selection of options).

Project selection for these failover systems will be based upon the ability to provide enhanced levels of redundancy and resiliency to key operational systems that might either more easily succumb to the impacts associated with extreme weather-related events in their current configuration, or the system's durability and availability would be critical to customer restorations during extreme events.

For communications projects, selection will be based upon the ability to provide additional platform capabilities for stakeholder/emergency response information and resource sharing with GMP, or to create more segmented/targeted customer communication during extreme events.

Q18. Do you have a list of IT and communication projects specifically planned for the first year if the CP is approved?

A18. Yes, we have a preliminary list of these projects. It is attached as **Exhibit GMP-MD-1**. We developed this list utilizing the criteria I discussed above. The list itself outlines a number of exploratory projects in year one to determine the efficacy and feasibility of the initiatives proposed, and then productionalizing and testing those services and infrastructures in the following years. Our goal would be to have a functional, out-of-band recovery and service infrastructure (meaning these systems can be utilized and operated without being dependent on GMP's data centers) in place by year three of the plan with key capabilities feathered in along the way. In the first year, discovery and architecture decisions will need to be made to determine the efficacy and practicality of operating critical systems remotely and in the cloud. In the second year, emphasis would be placed on the programming, development, networking, and security work required to ensure the functionality desired. Most, if not all, of GMP's primary storm management, control, and communications applications are deeply interconnected, relying on an amalgamation of middleware and Application Programming Interfaces ("APIs") to operate and share information between them. These systems would need to continue to talk to each other in a disaster scenario, requiring a method to duplicate them in the cloud and keep them refreshed, so that in the event we "cut over," the data and connectivity between applications would be consistent and reflective of the production environments in our data centers at the time of system loss.

At this time, costs for additional circuits, cloud-based services, and infrastructures are presented as estimates while discovery and then architectures are contemplated. Where possible, more detailed costs have been included in **Exhibit GMP-MD-1**. Generally, we expect development and provisioning costs to be similar or identical to services that are presently part of the production network and application environment at GMP. As always, technology costs change quickly and we will always pursue the best technologies and price points updated at the time we are ready to execute on these projects.

Q19. Are all of these capital projects? If not, how are you proposing to treat them from an accounting point of view?

A19. They are not all capital projects, though much of the Remote Terminal and other equipment identified for projects in the initial years of Plan implementation are capital costs. While we firmly believe that cloud-based subscription IT systems should be treated as capital going forward (as we proposed in the Regulation Plan proceeding, Case No. 18-1633-PET, and as endorsed by NARUC), we understand that the Regulation Plan did not in the end adopt that approach. Therefore, any such project would include operations expenses, in addition to capital, if there is equipment involved. Mr. Ryan explains how we expect to track those expenditures and separate them from the O&M platform under which we will operate until 2023.

Q20. Do you have already a list of future projects beyond the first year for IT and communications that fit within the CP?

A20. We do have a partial list beyond year one. Unlike the T&D and generation projects described by other witnesses, these areas of technology change very quickly and so we believe it is important to remain flexible as we work to improve systems and deploy solutions to better respond to severe storms. As a part of the annual planning process, we will consider what projects are within our normal, baseline planning and separately consider resiliency-related capital or operations expenses in the IT and communications areas that fit with the criteria we have laid out above and the workflow needs of GMP, after the scoping work we complete in the initial period. The normal IT capital process is predominantly focused on business enterprise systems and moves at a pace that is typically slower to be developed and completed, due primarily to the complexity of integrating multiple systems that are integrated with complex business processes. For example, implementing a replacement or upgraded Enterprise Resource System ("ERP") requires significant amounts of data cleanup, programming to connect systems together, testing to ensure billing accuracy, etc. While some resiliency projects also require this level of system integration, others—like upgrading Remote Terminals or adding solar panels to gatekeepers so that meter visibility and telemetry is maintained during a power loss—can happen much more quickly as they are more construction oriented in their nature, or can be outsourced.

Q21. Have you already experienced IT or communications impacts due to severe weather?

A21. Yes. Because our communications infrastructure often shares the same poles and rights of way as our distribution and transmission networks, when those portions of the infrastructure are damaged by weather, it is not uncommon that communications services are temporarily lost or damaged too. For example, during several major storms (Irene, Sandy, and several more minor wind storms) the loss of poles and wires has led to interruptions in communications as well. In instances where GMP offices, substations, generating facilities, etc., are fed by only one communications circuit, it has resulted in a loss of telemetry and control for extended periods of time (hours to days) while GMP crews and telecom providers reconstruct and repair those sections of infrastructure. In these cases, individuals must be dispatched to operate facilities manually.

Q22. Why does GMP believe it is important for customers to pursue these IT and communications projects in the near term as a part of its climate response, rather than simply including them at some point down the road in its normal capital and operational planning?

A22. The accelerating pace of weather events due to climate change have highlighted potential capacity and durability concerns that this Plan aims to address proactively, specifically within the suite of GMP storm applications and control centers, as well as the sustainability of gatekeepers and other devices located on the AMI network (which, when power is lost, have only a 24-hour or so battery life). The rise of more diverse outage types for longer durations has, as noted above, led at times to the temporary loss of important telemetry and communications systems, and has demonstrated the need to harden these systems so that they are decentralized; have alternate communications or power sources attached to them (like adding a solar panel to keep a gatekeeper device alive); and are able to be activated and operated from locations that are not impacted by outages. The loss of communications circuits, in particular, has underscored the need to provide redundant pathways for internal and external communications for the control of grid-side equipment that is not already served by diverse routes. Having a separate, focused Plan under which these redundancies can be implemented will allow for much quicker and focused implementation.

Taken separately, GMP's storm and outage response systems are unique in their architecture, but lend themselves, in most cases, to being moved to the cloud or an alternate hosting location. A compelling reason to do so proactively ourselves, as a part of the Plan, is that GMP's software vendors are lagging behind by several years. That means that if we want to develop the level of resiliency we desire, especially for customer-facing systems, it will be necessary to construct much of this functionality ourselves. The logic, data, and methods of building and managing these systems is already well understood by us, and would not have to be reengineered. This will allow for a much quicker stand-up of minimally-viable failover systems that can be utilized in the event of a catastrophic event to provide service to customers.

For the customer, the pursuit of these CP projects means that, over time, the loss of any one individual system or circuit can be worked around by bringing up a backup infrastructure immediately, and as a result, contributes to shorter duration outages, better methods of communicating the nature and status of those outages, and the ability for internal GMP operations personnel to maintain communications and control during an event.

Q23. Does this conclude your testimony at this time?

A23. Yes, it does.