STATE OF VERMONT
PUBLIC UTILITY COMMISSION

Petition of Green Mountain Power Corporation for approval of its new Multi-Year Regulation Plan pursuant to 30 V.S.A. Sections 209, 218, and 218d	)))	Case No. 21-____-PET

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

September 1, 2021

Summary of Testimony

Mr. Dincecco's testimony explains how Information Technology and Cybersecurity will require significant focus and investment for the benefit of customers in the years ahead, and how the next Multi-Year Regulation Plan will provide flexibility to address these investments in the context of rapidly evolving regulations and risk.

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

I. Introduction

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

A1. My name is Mark Dincecco. I am employed by Green Mountain Power ("GMP") as 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 ("IT") and Operations Technology ("OT") 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. Yes, I provided prefiled testimony in GMP's Climate Plan proceeding, Case No. 20-0276-PET, regarding climate resiliency IT investments.

Q4. Can you provide a summary of your testimony in this case?

A4. My testimony provides context on the rapid changes we are seeing in the technology and cybersecurity fields and the continuing critical importance of these areas for GMP and our customers. I explain the provisions within our next Multi-Year Regulation Plan (the

"New Plan") that allow GMP to focus investments in this area for the benefit of our customers while retaining flexibility to adapt to uncertainty over the New Plan period.

Safety is at the core of everything we do at GMP, and that extends into our approach for managing and adapting our technology to ensure we remain well prepared to guard against both natural risks and those from cyber-attacks. The national news has reported at length on breaches at Colonial Pipeline and SolarWinds, among other catastrophic cyber-attacks outside of the utility sphere that have recently occurred. Just last year in Vermont, the UVM Medical Center's IT systems experienced a very disruptive ransomware attack. These incidents illustrate the changes in the global threat landscape and were front of mind as GMP developed this New Plan. They are also front of mind for many regulators and lawmakers, as additional regulatory and industry standards likely will be forthcoming.

While we continue to evaluate the emerging risks posed by cyber criminals and nation-state actors, we are also continuing to transform our technology and communications infrastructures to both meet these challenges and provide more secure and resilient services to our customers. For example, OT and IT, traditionally two separate areas of utility investment, have converged to provide efficiencies in computing, storage, security, and networking infrastructures and to leverage the use of IT staff to provide support across all technology stacks.

At the same time, our ability to ensure reliable and resilient service needs to evolve due to the proliferation of connected and automated devices, whether located on the grid itself, or in the form of Internet of Things devices deployed within our

customer's homes and businesses. This is also true for the many Distributed Energy Resources ("DERs") being deployed to further enhance the resiliency and responsiveness of the grid while leveraging renewable generation and other customer services. Like many other technologies, DERs require secure connectivity and the orchestration of hundreds or thousands of assets and the movement of data into and across our system. As I discuss, the scale of our IT deployment in supporting these innovative and resilient services is necessarily and closely correlated with our cybersecurity profile.

To manage this important transition and to enhance failsafe redundancy of mission-critical applications—and seek more secure IT solutions—we are continuing to migrate many of our IT services to virtual, cloud-based solutions. Leveraging these cloud platforms will be an important strategy for accomplishing the goals listed above, and for maintaining a digital network that can weather storms, both real and cyber, and thus provide both reliable electric service and secure customer-facing services.

My testimony provides further detail on GMP's current IT, OT, and cybersecurity practices and touches on the potential for evolving risks and important work we are doing and want to do in this area. I also briefly discuss GMP's implementation of cloud-based services.

Q5. How does the work your team performs for operational reliability relate to cybersecurity work?

A5. When planning and maintaining our IT and OT systems, we focus on guarding against natural and human-made risks. Natural risks, most frequently in the form of wind, snow, or ice-bearing storms increasingly driven by climate change, are an ongoing challenge.

These events routinely take infrastructure out of service and require well-designed systems that can help detect and mitigate outages and restore service faster. In this New Plan, GMP will continue to incorporate resiliency planning into the capital planning philosophy of all departments, particularly in our Transmission and Distribution ("T&D") and IT Departments. *See* **Exhibit GMP-MB-1**. Our IT and OT teams will continue to support a technology infrastructure increasingly designed around resiliency by implementing remote and automated hardware and software systems such as motor-operated air brakes, transfer-trip devices, and self-healing circuits that can detect and isolate faulted line sections within seconds and re-energize much of the circuit from available feeder backups. From an operational perspective, our primary goal is to enable secure, remote access and telemetry to control these devices should centralized operations be unavailable during an emergency. This is more important than ever before as our customers electrify and decarbonize their transportation and heating.

As we implement and expand these new connected hardware and software solutions, we also need to ensure that they are inherently secure to minimize or eliminate cyber risk to our systems and to protect operational and customer data. We are no longer just an electric utility. We are now, in essence, a technology company. We use technology to enhance and expand upon traditional utility services—and offer new services such as battery backup and load management, among others. As a result, an increasing number of our applications and hardware devices connect to and interface with technology solutions to better harden and manage them for customers. This increases our need to guard against the threat of cyberattacks that could impact any aspect of our

system by exploiting faults inherently present in Internet Protocol-based ("IP") infrastructure. While good security and monitoring is needed to help prevent that, they are not a guarantee given the constantly evolving tactics that are being used by bad actors, including the elevated risks posed by nation-state actors made apparent by recent national events.

It is important to understand that GMP has many strategies in place at this time to combat such attacks, and that work must and will continue one way or the other. In fact, this work needs to deepen, and likely will have to expand, as we learn the lessons from recent energy sector cyberattacks and work with federal regulators on evolving requirements. Recent testimony by the Federal Energy Regulatory Commission ("FERC") in front of Congress and the President's recent Executive Order on cybersecurity make clear that there will be a heightened focus on the need for further cybersecurity protections for all infrastructure, including energy. We also know that there is an opportunity for coordinated and planned investment and system design that can achieve several goals during this period of shifting risks. For example, remote operation and SCADA control upgrades should be designed to achieve OT operational support and connectivity goals while also addressing cybersecurity risks and enhancing resiliency, whether it is a storm or a cyberattack that is disrupting service. Because it will take time to develop a full suite of failover capabilities while maintaining our current cybersecurity posture, these goals should be aligned as much as possible.

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 our information infrastructure to protect 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 and endpoint security software, encryption tools, and the use of "air-gapping," 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 as well as adherence to established cybersecurity frameworks such as the SANS Institute's Center for Internet Security ("CIS") Top 20 CIS Controls. Those provide a framework that prioritizes cybersecurity risk mitigation activities based on best practices. As an additional measure, GMP provides online cybersecurity training to all of our employees monthly to raise awareness of cyber threats, and in turn, heighten the human capacity of employees to be on the watch for potential threats or unusual behavior. The safety culture at GMP includes not only physical and mental wellness, but also, importantly, includes cyber safety.

Q7. Philosophically, how does your approach to cybersecurity inform the way you look at the investments that should be made during the New Plan?

A7. GMP's management of our 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. This resilient, "Zero Trust" philosophy supports and meshes with our best practices and defense mechanisms that seek to protect our systems at the initial point of attack and again if a successful attack is trying to move laterally between our systems. At its heart, our approach is again focused on resiliency: 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 therefore not result in a cascading loss of the entire system itself. It is critical and prudent to develop this synergistic relationship between cyber prevention and recovery methodologies too because it ensures that GMP's operations remain resilient during potential attacks and that redundancies in key cybersecurity and communications systems continue to provide protection from future attacks. As I testified in GMP's Climate Plan proceeding, this approach also offers protection against the possibility that a bad actor could take advantage of a natural disaster to launch an opportunistic attack.

Q8. How does the New Plan support these cybersecurity investments?

A8. Unlike many of our traditional areas of investment such as T&D, generation, and fleet, IT technologies and their inherent risks change very quickly, so we believe it is important to remain flexible as we work to improve systems and deploy solutions to better harden our systems and protect our customers. At the same time, the business-as-usual IT capital process can move at a slow pace and often requires overly prolonged development of business enterprise systems that integrate multiple systems that are tied into 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, and testing to ensure billing accuracy, etc. This "normal" IT process remains within or annual planning process and is included in base capital (and base O&M, as appropriate). As a part of our annual planning process, we will consider what projects are capable of advancement and that address our present cybersecurity and resiliency needs in a targeted and coordinated manner.

We also recognize that even for this fast-evolving field, the upcoming New Plan period could be marked by particularly rapid change. At the time of this filing, the U.S. Congress is holding hearings on several bills relating to utility cybersecurity, and FERC and the North American Electric Reliability Corporation continue to evaluate applicable orders and standards. Throughout, technology will continue to develop and new solutions or thinking may emerge. Indeed, we may find the need to innovate or develop GMP-specific solutions to address cyber risks even in the absence of regulatory guidance. As much remains uncertain—and because we cannot yet know how to prepare for all future contingencies—the New Plan provides additional flexibility to seek a new "Cybersecurity Plan" if needed during the term of the New Plan.

The Cybersecurity Plan would be filed in the event that additional investments for the benefit of system security and our customers were required during the New Plan. If presented to the Commission, it would be subject to Commission approval, must support investments that would be in the best interests of customers, and would provide the opportunity to set the best regulatory and accounting treatment for such projects. Rather than anticipating specific additional projects and costs at the outset of the New Plan when

the cybersecurity landscape is rapidly evolving, the ability to file a Cybersecurity Plan if needed would provide flexibility by allowing us to respond to the evolving regulatory and technological landscape best for customers.

Q9. Can you elaborate on GMP's use of cloud-based services for its IT needs?

A9. Cloud-based services are utilized for two general goals. The first has been discussed in this testimony and involves the creation of cloud-based redundancies for our key operational systems. Much of this is innovative and evolving, and we will have to develop the right solutions ourselves for GMP's specific needs and customers. We believe that we will serve our customers better if we have the ability to temporarily provide basic telemetry, 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, including a network-compromising cyberattack.

The second goal is broader, and may be able to support the first goal once implemented. It involves the migration, where feasible, of services from GMP servers and datacenters to cloud-based platforms. As we are increasingly becoming a connected, technology-driven company, IT for GMP—as for other utilities and contemporary businesses—is no longer a back-office support function, but instead is at the core of many of our critical utility functions. This is especially true as we integrate DER management and customer-facing communication services that require greater contributions from GMP's application, network, and IT assets. For services with an

available and prudent cloud solution, redundancy, remote access, and cybersecurity support are additional benefits of this approach.

Q10. Are there any new concerns created by implementing cloud-based systems, particularly in terms of cybersecurity and additional points of entry into GMP's system?

A10. While no significant additional concerns are anticipated by moving applications to a cloud-based site, it is important to recognize that cloud systems, like any technology system, remain fallible. While the nature of the cloud architecture provides resiliency benefits over premise-based solutions, a cloud computing system is still a combination of hardware, software, and communications functions. The same governance and audit frameworks one would apply to a premises-based technology solution must be applied in the cloud as well to ensure system and data availability and integrity.

Many businesses and utilities, including GMP, already utilize cloud-based services for existing production applications, and the same methods of best practice applied to securing user access, production changes, system isolation, physical security, and the like in our Vermont-based data centers are applied to applications developed within, or hosted in the cloud. GMP's policy is to utilize only secure, encrypted communications for these types of solutions, where any data in transit or at rest is encrypted over private networks. Moreover, GMP anticipates that for the time being, while the technology matures, the cloud-based resilient-hosting of our outage management applications and communications platforms will be on an as-needed basis,

typically used only in the event of a severe weather event or during the potential loss of capabilities in one or more of our physical data centers.

Q11. Are these cloud-based investments capital projects?

A11. As with our traditional datacenter-centric IT infrastructure, some aspects of cloud computing should be considered capital investments while other aspects involve operating expenses. We firmly believe that cloud-based subscription IT systems should be treated as capital going forward, as we proposed in the Multi-Year Regulation Plan proceeding, Case No. 18-1633-PET, and as endorsed by the National Association of Regulatory Utility Commissioners and several jurisdictions to reflect a modern understanding of the role these systems play in replacing traditional capital assets and better serving customers. To that end, we have adopted the 2018 Financial Accounting Standards Board's ("FASB") accounting changes that treat "implementation" costs of acquiring cloud-based service agreements as a capital investment, while ongoing service fees and other operating expenses remain expensed.[1] This approach aligns the treatment and incentive of these cloud service agreements to reflect current technology and business practices and ensures GMP is making prudent IT investments for our customers.

[1] FASB, *Accounting Standards Update 2018-15, Intangibles—Goodwill and Other—Internal-Use Software (Subtopic 350-40), Customer Accounting for Implementation Costs Incurred in a Cloud Computing Arrangement that is a Service Contract* (August 2018), available at https://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1176171138858.

Q12. How do enhanced capabilities and focus on cybersecurity also help GMP customers directly?

A12. In addition to supporting our overall system resiliency, enhancing our cybersecurity capabilities would have several direct benefits for our customers. Many of our customers are connecting some form of DER to the grid, such as controllable heat pumps, EV chargers, or residential battery systems, and we certainly hope and expect the number of connected DER resources to expand during the New Plan and into the future. Improving the security of this connected equipment and their connection to our systems—including logically and physically separating DER management systems from other IT/OT systems to minimize the propagation of an attack—improves the reliability and functioning of these devices for customers, including during emergencies, and provides protection of the customers' own systems and data, which may also be connected to the DER in some fashion.

The security of our own IT systems is also critical to our customers because we store and safeguard personally identifiable customer information and provide e-billing and account management services via our online customer portals. We take the safety of this information and these interactions very seriously and ensure that we are following all applicable requirements and guidance. Our cyber capabilities must continue to ensure the safety of customer information and our systems.

Q13. Are there other considerations regarding IT spending you believe the Commission should be aware of?

A13. As Mr. McDonnell and Mr. Nelson of Strategen state in their testimony, the FASB's updated Generally Accepted Accounting Principles, which allow partial capitalization of these cloud services, is a step in the right direction, and one GMP has already started to implement, but it does not go far enough to reflect the role that cloud computing services have inherited from traditional IT hardware. Their expert opinion emphasizes that it is important to consider the balance between capital expenditures ("CAPEX") and operational expenses ("OPEX") to align regulatory treatment to support options that present lower cost and higher value for customers. They provide, as an example, the concern with cloud computing I presented above—that cloud services often replace traditional servers and wires CAPEX approaches, but are still viewed as an OPEX solution. This area is quickly evolving past the traditional utility concept, and modern regulation allows for an opportunity to correct this misaligned framework.

This CAPEX/OPEX parity issue could be addressed through additional authorizations for capitalization of cloud services—for instance, following the New York Public Service Commission's approach described in Mr. McDonnell's and Mr. Nelson's testimony. Another approach could be considered through the implementation of our proposed Cybersecurity Plan, where, similar to the Climate Plan authorized during the Current Plan, GMP could make upfront capital and capitalized investments to ensure we are best equipped to manage cyber risks for our customers going forward. Like the Climate Plan, these potential investments respond to a new, evolving threat environment

and are likely to provide significant value over their lifetime as opposed to implementing slowly in a business-as-usual scenario, which may have been appropriate where risks were changing more slowly. While such a framework or investment would be evaluated in any proposed Cybersecurity Plan, I believe these concepts are important to keep in mind as context for our request.

Q14. Does this conclude your testimony at this time?

A14. Yes, it does.