STATE OF VERMONT
PUBLIC UTILITY COMMISSION

Tariff filing of Green Mountain Power Corporation requesting a change in rates, effective October 1, 2022	)))	Case No. 21-____-TF
Petition of Green Mountain Power for approval of its new multi-year regulation plan pursuant to 30 V.S.A. §§ 209, 218, and 218d	)))	Case No. 21-3707-PET

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

January 18, 2022

Summary of Testimony

Mr. Dincecco presents Green Mountain Power's ("GMP") Information Technology ("IT") capital investments included in this rate filing. In support of this filing, Mr. Dincecco describes the overall cybersecurity and IT operating environment and the critical role of IT at GMP, as well as GMP's request for new regulatory treatment of IT capital projects to enable flexible and responsive IT work. Mr. Dincecco also describes how the IT Team assisted the development of cost forecasts for the following three years of GMP's proposed new regulation plan ("New Plan").

Exhibit List

Exhibit GMP-MD-1   IT Capital Planning Framework
Exhibit GMP-MD-2   IT Five-Year Average Budget
Exhibit GMP-MD-3   IT Capital Additions (2022–2023)

TABLE OF CONTENTS

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

I.   Introduction

1   **Q1.   Please state your name and occupation.**

2   A1.   My name is Mark Dincecco. I am employed by GMP as Chief Technology Executive.

3   **Q2.   Please describe your educational and business background.**

4   A2.   I have been employed by GMP since 2010 as the leader of the company's IT and

5   operations technology ("OT") functions. I have previously worked as a technology and

6   IT security executive at Burton Snowboards, Ben & Jerry's Homemade, Inc., and the

7   United States Environmental Protection Agency. I graduated from Norwich University in

8   2004 with a Master's of Science in Information Security.

9   **Q3.   Have you previously testified before the Public Utility Commission ("PUC" or the**

10   **"Commission")?**

11 A3.   Yes. I provided prefiled testimony in GMP's Climate Plan proceeding, Case No. 20-

12   0276-PET, regarding climate resiliency IT investments, and direct prefiled testimony in

13   the new regulation plan proceeding, Case No. 21-3707-PET (the "New Plan").

14 **Q4.   What is the purpose of your testimony?**

15 A4.   My testimony serves two roles. First, in support of GMP's traditional rate case filing for

16   Fiscal Year 2023 ("FY23," beginning October 1, 2022), I summarize IT's level of capital

17   investment and operation and maintence ("O&M") expense expected during the rate year,

18   explain how we arrived at those figures, and introduce our exhibits submitted in support

1   of the rate case. As a part of that, I summarize the IT and cybersecurity environment

2   GMP operates in, and I describe GMP's request for a new regulatory treatment of IT

3   capital investments—allowing an overall IT Budget for anticipated spending needs,

4   including specifically identified projects and the IT blanket, all in line with baseline

5   spending in recent years—to operate effectively in this current environment and best

6   serve customers. My rate case testimony is contained within Sections II (overview) and

7   III (rate year capital investments).

8   Second, in support of our proposed New Plan, I discuss how GMP developed

9   forecasts for IT capital investments and O&M spending during the remainder of the New

10   Plan's term (FY24–26). These forecasted amounts will help establish the initial rate path

11   over the course of the New Plan and are covered in Section IV.

II.   IT Overview and Context

12   **Q5.   At a high level, can you describe the role of GMP's IT Team?**

13   A5.   The role of GMP's IT Team is expanding at pace with the rapid development of

14   technology-based solutions and systems in the energy sector. In prior decades, we

15   supported business operations as a back-office function. Today, in addition to our

16   business support role, the IT Team helps develop and manage technology-based solutions

17   that empower all areas of GMP's operations and increasingly comprise more of the

18   customer experience. In recent years, we have observed a convergence of the traditional

19   functions of IT, OT, cybersecurity, and energy services, that have resulted in our

20   transition to an even more technology-based company.

1   For example, IT work is significantly embedded in our efforts to transform the

2   grid and electrify everyday activities through controlled distributed energy resources

3   ("DERs"). These resources—now expanding across the grid to help cut carbon and costs

4   and boost resiliency—require a communication and coordination infrastructure to

5   maximize the available system benefits (such as real-time peak shaving from storage

6   resources) for customers. In addition to building grid resiliency through support of

7   DERs, IT improvements can directly advance resiliency objectives, including by creating

8   failover redundancy for critical systems and enhancing communication systems during

9   disruptive events for GMP crews, first responders, and customers. These types of

10   resiliency initiatives will carry forward into the New Plan, as we continue to harden the

11   critical infrastructure that supports all our operations.

12   Customer support and communication is another area where the IT Team is

13   involved. We help develop the billing and self-service portals that allow customers to

14   closely track and engage with their use of electricity, and particularly to improve

15   communication and tracking of service quality and outages. We have worked hard

16   recently along with the customer care team to develop these capabilities and increase the

17   methods for customers to engage with GMP and get the information and resources they

18   need when they need it.

19   As I described in my direct testimony on the New Plan, the expanding role of

20   technology in GMP's operations must be accompanied by an equal focus on security.

21   Our grid is comprised of an increasing number of connected and automated devices, from

22   OT infrastructure on our own systems, down to DERs and customer-controlled smart

1   appliances on customer systems. While we practice isolation and other methods to

2   robustly protect our systems, the sheer number of connections we have to effectively

3   serve customers does increase the potential exposure to cybercrime and the risk, given the

4   role of these IT systems. This is a risk we take very seriously, as discussed at length in

5   my earlier testimony, which details the threats posed by sophisticated bad actors who

6   have recently targeted energy infrastructure and other essential services in the U.S. I also

7   described the Cybersecurity Plan that we may file under the New Plan to provide

8   additional resources to safeguard and prepare our core systems, in addition to our

9   everyday security work, if needed.

10   In sum, the effort and investments of the IT Team support, defend, and amplify

11   the work done throughout GMP, and developing these IT capabilities is extremely

12   important to the work we do.

13   **Q6.   Can you provide some examples of the work the IT Team has recently implemented**

14   **in these areas?**

15   A6.   Yes. GMP's recently filed Integrated Resource Plan ("IRP") now includes a chapter

16   focused specifically on the technology and security improvements managed by our team.

17   Chapter 4 of the IRP provides additional detail on the work currently being completed

18   and planned by the IT Team; I have identified several key examples to highlight here.

19   *Improving the Customer Experience:*

20   The IT Team has devoted significant focus on improving the general customer

21   experience—for example through a redesign of GMP's website to provide easier access

22   to account self-service and usage information—and to strengthen real-time customer

1   communication through a variety of channels during outages and storms. On this latter

2   focus, we created an Outage Center, through which customers can report and view

3   outages; a GMP app, which also provides for outage reporting and self-service; a text-

4   based notification platform; and a redesigned vtoutages.com—used to coordinate outage

5   response and emergency management for utilities statewide.

6   *Enhancing Management of the Grid:*

7   Building off GMP's current Advanced Metering Infrastructure ("AMI") system,

8   we are continuously migrating and improving digitized monitoring and control of grid

9   resources. This rate filing furthers that important work. As discussed below, we have

10   evaluated and planned for critical upgrades to the "Gatekeeper" AMI devices within the

11   Rate Year, which will allow our deployed AMI devices to communicate on modern

12   cellular LTE networks. We have also recently improved the security, resiliency, and

13   ability to automate our digital grid management resources, including a replacement of our

14   SCADA core and other critical automated OT systems.

15   *Improving Security:*

16   Digitizing and upgrading our OT systems also included continued work to isolate,

17   harden, and provide redundancy for these key operational systems. At the same time,

18   computer systems across the company received ongoing updates to firewalls and threat

19   detection.

20   *Streamlining and Improving Operations:*

21   As our operations are increasingly connected and digitized, the IT Team can assist

22   with data analytics and provide new insight on how we can improve operations for

1   customers. One such project is GMP's engineering circuit model, which identifies

2   underperforming circuits. Through this tool, our distribution designers can identify

3   reliability and resiliency gaps and responses to optimize these circuits and prevent

4   outages from occurring in the first place.

5 **Q7.   What are the overall IT priorities during FY23 and how do you account for them in**

6   **FY23 project planning?**

7 A7.   The increasing importance of IT projects, as I just described, assures that the IT Team

8   will be busy during the Rate Year deploying and managing the technology that drives

9   much of our work and offerings on behalf of customers. In addition, we are

10   supplementing our ongoing, normal security work with a further, deeper review of

11   evolving security risks. As a result of that process, we expect to identify and prioritize

12   additional security needs, and reorder projects in development in accordance with any

13   newly identified priorities during the Rate Year and into the remainder of the New Plan

14   period.

15   These needs for quick reaction and refreshed planning and project deployment

16   guide the way our team functions and the updated regulatory treatment we seek. In

17   essence, our IT Team needs to remain flexible, nimble, and prepared to respond to

18   emergent security threats or regulatory changes. For example, in late December 2021, as

19   covered in various news stories, a zero-day vulnerability emerged around the world

20   known as "log4j" that, if exploited, created the potential to allow for total, remote

21   takeover of any system or host containing the affected software. For GMP, responding to

1   this potential threat became an immediate need and required us quickly to enumerate,

2   isolate, and patch hundreds of systems across all areas of our technical landscape.

3   This event is not something we could have specifically planned for, and it shifted

4   personnel and other resources immediately and appropriately to cover this risk for GMP

5   and our customers. This example helps illustrate why the IT Team is asking for greater

6   flexibility in project identification in our FY23 rate request and in the New Plan. Given

7   the rapidly changing landscape, now more than ever, our planning cycle has to be rapid,

8   and our operations and capital projects have to allow us to deploy solutions not

9   specifically contemplated more than a year ahead of time. Indeed, to attempt to meet a

10   more traditional multi-year capital plan like most other teams undertake would be

11   counterproductive to the security and technology requirements of GMP and our

12   customers.

13   **Q8.   What considerations are made when determining the right capital- or expense-based**

14   **solutions to meet these IT priorities?**

15   A8.   As I discussed in my direct prefiled testimony in the New Plan case, much of our IT

16   computing needs are migrating to cloud-based services from on-premise servers. A

17   consequence of this transition, currently occurring throughout many industries, is that the

18   traditional separation between capital and operating expense is no longer applicable.

19   Cloud computing services may be appropriately classified as either capital or O&M, or

20   both, based on the function and timing of expenses associated with that service.

21   Therefore, competing and otherwise similar solutions may actually require different

22   accounting treatment to maximize the value for customers.

1   Our current accounting practice, following current Generally Accepted

2   Accounting Principles ("GAAP"), is to treat all "implementation" costs of acquiring

3   cloud services as capital, while ongoing service fees are expensed. Even under this

4   practice, two candidate cloud solutions could have a similar overall cost, but one could

5   require greater up-front implementation investment and therefore present greater capital

6   spending in our accounting, while the other might entail greater fees over time and

7   therefore have a larger expense impact. For example, when we upgraded our call center

8   technology a few years ago, in addition to evaluating whether proposals met our project

9   needs, we also needed to weigh the benefits of various cloud-based, hybrid, or on-

10   premises solutions and the resulting accounting. These capital and expense impacts

11   therefore become another factor to consider when balancing the many requirements we

12   evaluate for complex IT projects in our preliminary project screening process to ensure

13   we are making prudent investments.

14   These decisions are guided in part by customer cost over the period of investment

15   or service contract, as well as the benefits of meeting critical IT requirements—in

16   particular, alignment with our security needs and philosophies. In evaluating options, we

17   will also consider the additional value a certain solution presents, including the ability to

18   integrate and support other operations, create resiliency benefits, or improve customer

19   convenience, and we will also consider the degree to which future system flexibility is

20   maintained. We will also carry forward the philosophy of GMP's current Climate Plan—

21   now incorporated into our proposed New Plan—in identifying proactive investments to

22   address critical resiliency or security needs to provide cumulative benefits over time.

1   Further, because of the rapid pace of change in the technology sector, a new, flexible

2   approach to IT project planning and documentation is needed to enable flexible and

3   responsive investments as technology and threats develop rapidly. This will help ensure

4   that prudent capital investment alternatives to O&M solutions can be swiftly evaluated.

III.   IT FY23 Capital Investments

5   **Q9.   How are IT capital projects identified and selected?**

6   A9.   **Exh. GMP-MD-1** describes the IT capital planning process, which identifies projects

7   that deliver value through customer service, operational, capacity, resiliency, and security

8   improvements, while exploring new technologies to achieve these improvements.

9   This rate filing also incorporates a new proposed regulatory accounting practice

10   for the IT Team. We are requesting an IT Budget for capital investments in the Rate

11   Year based on a historical five-year average of IT investments. This request is driven by

12   the accelerated planning cycle for IT projects, which often require a nimble project

13   planning process to account for technological and security developments occurring within

14   the planning horizon.

15   **Q10.   Please identify the capital investment level on IT projects included in this filing.**

16   A10.   We are proposing just under $8.0M of overall capital investment in IT projects during the

17   Rate Year. As described below, this total is equal to the historical five-year average IT

18   capital investment. It includes the traditional IT blanket for smaller, as-needed projects,

19   identified FY23 projects, and our request for capital projects that fit our more rapid

20   development cycle and emerging needs (in total for FY23, referred to as the "IT

1 Budget"). **Exh. GMP-MD-2** breaks out our IT Budget by project category, while **Exh.**

2 **GMP-MD-3** sets out the individual projects included within the budget.

3   This filing also describes capital additions and retirements during FY22 (the

4 "Interim Year") under the Current Plan's capital framework. These are presented in **Exh.**

5 **GMP-MD-3**. These projects have been documented consistent with the standard

6 established in Exhibit 2 to the Memorandum of Understanding ("MOU") between GMP

7 and the Department of Public Service ("DPS" or the "Department") in Case No. 17-3112-

8 INV, described by Mr. Burke and included in this filing as **Exh. GMP-MB-5**.

9 **Q11.** **Please describe the Rate Year IT blanket included in this rate filing.**

10 A11. The IT blanket continues to be an important mechanism to match up some expected Rate

11 Year spending that always arises but cannot be precisely identified given the pace and

12 flexibility needs of IT work. Consistent with GMP and the Commission's prior practices,

13 we have identified and included our traditional IT capital blanket, intended to cover

14 smaller, incidental, and emergency capital requests throughout the Rate Year. These

15 expenses are typically routine and repeated, but not individually identifiable in advance.

16 Capital expenses previously subject to the IT blanket will continue to be covered under

17 this project. The level of the blanket is set based on historical five-year averages in this

18 category. For the Rate Year, the IT blanket is $0.32M.

1   **Q12.   Can you explain why approving an overall IT Budget for the Rate Year is**

2   **appropriate?**

3   A12.   The planning cycle for the IT Team's capital projects is fundamentally different than

4   planning cycles for many other capital projects. The speed of the IT planning cycle is

5   driven largely by the pace of development in this industry. Unlike many physical capital

6   projects, including traditional "servers and wires" IT projects, digitized solutions can

7   often be deployed very quickly and project turnaround times are shrinking rapidly.

8   Adapting to these shortened timelines allows the IT Team to implement projects with the

9   best available technology for customers when we deploy the service or program. At the

10   same time, bad actors are similarly developing and implementing digital tools for attack

11   at an equally quick pace. The ability to react with speed and flexibility, and to be

12   prepared for contingencies, is critical to digital security.

13   A nimble planning cycle also supports several important goals. Our work is

14   closely integrated in all our innovative projects, providing technical capability for new

15   services that may not yet have established IT solutions. And our customers' expectations

16   of communications, billing, self-service, and how they use electricity continue to drive

17   advances and new approaches.

18   Achieving these goals in the framework of the standard rate case planning-and-

19   review cycle for capital projects is increasingly difficult, and does not best serve our

20   customers or our overall security footing. Planning for projects 12–24 months out, our

21   team usually will not know project program or equipment details at the same level of

22   certainty as for other physical projects, such as a necessary/planned substation upgrade,

1   for example, that usually has clear parameters and a known range of solutions and costs.

2   For example, in the time between initiating and implementing an IT project, we may need

3   to develop or co-develop new software or system interfaces, and in that same time new

4   services or technology could arise, as could new threats and operating constraints.

5   For these reasons, the details change for most IT projects between the initial

6   identification and documentation and the closing of a project. The standard capital

7   planning and documentation cycle used for other types of projects therefore does not

8   always provide a useful process, nor does locking in a specific project in advance serve

9   our paramount need to plan with speed and flexibility. To provide projects that best serve

10   customers, the IT Team should be focused on analyzing and justifying projects based on

11   a shorter timeframe that better matches the actual implementation and current—

12   sometimes emergent—need at the time.

13   To help the Commission's review of this request, **Exh. GMP-MD-2** presents our

14   overall five-year average IT capital expenditures by functional category, inflated to FY23

15   levels. As is evident, costs fluctuate between categories and year over year, but overall

16   trend within a similar range of the average investment over time. Within these

17   categories, we also expect security spending to increase as a percentage of the total

18   budget going forward, and as noted in my direct New Plan testimony, we have requested

19   further regulatory accommodation to file an additional Cybersecurity Plan if needed to

20   enhance this critical security work.

1   **Q13.**   **What specifically are you asking the Commission to approve for the overall IT**

2   **Budget?**

3   A13.   In addition to the IT blanket and the specifically identified FY23 projects expected to

4   close during the Rate Year described in more detail below, we are seeking Commission

5   authorization to include in FY23 rates an IT Budget based on historical IT spending, net

6   of identified projects.

7   GMP's proposed approach is akin to the Commission's practice in allowing

8   blanket work orders, based on proven need over the years for spending at average annual

9   levels even though precise projects are not identified. For this additional budget amount,

10   GMP is guided by five-year averages for our overall IT spending, like the approach we

11   take specifically for our blanket requests, to reflect the baseline annual need. We began

12   by including the Rate Year capital projects I identify below, including the small IT

13   blanket based on historical five-year averages strictly for that category. The budget we

14   propose would cover all remaining IT spending in the Rate Year up to the historical

15   baseline, or just under $8.0M in total. As reflected in **Exh. GMP-MD-2**, the net of this

16   budget item represents $3.27M in capital investment. This balanced approach provides

17   the flexibility needed to make sure we have the resources to implement the right solutions

18   during the rate year to deliver strong benefits for customers at the time the software,

19   service, or product is rolled out.

1   **Q14.   What individual projects expected to close during the Rate Year are included within**

2   **this filing?**

3   **A14.**   We have identified several larger IT projects closing during the Rate Year. These

4   projects plus the blanket previously described represent approximately $4.7M of the

5   nearly $8.0M total IT Budget request and are also included within this filing as set forth

6   in **Exh. GMP-MD-3**. The most significant of these Rate Year projects include:

7   **Project 176800 Mobility Networks & AVL - $1.79M:** This project was

8   prompted by the sunsetting of support for cellular routers used in our in-vehicle wireless

9   communications and automated vehicle locator ("AVL") technology. Replacing these

10   routers is critical for safety to maintain communications to and from our fleet and our

11   teammates in the field, particularly to facilitate recovery operations in remote areas.

12   **Project 177062 Gatekeeper Comm Device Replacement - $1.25M:** This project

13   was also initiated in response to sunsetting cellular routers, in this case, the routers

14   powering AMI collection devices. This update will change out equipment to conform

15   with LTE service and is critical to avoid obsolescence of these devices and to interface

16   with modern cellular technology and frequencies.

17   **Project 176781 RECON Rewrite - $0.39M:** This **s**oftware upgrade project

18   modernizes the program GMP uses for reconciling built capital projects with their design.

19   It is a critical step in the financial workflow and plays a key role in creating and retiring

20   assets within GMP's business management system. The modernized system will be

21   adaptable to our future needs while replacing an outdated solution that is growing

22   difficult to support.

1   **Project 176782 Oracle Util Test Accel - $0.34M:** As I discuss below, GMP is

2   preparing for a necessary migration of its Oracle business management software from

3   products Oracle will no longer support to an enhanced new utility suite that combines our

4   Meter Data Management system with our Customer Care and Billing system. Planning

5   for this migration and testing the software in anticipation of this migration are essential

6   steps. This project involves the purchase of an automated testing tool that is 70% faster

7   than our current manual testing process that requires the IT team to run the tool. This

8   work will enable us to continue this important project in the years beyond FY23.

9   **Q15.** **Beyond these specific FY23 projects you have identified, how will the IT Team**

10   **utilize the remaining IT Budget requested here?**

11 A15. Based on experience, we know we will make several additional investments in FY23, at

12   the overall levels demonstrated in **Exh. GMP-MD-2** (IT Five-Year Average Budget).

13   Our expected further capital needs during the Rate Year are summarized at a high level

14   below, though as noted, our planning environment would not serve GMP or customers

15   well if we set these projects in stone now. As discussed above, rapidly changing

16   priorities, requirements, or circumstances will occur within this forecasted timeframe,

17   and alternatives to what we may currently expect no doubt will prove more necessary and

18   more beneficial to customers.

19   **Security Operations Center ("SOC") Enhancement:** GMP's operation center

20   monitors our grid infrastructure on a 24/7 basis and allows for coordinated responses to

21   outage and grid events. We take a similar approach through internal and external

22   resources for our cybersecurity. To further enhance those capabilities, we expect to

1   strengthen this type of dedicated framework for continual monitoring of our information

2   systems' security, particularly as the cybersecurity threat environment evolves. We are

3   scoping this work and expect to continue that into the Rate Year and beyond, likely in

4   phases as we do with many IT projects to ensure that we stay in line with current

5   technology and security needs.

6   **FERC Security Infrastructure Compliance:** As I discussed in my opening New

7   Plan testimony, cybersecurity is a current focus and area of action for federal regulatory

8   agencies including the Federal Energy Regulatory Commission ("FERC"), which is part

9   of the reason we have requested the option to propose a Cybersecurity Plan during the

10   New Plan. As part of ongoing review of regulated hydropower facilities, FERC has

11   directed facility owners, including GMP, to enhance cybersecurity protocols. We are in

12   the initial stages of review for six facilities, and are approaching this work with a focus

13   on developing a compliance protocol that we can then iterate to enhance *all* generating

14   facilities and assets that the protocol would be appropriate for, because the threats are not

15   unique to FERC-regulated facilities.

16   **GMP website and mobile app updates:** Our GMP website is the portal through

17   which many of our customers interact with GMP, and we are continuously updating its

18   performance and functionality. This work is a good example of ongoing, routine

19   investments that we know that we will continue to make, and we do expect to make

20   additional upgrades to the website during the Rate Year. These continual updates are

21   often made to take advantage of the most up-to-date software or service, to ensure a

22   secure and optimal customer experience. However, incorporating beneficial advances as

1   they are developed does not allow for extended planning cycles for these projects,

2   particularly as vendors and services consistently evolve in this area.

3   **Outage Management System and GIS upgrades:** Our outage management and

4   GIS systems have reached their end of life and need updating. While the precise scope of

5   this project is uncertain at this time because prerequisite work on projects involving the

6   underlying systems that are managed by other teams must be completed first to inform

7   the best IT solution for these updates, this project will be critical for GMP to advance for

8   customers in the coming year.

9   **Oracle Migration:** GMP's utility management software is provided by Oracle,

10   which is sunsetting their existing utility suite tools and transitioning to a new, combined

11   Meter Data Management and Customer Care and Billing product. Upgrading our

12   systems and migrating to the new product will be a substantial undertaking requiring

13   several years of work. We have just started the preliminary assessment phase of this

14   future work and are in the meantime completing several smaller projects that will bridge

15   to this work as reflected in the capital projects included in this filing. GMP has not yet

16   scoped this project, and given its complexity, does not anticipate it will close in the Rate

17   Year. We do anticipate, however, that this project will require additional investment

18   above the baseline IT historical spending level over the course of the New Plan, driven by

19   specific GMP architecture and security requirements in its implementation, which would

20   be identified in any future Cybersecurity Plan request, or if warranted, as a strategic

21   investment for customers.

IV.   IT FY24–FY26 Forecasts

1 **Q16.   How are GMP's IT forecasts for the remainder of the New Plan presented in this**

2 **filing?**

3 A16.   Forecasted IT capital investments and a summary of representative expected work are

4 provided in **Exh. GMP-MB-4**. Mr. Burke's testimony sets out, in detail, the general

5 capital forecasting process employed across all teams to arrive at the level of investments

6 presented in that exhibit, including for IT. O&M expenses throughout the Rate Year are

7 set by general category as explained by Mr. Ryan and Mr. Bingel.

8 **Q17.   How did GMP develop these forecasts of IT capital investments and the remainder**

9 **of the New Plan?**

10 A17.   We supported the work of GMP's finance team to develop forecasts for FY24–26 for the

11 New Plan by reviewing the realistic timeframe for planning and implementation for

12 already-known or anticipated IT/OT projects, along with their expected scope and

13 magnitude. We also evaluated, based upon our review of the historical five-year average

14 spending, the likely additional IT project spending that will occur for projects not yet

15 specifically contemplated, but that will be required in a faster planning cycle. As

16 described above, this faster planning cycle is, in part, a function of the pace of

17 technological improvement and IT project management, but it also reflects a degree of

18 uncertainty about the regulatory and security environment in coming years. We have

19 planned around this uncertainty to a degree by incorporating a single IT Budget during

20 the Rate Year and incorporating historical averages in our forecasts.

1   Included in these forecasts are currently anticipated levels of security work, and

2   expected levels of spending for known applications and operations upgrades and

3   deployments. This includes likely additional investments (like some of the capital

4   projects specifically described in the Interim Year and Rate Year) for migration to new

5   Oracle applications and upgrades, though we expect this need may grow as that project

6   advances.

7   Similarly, we have not included enhanced spending that may be required after

8   completion of our deep security review mentioned above, nor have we included project

9   costs that may be required to further enhance our security operations. The option to

10   propose a Cybersecurity Plan, as described in my opening New Plan testimony, provides

11   another way to address the uncertainty associated with evolving federal regulatory

12   standards and expanding security risks throughout the remainder of the New Plan.

13   **Q18.** **Can you speak further to how GMP's proposed Cybersecurity Plan impacts your**

14   **forecasting?**

15   A18. Our forecasts were developed to account for all IT work going forward, without including

16   any potential Cybersecurity Plan authorization or investment. The forecasts represent a

17   business-as-usual scenario, based on our currently available knowledge, plus reasonably

18   expected investment in this area. The Cybersecurity Plan, on the other hand, would be

19   offered to provide flexibility and allow for effective responses to new regulatory

20   requirements, industry accounting changes, an evolving threat environment, unforeseen

21   advances or new technology we should invest in for the benefit of customers, or other

22   opportunities to make strategic system security upgrades for the benefit of customers or

1   to optimize regulatory and accounting treatment for certain IT projects. Each of these

2   contingencies speaks to the level of uncertainty and growth within the IT sector.

3   Accounting for that uncertainty is the purpose of the Cybersecurity Plan.

4   Because the purpose of the Cybersecurity Plan would be to enhance investments

5   beyond those currently planned, we are not including an estimated cost in our forecasts at

6   this time. Instead, our forecasts are based on an evaluation of the investments that best

7   secure systems and serve customers using the information currently available. If that

8   evaluation changes significantly—and it may, given the nature of this field—we will use

9   the same process to determine whether alternative investments through the Cybersecurity

10   Plan serve customers better at that time. Those would require Commission review and

11   approval.

12   **Q19.   Can you speak to how capitalization of cloud expenses impacts IT O&M expense?**

13   A19.   We expect to experience ongoing O&M expense pressure in IT because of our expanding

14   role and the increased attention warranted by emerging cybersecurity concerns. We

15   engage with external services to augment our personnel, particularly with security

16   consultation, and expect to need additional internal resources and talent in the years

17   ahead to manage the obligations and necessary workflow to keep our systems cyber safe.

18   With the increased complexity and frequency of cyber attacks and likely increased

19   regulatory requirements for cybersecurity, this work will only accelerate going forward.

20   We plan to manage around this pressure to the extent possible to minimize rate impacts

21   for customers, and an important tool will be the capitalization of services, particularly

22   cloud services. We are capitalizing some of these expenses through implementation of

1   the current GAAP guidance, as described earlier in my testimony, and will seek further

2   regulatory authorization through the Cybersecurity Plan as necessary.

3   **Q20.   Does this conclude your testimony?**

4   A20.   Yes.