Montana Public Service Commission
Docket No. 2022.07.078
Electric and Natural Gas General Rate Review

PRE-FILED DIRECT TESTIMONY

OF JEANNE M. VOLD

ON BEHALF OF NORTHWESTERN ENERGY

TABLE OF CONTENTS

Witness Information

Q. Please provide your name, employer, and title.

A. My name is Jeanne M. Vold. I serve as NorthWestern Energy's ("NorthWestern" or "Company") Vice President – Technology.

Q. Please provide a description of your relevant employment experience and other professional qualifications.

A. I have worked in the utility industry for 25 years. Early in my career I performed overhead and underground line construction. My engineering career then forayed into medium voltage systems, control systems, and high speed manufacturing. I joined NorthWestern in 1999 with a career shift into Information Technology ("IT"). Due to the partnership with the business and alignment with business strategy, NorthWestern includes "IT" under the broader umbrella of Business Technology ("BT"). I have held several leadership positions in the technology area and have led key system implementations for the Company. I have been overseeing all of BT for NorthWestern since 2007 and assumed my current position in 2021. My experience includes control systems and applications as well as knowledge in data center, networking, and cyber security. My undergraduate degree is in electrical engineering from the South Dakota School of Mines and Technology.

I am active in several industry associations including Edison Electric Institute, the Western Energy Institute, and the Institute of Electrical and Electronics Engineers. In addition, I also serve on the MT-ISAC (Montana Information Security Advisory Council).

Purpose and Summary of Testimony

Q. What is the purpose of your testimony in this docket?

A. My testimony provides a high-level overview of Business Technology and its role at NorthWestern with a focus on the importance of cyber security and the challenges we face. The threats the Company faces are significant, and our ability to identify, detect, defend, respond, and recover is essential. In order to provide safe and reliable service to our customers, we must adapt and invest in tools to thwart the ever-evolving threats we face related to cyber security.

Q. Please summarize your testimony.

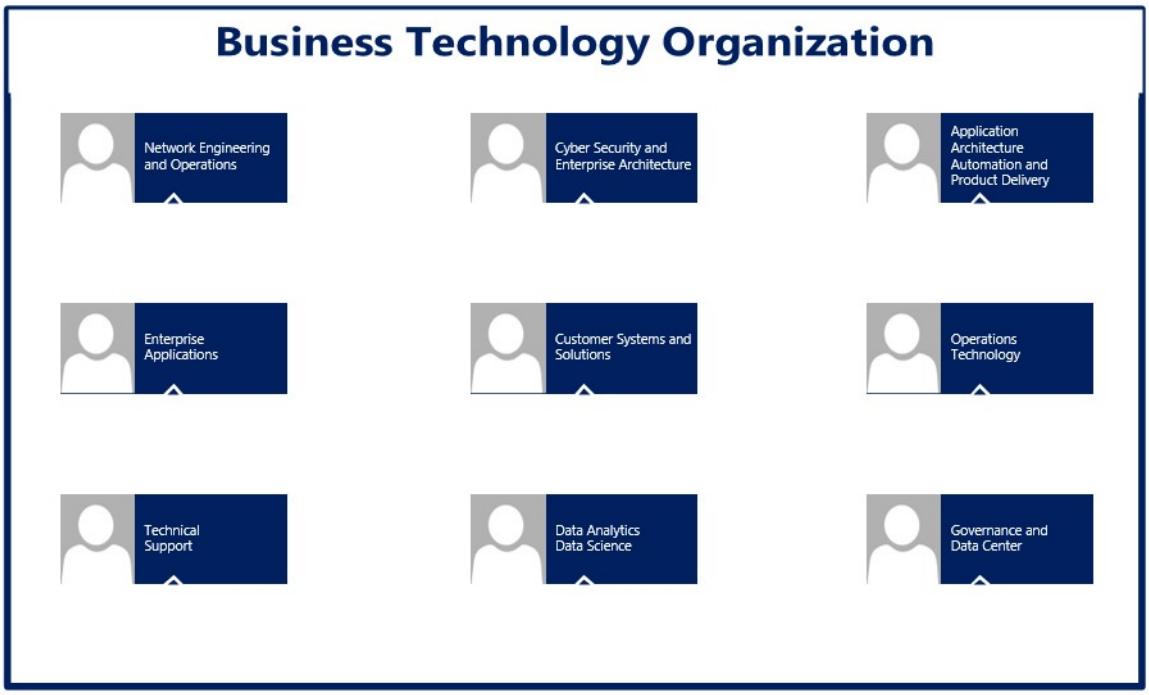
A. I provide insight into the complex eco-system we must protect to ensure safe and reliable service to our Montana customers. Our systems are comprised of software and hardware connected by networks which allow all the necessary communication to occur. It all begins with building and protecting the networks. One can think of them like data highways that include all the on ramps and off ramps for users to access systems and perform their work. Our defense in depth model serves us well in this regard with critical systems, such as those operating the grid, buried deep inside many layers of security. Leveraging the CIA (Confidentiality, Integrity, and Availability) triad is paramount. We must make sure we protect the confidentiality, integrity, and availability of our data. Living by the mantra of least privilege (only users who need access to the data have

access to the data) is critical. We must ensure the integrity of our data. People's lives depend on it. A piece of malware could change or manipulate data which may lead to incorrect decisions based on corrupt data. Hypothetically, nefarious actors could manipulate systems and provide incorrect information about the status of our electric or natural gas systems. The Company could potentially make decisions based on the incorrect data input by the nefarious actors. Inadvertently relying on the incorrect data, we could energize a line or open a valve in a situation that could cause severe injury or death. Finally, the availability of the data is vital. We need to have access to it when we need it. To this end, NorthWestern has combined the role of Enterprise Architect and Security Officer. This means security is embedded into our architecture design from the very beginning. Many companies bolt on security after something is built. Our approach has served us well by embedding the security into the build of systems. This puts us in a better defensive position to prevent attacks.

Overview of NorthWestern's Business Technology Department

Q. Please describe NorthWestern's Business Technology Department.

A. NorthWestern's Business Technology Department is organized into several practices that work together as matrixed teams to protect, defend, run, upgrade, and implement new systems. These functions are graphically illustrated below.



Q. Please describe the BT Department's different practice areas.

A. The nine areas depicted in the illustration above are described below:

- Cyber Security and Enterprise Architecture: As mentioned above, NorthWestern has combined the roles of Enterprise Architecture and Cyber Security since 2010. We believe this provides a unique solution to embedding cyber security into any system we build. The

internal threat hunting team is also part of this group. The team actively monitors cyber threats on a global scale and applies real-world learning to seek out potential threats in our enterprise. The team is responsible for all firewalls and end point protection, which includes all computers, smartphones, and IoT (Internet of Things) devices. Intrusion detection, intrusion prevention, and network access control are all managed by this team. The team leverages tools such as Security Information and Event Management ("SIEM") to aggregate inputs from cyber security systems and perform event correlation. Network and application security also roll up under this group. Last but certainly not least, this group leads the disaster recovery and incident response efforts with support from the whole organization.

- Network Engineering and Operations: This group operates an expansive communication network across all states in which we operate and includes NorthWestern-owned (on-net) systems and third party-owned (off-net) systems. The team is responsible for the wide area network including all of our fiber, microwave, and mobile radio systems which provide the communication channels for protective relaying and our numerous Supervisory Control and Data Acquisition ("SCADA") systems. This group manages all wired and wireless networking, switching, and routing. Engineering for network expansion in all of these areas, especially system control, is also

performed by this group. Finally, all telephone, telecom carriers, and internet presence is supported by this team.

- Governance and Data Center: This team provides necessary Technology Governance which includes oversight for policies, records management, licensing and leasing, contracts, and budget. All internal and external audit requirements are managed through this group. From a data center perspective, the team is responsible for data center operations in both primary data centers and all server infrastructure (virtual and stand-alone). The team performs server patching, application delivery, file storage, and full system backups. They are responsible for building secure server images for application deployment which includes virtual desktops and application delivery.
- Application Architecture, Automation and Product Delivery: This team works very closely with the Enterprise Architect to integrate, automate, and deliver applications to users. Large technology projects are managed out of this group. Application integration (making sure all the systems that need to exchange information in real time are doing so in a secure and efficient manner) is also the responsibility of this group ensuring interoperability across platforms. Sophisticated application development is sourced out of this team leveraging agile methodologies (iterative dialogue and solution delivery in concert with users) as a mechanism to deliver solutions.

- Enterprise Applications: This team is responsible for Business Relationship Management as it relates to applications used across the enterprise. The team works very closely with business constituents to ensure solutions are providing required functionality. In addition, they support the evaluation and implementation of new technology in concert with the Enterprise Architect. Responsibilities include application development and application support as well as database administration. The largest system the team supports is the SAP Enterprise Resource Planning system which includes finance, materials management, work management, project financials, and human resources. Other systems which reach across the enterprise and fall under this group include the learning management system, physical security key card system, and environmental software.
- Operations Technology: This team is responsible for Business Relationship Management as it relates to applications leveraged in Operations. The team works very closely with business constituents to ensure solutions are providing required functionality. In addition, they support the evaluation and implementation of new technology in concert with the Enterprise Architect. Responsibilities include application development and application support. Applications supported include field force automation, generation, and multiple SCADA systems.

- Customer Systems and Solutions: This team is responsible for Business Relationship Management as it relates to all customer facing systems. The team works very closely with business constituents to ensure solutions are providing required functionality. In addition, they support the evaluation and implementation of new technology in concert with the Enterprise Architect. Responsibilities include application development and application support. Applications supported by this team include call center technology stack, cash processing, web site, and advanced metering infrastructure.
- Data Analytics and Data Science: The team drives strategy for data, analytics and artificial intelligence. They work across the entire organization to leverage data as an asset. The team manages the data science and analytics program and works with business and operational groups to platform solutions leveraging analytics and artificial intelligence ("AI") to solve complex problems. For example, the team has successfully implemented an analytics program in partnership with distribution operations to analyze distribution level outages to determine the circuit segments with the most outages and leverage AI to focus on plans for addressing circuit segments with poor reliability.
- Technical Support: This group is our front line support group serving not only as our help desk but supporting rollouts of new technology

across the enterprise. They must be knowledgeable in many areas of the Company and adept at troubleshooting. They are responsible for all PC images (secure hardening of all PCs), PC rollouts, and end user device support as well as being front-line support for all applications.

Q. How does the Business Technology Department ensure safe and reliable service to NorthWestern's customers?

A. Any process we perform as a company is touched by technology in some way. Providing safe and reliable service to customers is paramount to our mission. The Business Technology group supports all business and operational functions across the Company. From an applications perspective, we support customers, operations, and the enterprise with an array of integrated complex systems to provide the reliability customers expect. For instance, an outage notification from a customer call begins with a service order in the Customer Information System ("CIS"). The information is passed in near real time to our field software on a tablet and the service technician is dispatched. Information from the field updates our outage map on the web site as well as our Advanced Distribution Management System/SCADA and field service system. When the outage is fixed in the field, the service order is closed on the back end in CIS and the outage map is updated. The team also provides the complex network enabling the data to flow where it needs to be. All departments rely on us

for the availability of systems. We have extensive monitoring processes encompassing the status of applications and networks which provide pro-active alerts concerning the health and status of our eco-system – the ever-changing landscape of applications, networks, and IoT devices. NorthWestern could not take a call, read a meter, dispatch a service order, process a payment, provide a financial statement, or respond to an outage without the technology the Business Technology Department provides.

Q. Why else is the Business Technology Department vital to NorthWestern and customers?

A. First and foremost, NorthWestern owns and operates critical infrastructure. The service we provide is vital to the citizens of the State of Montana. Therefore, we take the protection of all our systems extremely seriously. When it comes to the systems that control and monitor our generation, electric, and natural gas infrastructure, we secure and architect these systems so they can function in isolation and are protected from the Internet. Protection from the Internet is crucial since it is an absolutely untrusted environment. Anything connected to the Internet is subject to brute force cyber-attacks from literally anywhere in the world. External defenses such as firewalls and defense in depth strategies help, but it is important critical operations can continue to function without the Internet. Our strategy is network segmentation, which offers the flexibility for these critical systems to be islanded and operational on their own.

This strategy is solid and best practice across the industry. Threat actors or people/entities having the ability or intent to impact the security of other individuals or companies never rest. They may be motivated by financial gain such as a ransom or they may be trying to disrupt critical infrastructure through a cyber-attack causing distrust and panic. They may be motivated by geo-political tensions. Regardless of their motivations, NorthWestern's response must be continuous investment in the cyber defense systems necessary to defend against the ever-evolving threat landscape and the desire of threat actors to disrupt critical infrastructure operations.

Cyber Security Threats and Technology Upgrades

Q. What cyber security threats does NorthWestern face?

A. I will discuss this in two parts as I view threats to be in two categories: malicious and non-malicious. From a malicious perspective, NorthWestern is under constant attack. Firewalls, which block unknown or malicious traffic and allow known communication through a succinct rule set, are integral to our defense in depth strategy. Our external firewalls constantly thwart attacks. Externally nefarious entities use automated tools to probe our network for holes finding ways to enter. These attacks vary from what I would classify as "drive-by" threats, which are casual automated scans to see if we left an easy vulnerability vector open, to specific, targeted attacks directed at our Company. Targeted attacks are

specifically designed to infiltrate our Company with a specific goal in mind. The attacks are persistent, and much more effort is spent trying to infiltrate our defenses. Our threat hunting and monitoring teams leverage tools to aggregate and analyze these threats and respond accordingly. The tools used are extremely sophisticated with embedded AI which learns what is normal and what is not normal. The tools aggregate data and alert our team when anomalies arise. The team subsequently investigates the alerts. It is not uncommon to see nation states hostile to the United States as the source of such attacks.

We are also vulnerable to phishing and spear phishing attacks. While phishing casts a wide net and is a broader practice of sending emails trying to induce individuals to reveal personal information, log in credentials, or company information, spear phishing targets specific individuals or groups with much more sophistication. Spear phishing targets have been well researched with much more time and research put into the target's work function and companies or people they may work with in order to deceive the user into providing information such as log in credentials, which would provide an access point for them. Although employees are required to take annual cyber security training, it only takes one human mistake to introduce malware. For example, a user could click on a link or open an email attachment which delivers malware or ransomware rendering the systems inoperable. If malware is introduced,

threat actors could lurk and learn in a system for months before launching a targeted attack.

The Company also has the potential for malicious insider threats due to a disgruntled employee or contractor wishing to do harm to the Company. Employees or contractors could harvest data, place malware on critical systems, or install back doors to allow for undetected access to critical financial or operational systems. Non-malicious threats could be unintended human error such as an employee accidentally emailing information to the wrong person or misconfiguration of software or hardware that allows unintended access that a threat actor could exploit.

Q. How does the Business Technology Department address these threats?

A. One of the most important measures we perform is just good hygiene. This encompasses the blocking and tackling of cyber security. The team removes user access in a timely manner, keeps systems up to date and patched, and ensures sufficient complexity of passwords and multi-factor authentication is used. Patching is key since it applies software updates addressing bugs and cyber security vulnerabilities. In addition to hygiene, NorthWestern has a threat hunting team. This team researches and monitors threats across the globe, regardless of industry, which could impact NorthWestern. They proactively use tools and leverage AI to scan

and detect anomalies throughout the network. The team performs vulnerability assessments and assigns remediation activities. Vulnerability assessments are important because they are continuously run to help us identify any technical weaknesses we may have, and remediation activities identify how to fix them. The team has isolation and recovery tools available to recover after events such as ransomware. Isolation tools allow us to island a system and leverage backups and software, allowing us to return a system to the state it was in before an attack. For example, we can essentially return encrypted files targeted in a ransomware attack to their original state.

Q. What could happen if potential threats are not adequately addressed?

A. If we do not adequately adapt and evolve to combat the changing threat landscape, we put the delivery of energy to our customers at risk. For example, if a threat actor gained access to the systems that run our transmission or distribution systems, they could shut down our operations and cut energy supply to our customers. The nation saw what could happen with a ransomware strike when threat actors shut down the Colonial Pipeline and disrupted oil supply throughout the eastern United States. The Colonial Pipeline Company was a victim of a ransomware incident targeting their billing system that caused them to shut down operations in May of 2021. Adapting and evolving requires investment in

tools, replacement of end-of-life security systems, and patching systems with vulnerabilities. All of this requires significant ongoing investment. These costs are rising exponentially due to pricing escalation in support agreements, vendors moving to subscription pricing models, and the necessity to procure new tools. NorthWestern must carry support agreements for hardware and software. Without these agreements, we are not eligible for security patches from vendors for their products. In addition, we are seeing more software vendors move from a licensing model under which we own the software to a subscription model where we just "rent" the software. The initial purchase of licensed software is treated as a capital expenditure, but maintenance and subscription models are classified as operation and maintenance ("O&M") costs, and the situations described above are all contributing to our rising expenditures.

Q. Please provide some examples of recent cyber security threats faced by NorthWestern.

A. The end of 2020 brought us SolarWinds. SolarWinds was a supply chain incident whereby hackers inserted malware into software updates ultimately downloaded by SolarWinds Corporation customers. At the time of the event, NorthWestern was a SolarWinds customer. NorthWestern responded by immediately by removing the software from its environment and performing vulnerability assessments. Ultimately, we were not impacted by this supply chain attack. The malware created a back door

on vulnerable systems allowing for threat actors to transfer files, execute files, profile the system, reboot the machine, and disable system services.

The end of 2021 brought us Log4j. Log4j is by far the most challenging vulnerability all industries have faced. The vulnerability allows remote code execution through web requests with no authentication. This means any vulnerable system could be used to cripple systems and render them unusable as well as steal information. NorthWestern responded to this threat by assessing all systems, prioritizing remediation, and implementing software updates. NorthWestern repeated the assessment and remediation cycle until the vulnerability was fixed. This piece of open source (publicly available code which anyone can use) logging software is embedded in thousands of systems and applications. The severity ranking of the SolarWinds incident was 8.8 while the severity ranking of Log4j is a 10.0. This is the top of the vulnerability scale. Jen Easterly, Director of the U.S. Cybersecurity and Infrastructure Security, said this vulnerability is “one of the most serious I've seen in my entire career, if not the most serious."[1] These two examples are indicative of the vigilance we must have as a Company. Log4j is on its fourth or fifth variant, and nefarious actors are finding new ways to exploit it each day.

[1] Quote from Jen Easterly, Director of CISA Concerning The Log4J Vulnerability Will Haunt the Internet for Years | WIRED

NorthWestern was impacted by both of these attacks. Fortunately, by having a defense in depth strategy and a threat hunting team, we were able to mitigate these threats before these vulnerabilities compromised our systems. We were able to identify, isolate, and remediate impacted systems. Ignoring such vulnerabilities is not an option, and the impacts of not addressing them could be devastating for our customers if these threats caused loss of the systems that deliver energy. This would not have been possible without the investment made in the tools used by the team – continuous investments in updates for existing tools and investments in new tools necessary to thwart ever-changing threats.

Q. Can you provide some examples of when cyber security threats have overwhelmed utilities or other similarly-situated businesses?

A. Yes. The most famous and successful interruption of service was the 2015 attack on Ukraine. The primary attack vector was spear phishing, which harvested user credentials and allowed remote access. This access was leveraged to lurk and learn in the system for months and gain access to industrial control systems before the actual attack was launched. This attack was particularly interesting because it was a coordinated and well-orchestrated attack. As stated, the threat actors spent months lurking in utility systems before launching the synchronized command and control attack that impacted over 250,000 people. The nefarious actors were successful in simultaneously interrupting distribution

operations for two utilities by causing widespread outages. By leveraging the remote access and malware, they were able to control and corrupt control systems as well as place malware on end-point monitoring devices in conjunction with a denial of service attack on the call centers of the impacted utilities. The denial-of-service attack prevented customers from reporting outages and operators lost visibility to the system.

Another example is the attack in 2021 on a Florida water treatment plant. This attack highlighted the importance of good cyber hygiene. In this case, attackers leveraged computers with unsupported operating systems to gain access to a remote access platform which was no longer used but not yet decommissioned. Good cyber hygiene (not running outdated software and decommissioning unused systems) would have prevented this attack. As mentioned earlier, the Colonial Pipeline attack disrupted energy supply up and down the East Coast. In this case the hackers took advantage of an unused virtual private network account which did not require multi-factor authentication. The simple requirement of multi-factor authentication would have prevented this attack.

Q. How does BT support other departments' regulatory compliance obligations associated with cyber security?

A. NorthWestern must maintain compliance with regulations from several entities including Sarbanes-Oxley, Pipeline and Hazardous Materials

Safety Association, and North American Electric Reliability Corporation Critical Infrastructure Protection ("CIP"), all of which have an element of cyber security. The CIP reliability standards have the most rigor, and to ensure our compliance with them, we are audited by the Western Electricity Coordinating Council every three years. Compliance with these and other standards is tantamount to the reliable delivery of electricity.

Q. How did the COVID-19 pandemic affect cyber security threats and regulatory compliance obligations?

A. The pandemic was a game changer for utilities and our computing edge. Globally, cyber security threats and attacks increased as the attack surface was broadened. Ransomware attacks doubled from 2020 to 2021[2] with cyber-attacks in general increasing by 50%.[3] The cyber security team literally architected changes on the fly as we moved to isolate and "pod" mission essential workers. These moves had a domino effect by displacing other workgroups as well as moving employees to home offices. Throughout the podding and additional remote access, we maintained all compliance. In many cases, this meant building new

[2] Ransomware cyberattacks surged in 2021 according to a new report | Fortune

[3] Check Point Research: Cyber Attacks Increased 50% Year over Year - Check Point Software

secure entry points into segmented networks and providing necessary user authentication.

Q. What technology upgrades are necessary for NorthWestern to continue to address cyber security threats and associated regulatory compliance obligations?

A. We must keep all technology related to compliance patched and current. We must replace all end-of-life hardware and software. As threats continue to evolve, we must deploy new security tools leveraging machine learning and AI to alert us when patterns are “not normal”. Continued investments in SIEM and other event correlation tools to aggregate inputs from multiple systems are also essential.

Q. How often are these technology upgrades needed?

A. First and foremost we depend on support and maintenance agreements or subscriptions from every vendor in order to patch system vulnerabilities and keep current with deployed versions. The cyber security landscape changes so rapidly it requires constant evaluation of our software and systems coupled with active threat hunting. All hardware has a defined lifecycle and must be replaced before the end of life. The lifecycle can vary from three to five years depending on the type of hardware and support received from the vendor.

Q. Please describe other technology upgrades necessary for NorthWestern to continue to provide safe and reliable service to customers.

A. Any hardware or software that is at the end of its life or no longer supported must be upgraded or replaced. NorthWestern constantly evaluates replacement technologies for new technology or approaches to solve emerging customer expectations or business problems. We strive to have no single point of failure for our customers.

Cyber Security and Technology Initiatives

Q. What initiatives has NorthWestern implemented to address cyber security threats and technology upgrades?

A. As mentioned above, NorthWestern has an established a threat hunting team made up of our finest cyber security employees. The Company has invested in sophisticated threat hunting tools such as next generation tools for threat and anomaly detection using self-learning AI to identify advanced threats. Such tools can detect the full spectrum of known threats as well as unknown and never-before-seen threats such as zero day attacks. Zero day attacks are particularly challenging because the vulnerability is exploited before a patch can be developed and applied. NorthWestern has also deployed data protection and data loss prevention tools. These implementations also leverage AI and machine learning to model user behavior for anomalies addressing insider threat and provide

data recovery as a defense against ransomware. The AI engine learns what is normal user behavior and alerts the team when it detects abnormal behavior. The focus in recent years has been in deploying pre-emptive cyber security technology. In addition, NorthWestern thoroughly evaluates any new initiative, upgrade, or replacement from a cyber-security perspective prior to deployment. In 2022, major initiatives will include replacement of our external facing firewalls as well as a replacement of the end point security suite on every personal computer.

Q. What tools does the Business Technology Department need to implement these initiatives?

A. We will need next generation AI and technologies, some of which have not yet been imagined. We will also need tools that enable us to more quickly analyze risks with event correlation, logging and alerting events while they happen and leveraging emerging tools to provide alerts on events even before they happen. SIEM tools, mentioned earlier, and their evolution will continue to be even more sophisticated as they correlate real time and predict the future. Next generation products will provide alerts on events in real time. Micro-segmentation implementation will be key as we continue to secure down to the workload level allowing separate processes to be isolated from the rest of the network in the case of a cyber-security event.

Q. What difficulties will NorthWestern face in funding these initiatives?

A. We have seen costs grow at an exponential rate as well as changing cost models. As mentioned above, our maintenance and support agreement costs continue to rise, and vendors moving to subscription models increases our O&M expenditures. Overall, we expect drastic increases due to the pandemic, chip shortages, and supply chain challenges. Microsoft has already warned customers to expect at least a 15% increase in licensing costs as an example. Our Microsoft Enterprise Agreement must be renewed by 2023. We fully expect to see this trend continue.

Q. Will test-year costs plus known and measurable adjustments for costs 12 months beyond the test year be sufficient to adequately fund the required initiatives?

A. Unfortunately, I do not believe test year costs with known and measurable adjustments will cover the rising costs that are out of our control. Since 2017, we have seen support and maintenance costs on average rise 17.0% due to vendor increases, expansion of existing technology, new implementations, and the increasing shift to subscription models. I mentioned Microsoft earlier, every entity using their operation systems and office suite will face this challenge of their escalation in pricing. In addition, our threat landscape is changing so rapidly it is nearly impossible to predict the cyber security tools we may need and how much they will cost. Many of our threat hunting tools did not even exist in 2018. The

Pre-filed Direct Testimony of Sean M. Cleverly provides further details regarding these needs and their potential costs. There are undoubtedly tools NorthWestern will require that have not even been invented yet because threats change so quickly and rapidly. The limitations of the historic test year model with known and measurable adjustments are discussed in the Pre-filed Direct Testimonies of Crystal D. Lail and Cynthia S. Fang.

Q. How does NorthWestern propose to fund the ever-changing costs associated with cyber security threats and technology upgrades?

A. NorthWestern's proposals for more forward-looking cost recovery of BT/cyber security costs are discussed in greater detail by Ms. Lail and Ms. Fang.

While some of the technology needs are unknown as the landscape is constantly changing, we can project expected costs based on analysis of historical increases as well as plans for new technology implementation. From an historical perspective we have seen escalating costs associated with maintenance agreements, subscription based services and upgrades. In addition to these rising costs, we continue expand current technology and implement new technology to increase reliability, customer satisfaction and safe delivery energy to customers. Not all software and hardware support agreements are directly related to cyber security tools.

Nevertheless, they all play a part in the overall cyber security landscape because vulnerabilities can occur in any system at any time and vulnerabilities must be patched. We rely on our vendors to supply these patches. If these agreements are not in place, we are not eligible to receive vulnerability patches.

The Log4j vulnerability is a great example. We leveraged our vendor support agreements in every instance we found Log4j in order to force them to provide us a patch. There were over a thousand instances of Log4j throughout our ecosystem. If we had not had these agreements in place our systems would have remained vulnerable to attack and put the safety and reliability of the grid at risk.

These support agreements must remain in place and we are subject to price escalations each renewal period. Some year-over-year increases are larger than others which make the trends “lumpy”. The increases are due to price escalation of existing agreements, expansion of technology as well as the implementation of new technology. Our largest agreements are typically negotiated over multiple years, which holds pricing for a time but then we see an escalation at the end of the agreement as we negotiate a new one. The costs described can be categorized into three buckets as described below:

1. **Maintain:** This relates to general vendor price escalations for maintenance and subscription agreements.
2. **Grow:** This is the additional cost for licenses and/or subscriptions as the use of technology grows or expands throughout the organization. An example of this is our analytics tool. More and more users are reaping the benefits of this tool and we are obliged to pay for the licensing as the use expands. The same is true for our cyber security tools. The first purchase is generally for a smaller footprint while we learn the tool and continue to grow the footprint and expand it across the network.
3. **New Technology:** There are new technology implementations every year which are additive to the overall care and feeding of our technology systems.

Table 1 below demonstrates some historical trends we have seen concerning the escalation of technology costs. NorthWestern vets and negotiates all renewals in order to obtain the best pricing possible from every vendor.

Table 1: Technology Costs Escalation

	Total Maintenance and Subscription Costs	% Total Increase from Prior Year	Cyber Security Maintenance and Subscription Costs	% Cyber Security from Prior Year	Total Less Cyber	% Total Less Cyber from Prior Year
2017 Actual	$6,525,095	15.8%	$1,847,804	2.8%	$4,677,291	21.4%
2018 Actual	$7,451,945	13.3%	$1,937,451	4.7%	$5,514,494	16.4%
2019 Actual	$7,758,076	4.0%	$1,830,282	-5.7%	$5,927,794	7.2%
2020 Actual	$9,477,628	20.0%	$2,430,301	28.2%	$7,047,327	17.3%
2021 Actual	$10,255,403	7.9%	$3,249,600	28.8%	$7,005,804	-0.6%
2022 Forecast	$15,400,512	40.1%	$4,212,467	25.8%	$11,188,045	46.0%
Average % Difference Year Over Year		16.8%		14.1%		18.0%

As demonstrated in Table 1 above, costs continue to escalate for technology and cyber security. NorthWestern is asking for forward-looking cost recovery for technology and cyber security adjusted for inflation as discussed in Ms. Fang's testimony. This is well below the escalation of these costs as shown in Table 1 above. Thus, our recommendation is a conservative approach that allows us implementation recovery of essential costs that are critical to providing our customers with safe and reliable service.

Q. Why is it crucial for the Montana Public Service Commission to ensure NorthWestern has sufficient funding to address cyber security threats and technology upgrades?

A. I will start where I began with the importance of adhering to the CIA triad of Confidentiality, Integrity, and Availability to ensure we provide safe, reliable and resilient service to our customers. NorthWestern would not

have been able to mitigate Log4j without vendor patches funded by our maintenance and support agreements and the threat hunting tools we acquired. We simply must have the ability to upgrade to address vulnerabilities that could arise in virtually any system we operate. The Technology Leadership Team takes great care in evaluating vendors and prudently funding necessary projects. The employees genuinely care about the citizens of Montana and take great pride in their role delivering critical service to our customers. The safety of our customers directly relates to the cyber security the team provides.

Q. Does this conclude your testimony?

A. Yes, it does.

VERIFICATION

This Pre-filed Direct Testimony of Jeanne M. Vold is true and accurate to the best of my knowledge, information, and belief.

/s/ Jeanne M. Vold
Jeanne M. Vold