

Board Policy Committee Meeting and Special SMUD Board of Directors Meeting

Date: Wednesday, November 17, 2021

Time: Scheduled to begin at 5:30 p.m.

Location: Virtual Meeting (online)

AGENDA

BOARD POLICY COMMITTEE MEETING AND SPECIAL SMUD BOARD OF DIRECTORS MEETING

Wednesday, November 17, 2021

Scheduled to begin at 5:30 p.m.

Zoom Webinar Link: [Join SMUD Board Policy Committee Meeting Here](#)

Webinar/Meeting ID: 160 836 5111

Passcode: 387437

Phone Dial-in Number: 1-669-254-5252 or 1-833-568-8864 (Toll Free)

Pursuant to Government Code section 54953(e) and the Emergency Board Meeting Procedures adopted by the SMUD Board of Directors, the regular Board meeting and other public meetings are currently conducted solely via virtual (online/teleconference) meeting to align with state, local, and federal guidelines for the containment of the coronavirus.

Live video streams and indexed archives of meetings are available at:
http://smud.granicus.com/ViewPublisher.php?view_id=16

Members of the public may register to provide verbal comments at an upcoming Board or Committee meeting by emailing a request to speak to PublicComment@smud.org. Please include the date of the meeting, name, and topic or agenda item the requestor wishes to speak on. The request may also be submitted while the meeting is in progress during the standard time for the agenda item or topic. **Pre-registration is strongly encouraged by no later than 3:00 p.m. on the day of the meeting.**

Members of the public may provide written public comments on a specific agenda item or on items not on the agenda (general public comment) by submitting comments via e-mail. Comments may be submitted to PublicComment@smud.org and will be placed into the record of the meeting.

Members of the public that are listening to or watching the live stream of a Committee meeting and wish to comment on a specific agenda item as it is being heard may submit their comments, limited to 250 words or less, to PublicComment@smud.org, noting the agenda item number in the subject line. The Committee Chair may read comments for items on the agenda into the record, in his discretion, based upon such factors as the length of the agenda or the number of e-mail comments received. General public comment for items not on the agenda will not be read into the record but will be provided to the Board and placed into the record of the Board meeting if it is received within two hours after the meeting ends.

This Committee meeting is noticed as a joint meeting with the Board of Directors for compliance with the Brown Act. In order to preserve the function of the Committee as advisory to the Board, members of the Board may attend and participate in the discussions, but no Board action will be taken. The Policy Committee will review, discuss and provide the Committee's recommendation on the following:

ANNOUNCEMENT OF CLOSED SESSION AGENDA

1. **Threat to Public Services or Facilities.**

Pursuant to Section 54957 of the Government Code:

Consultation with: Laura Lewis, Chief Legal & Government Affairs Officer;
Stephen Clemons, Chief Innovation & Information Officer; and Antiwon
Jacobs, Director, Cybersecurity.

OPEN SESSION AGENDA

DISCUSSION ITEMS

1. Antiwon Jacobs
Rob Lechner
Jennifer Jackson Accept the monitoring report for **Strategic Direction SD-16, Information Management and Security.**
Presentation: 18 minutes
Discussion: 15 minutes
2. Russell Mills Accept the monitoring report for **Strategic Direction SD-17, Enterprise Risk Management.**
Presentation: 10 minutes
Discussion: 15 minutes
3. Laura Lewis Make findings pursuant to Government Code section 54953(e) to continue holding meetings virtually during proclaimed state of emergency (recurring item, every 30 days).
Discussion: 5 minutes

INFORMATIONAL ITEMS

4. Nancy Bui-Thompson Board Work Plan.
Discussion: 5 minutes
5. Public Comment
6. Heidi Sanborn Summary of Committee Direction.
Discussion: 1 minute

Pursuant to Resolution No. 20-06-08 adopted on June 18, 2020, Emergency Board Meeting Procedures are in effect:

Members of the public may make either a general public comment or comment on a specific agenda item by submitting comments via email. Comments may be submitted to PublicComment@smud.org.

Comments will be provided to the Board and placed into the record of the Committee meeting if it is received within two hours after the meeting ends.

Members of the public that are listening or watching the live stream of a Board meeting and wish to comment on a specific agenda item as it is being heard, may submit their comments, limited to 250 words or less, to

PublicComment@smud.org. The Board Chair may read the comments into the record, in her discretion, based upon such factors as the length of the agenda or the number of email comments received.

Comments will be provided to the Board and placed into the record of the Committee meeting if it is received within two hours after the meeting ends.

*Members of the public may register to provide verbal comments at an upcoming Board or Committee meeting by emailing a request to speak to PublicComment@smud.org. Please include the date of the meeting, name, and topic or agenda item the requestor wishes to speak on. The request may also be submitted while the meeting is in progress during the standard time for the agenda item or topic. **Pre-registration is strongly encouraged by no later than 3:00 p.m. on the day of the meeting.***

ADA Accessibility Procedures: Upon request, SMUD will generally provide appropriate aids and services leading to effective communication for qualified persons with disabilities so that they can participate equally in this virtual meeting. If you need a reasonable auxiliary aid or service for effective communication to participate, please email Toni.Stelling@smud.org, or contact by phone at (916) 732-7143, no later than 48 hours before this virtual meeting.

SSS No.
CYBER 21-001

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date Policy, November 17, 2021
Board Meeting Date November 18, 2021

TO	TO
1. Antiwon Jacobs	6. Farres Everly
2. Claire Rogers	7.
3. Jennifer Davidson	8.
4. Stephen Clemons	9. Legal
5. Brandy Bolden	10. CEO & General Manager

Consent Calendar	<input checked="" type="checkbox"/>	Yes		No <i>If no, schedule a dry run presentation.</i>	Budgeted		Yes	<input checked="" type="checkbox"/>	No <i>(If no, explain in Cost/Budgeted section.)</i>
-------------------------	-------------------------------------	------------	--	--	-----------------	--	------------	-------------------------------------	---

FROM (IPR) David Bitter	DEPARTMENT Cybersecurity	MAIL STOP E114	EXT. 6901	DATE SENT 11/5/2021
----------------------------	-----------------------------	-------------------	--------------	------------------------

NARRATIVE:

Requested Action: Accept the monitoring report for Strategic Direction SD-16, Information Management and Security.

Summary: Present the 2020-2021 Board Monitoring Report for SD-16, Information Management and Security.

Board Policy: SD-16, Information Management and Security.
(Number & Title)

Benefits: Provides an update to the Board of Directors on the progress and status of the Information Security, Privacy and Records Management programs.

Cost/Budgeted: N/A

Alternatives: N/A

Affected Parties: SMUD

Coordination: Cybersecurity

Presenter: Antiwon Jacobs, Jennifer Jackson, Rob Lechner

Additional Links:

SUBJECT Strategic Direction SD-16, Information Management and Security	ITEM NO. <i>(FOR LEGAL USE ONLY)</i>
---	--------------------------------------

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SACRAMENTO MUNICIPAL UTILITY DISTRICT

OFFICE MEMORANDUM

TO: Board of Directors

DATE: November 9, 2021

FROM: Claire Rogers *CR 11/9/21*

**SUBJECT: Audit Report No. 28007346
Board Monitoring Report; SD-16: Information Management and
Security**

Audit and Quality Services (AQS) received the SD-16 *Information Management and Security* 2021 Annual Board Monitoring Report and performed the following:

- A review of the information presented in the report to determine the possible existence of material misstatements;
- Interviews with report contributors and verification of the methodology used to prepare the monitoring report; and
- Validation of the reasonableness of a selection of the report's statements and assertions.

During the review, nothing came to AQS' attention that would suggest the SD Board Monitoring report did not fairly represent the source data available at the time of the review.

CC:

- Paul Lau

Board Monitoring Report 2021

SD-16, Information Management and Security



1) Background

Strategic Direction Information Management and Security Policy states that:

Proper management of cyber and physical information, as well as physical security, is a core value. Robust information management and physical security practices are critical to effective risk management and to ensure regulatory compliance, business resiliency and customer satisfaction. SMUD shall take prudent and reasonable measures to accomplish the following:

- a) **Information Security:** SMUD will protect customer, employee and third-party information, and SMUD information systems are protected from unauthorized access, use, disclosure, disruption, modification, or destruction.
- b) **Physical Security:** SMUD will safeguard its employees while at work as well as customers and visitors at SMUD facilities. SMUD will also protect its facilities and functions that support the reliability of the electric system and overall operation of the organization from unauthorized access or disruption of business operations.
- c) **Customer Privacy:** SMUD will annually notify customers about the collection, use and dissemination of sensitive and confidential customer information. Except as provided by law or for a business purpose, SMUD will not disseminate sensitive and confidential customer information to a third party for non-SMUD business purposes unless the customer first consents to the release of the information. Where sensitive and confidential information is disseminated for a business purpose, SMUD will ensure: (i) the third party has robust information practices to protect the sensitive and confidential customer information, and (ii) use of the information by the third party is limited to SMUD's business purpose. SMUD will maintain a process that identifies the business purposes for which SMUD will collect, use and disseminate sensitive and confidential customer information.
- d) **Records and Information Management:** SMUD will maintain the efficient and systematic control of the creation, capture, identification, receipt, maintenance, use, disposition, and destruction of SMUD records, in accordance with legal requirements and Board policies.

2) Executive summary

a) The Information Security, Physical Security, Privacy, and Records and Information Management programs and initiatives align directly with the “Value Our Customers and Community” and “Operational Excellence” points on SMUD’s North Star. These programs work towards ensuring that SMUD continues to be a good steward over customer information, physical security, privacy, and records in accordance with our customers’ high expectations.

b) SMUD is substantially in compliance with SD-16 Information Management and Security Policy.

c) Summary:

SD Requirement	Program/initiative /policy	Purpose	Outcome	Notes
Information Security: protect systems and information from unauthorized access	Information security program; AP 07.03.01 Information Security Concepts and Roles	Protect systems and information; provide policy supporting the Cybersecurity program	Closed door briefing to be held in November	Discuss security controls and processes in place to protect people, processes and technology
Customer Privacy: Annually notify customers about use of information	Annual notice of privacy practices	Notify customers of our privacy practices	Notice sent in the May bill package	Language updated to clarify when SMUD seeks customer consent
Customer Privacy: Ensure security where data is shared	System Security Plans and SOC 2 audit reports requirement	Evaluate the information practices and security controls of third parties	High confidence that vendors are using best practices to protect SMUD sensitive and confidential information	
Customer Privacy: Maintain a process that identifies purposes for information	Data Sharing Policy, Data Sharing Request/Approval Process	Track NDAs, the data being shared, and the business justification for sharing	Data Sharing process is being observed and maintained	

collection and dissemination				
Records & Information Management: Identify and manage records and information	Records Evaluations	Evaluate and classify records and ensure retrieval, disposal and protection.	On-track to meet 5-year plan of completing evaluations for entire enterprise.	
Records & Information Management: Ensure all information systems are compliant with RIM requirements and best practices.	Information System Evaluations	Review of software tools housing SMUD data and information.	Evaluate software tools for RIM compliance	RIM being added to software purchase process.
Records & Information Management: Education	Ongoing Enterprise training and Records Custodian Forums	Provide training to all of SMUD, with focused efforts on the Records Custodians	Annual training provided to all employees, with supplemental support, as needed. Also quarterly focused support for Records Custodians.	
Physical Security: safeguard employees, customers, and visitors	AP 06.03.01 Increase interoperability with local law enforcement agencies during critical incidents	Protect SMUD employees and those who visit SMUD facilities	Completing project to facilitate direct radio contact with local law enforcement agencies	SMUD Security Operations Supervisors and Dispatchers communicate in the field and via dispatch 24/7
Physical Security: protect SMUD facilities	AP 06.03.01 Physical Security Assessment(s) of SMUD physical properties and assets	Protect SMUD campuses and grid facilities through assessment and implementation of security-	Security Operations personnel continue to provide security evaluations for SMUD real properties.	Third-party Risk, Threat, and Vulnerability Analysis scheduled to begin Q1 2022

		industry best practices		
--	--	-------------------------	--	--

3) Additional supporting information

Information Security

SMUD, customer, employee and third-party information and SMUD information systems are protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

The Chief Innovation and Information Officer’s (CIIO) Cybersecurity group, under the direction of the Chief Information Security Officer, continues adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to establish prudent and reasonable measures intended to protect SMUD’s operations from a cyber-attack, disruption and other threats to enterprise technologies, processes and information. The CSF has five core functions (Identify, Protect, Detect, Respond, and Recover) which comprise both administrative and technical controls to effectively manage information and cybersecurity risk. Cybersecurity is actively working to implement the CSF measures to enhance information management and security risk management practices and processes in support of SD-16. Cybersecurity will highlight the cybersecurity capabilities provided in an update to the board for SD-16 during an upcoming closed session.

Physical Security

SMUD will safeguard its employees while at work as well as customers and visitors at SMUD facilities.

Physical Security worked with the Sacramento County Sheriff’s Department to obtain permission to utilize the Sacramento Regional Radio Communications System (SRRCS) in order to communicate directly with law enforcement agencies throughout SMUD’s service territory in the valley. This addition of a communications system that links directly to local law enforcement will facilitate nearly instantaneous responses from the agencies in the area when a critical incident occurs. This project is part of an overarching effort to better integrate with Local Law Enforcement Agencies (LLEA’s) who can provide the most effective support during critical incidents to ensure employee and visitor safety.

SMUD will also protect its facilities and functions that support the reliability of the

electric system and overall operation of the organization from unauthorized access or disruption of business operations.

Physical Security worked with a cross departmental group of stakeholders to put together a comprehensive risk report that outlined the existing vulnerabilities of the current Physical Access Control System, which is the first line of defense for protecting the bulk electrical system. This risk assessment was distributed to stakeholder directors and regulatory compliance. This document was authored to align with the NIST Cybersecurity Framework to assess the controls that are currently in place.

Physical Security is currently working on a project to provide the entire HQ Campus with a Risk, Threat, and Vulnerability Analysis (RTVA) conducted by a third party to examine the overall security posture as it currently exists. This RTVA will prove to be an invaluable tool to allow for the identification and mitigation of security-centric issues.

Security Operations personnel has also worked with the Substations team to formulate a process for continuously evaluating the security posture at substations throughout the valley. Security evaluations are conducted by Officers on patrol to ensure that the integrity of each inspected substation is maintained and then documented in a Security Operations repository.

Customer Privacy

SMUD will annually notify customers about the collection, use and dissemination of sensitive and confidential customer information.

SMUD sent out our annual privacy notice via email and as a bill insert to customers during the May bill cycle. The notice was updated this year to clarify we will ask for consent prior to using customer data for non-SMUD business purposes. The notice is otherwise very similar to previous years and continues to include plain language regarding SMUD's collection, use, and release of customer sensitive and confidential information, the business purposes for which customer information is used, as well as a reaffirmation of SMUD's commitment to customer privacy.

Except as provided by law or for a business purpose, SMUD will not disseminate sensitive and confidential customer information to a third party for non-SMUD business purposes unless the customer first consents to the release of the information.

No sensitive and confidential customer information has been sent to a third party for non-SMUD business purposes this year.

Where sensitive and confidential information is disseminated for a business purpose, SMUD will ensure: (i) the third party has robust information practices to protect the sensitive and confidential customer information, and (ii) use of the information by the third party is limited to SMUD's business purpose.

Cybersecurity and Procurement continue to follow a formalized supply chain risk management process, in compliance with NERC CIP requirements. The process is aligned to the NIST Cybersecurity Framework (CSF) and is reviewed on at least an annual basis to ensure it is functioning as designed and incorporates lessons learned as new procurements follow the process. The process includes a mandatory procurement requirement for vendors to allow the Cybersecurity team to evaluate the security posture of a proposed vendor solution. The American Institute of CPAs (AICPA) Service Organization Control 2 (SOC 2) Type 2 continues to be our procurement standard as it is an independent assessment focused on a solution's security controls which includes tests of the security controls' efficacy. SOC 2 Type 2 reports provide staff confidence that vendor security controls are robust and sufficient to protect SMUD information. Contract and non-disclosure agreement language is used to provide assurance that SMUD provided sensitive and confidential information will not be used for any unapproved purposes.

SMUD will maintain a process that identifies the business purposes for which SMUD will collect, use and disseminate sensitive and confidential customer information.

MP 07.03.01.122 - Data Sharing requires an approved data sharing request prior to sharing information with a third party for SMUD business purposes. The request form requires the identification of the data categories to be shared and the business justification that requires the sharing of data. This facilitates an approval process which includes the requester's management, Supply Chain, the Data Governance Program Manager, the data owner(s), and Cybersecurity. There were no significant changes to the process this year.

Records and Information Management

The efficient and systematic control of the creation, capture, identification, receipt, maintenance, use, disposition, and destruction of SMUD records, in accordance with legal requirements and Board policies.

The Records and Information Management (RIM) Program is making continued progress toward our 5-year plan of completing record evaluations for all business areas; we are currently in year 3, and projecting completion by year 5. We have streamlined our evaluation processes to make the identification of gaps, and implementation of compliant solutions, easier and faster. These changes provide us with a high level of confidence that SMUD records will be identified and managed appropriately once this effort is complete.

The RIM Program successfully implemented MP 07.02.01.102, Electronic Communications Retention, around management of emails, chats and electronic recordings.

The RIM program is continuing to partner with IT to review and support new software integrations to ensure they meet records policies and information management requirements. This is imperative as new software often produces and stores records outside of official repositories. RIM is being added to the purchase approval process to support this effort.

The RIM Program continues to collaborate with the Microsoft 365 Governance Oversight team, Cybersecurity, the CIP Program, Data Governance, and other business partners to ensure compliance with records policies and information management requirements.

4) Challenges

Information Security

As the news continues to keep cybersecurity threats and data breaches at the top of mind for people, legislators and regulators continue to look at ways they can appease constituents by proposing new and revised compliance requirements. SMUD Cybersecurity is actively engaged in understanding and managing compliance activities related to these legal and regulatory requirements.

Our PCI compliance related transaction volumes continue to increase, although SMUD is still a Level 2 Merchant. SMUD is again compliant this year as determined by an independent third-party PCI Qualified Security Assessor. Our required assessment documents were submitted to Chase Paymentech in July.

The Cybersecurity team continues to ensure compliance with updated Critical Infrastructure Protection (CIP) standards as well. This year SMUD commissioned an independent assessment team to perform a mock audit of our compliance with the CIP standards. The team worked with internal and external stakeholders to ensure our

ability to demonstrate compliance to the standards to prepare for our official audit scheduled for Q3 2022.

In addition to the compliance related work that results from the breaches in the news, SMUD Cybersecurity has also continued to mature our Incident Response capabilities, now a part of a larger Cybersecurity Emergency Operations Program (CEOP). The CEOP published an Enterprise Cybersecurity Incident Response Plan (CIRP) in April 2021 and conducted SMUD's first enterprise-wide cybersecurity incident response exercise in August 2021. The program plan met all test objectives and validated capabilities in place to respond to a cyber incident. In the past, SMUD only tested cyber incident response capability for its North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) regulated environment.

Physical Security

Physical Security is the first line of defense to safeguard SMUD's employees and visitors, as well as SMUD's assets, facilities, and infrastructure. Due to our 'open campus' construct, Physical Security will continue to experience challenges in preventing unauthorized persons from entering SMUD property and buildings. Physical Security continues working to limit unauthorized physical access to SMUD.

Security's role of 'First Responder' to cyber incidents is reinforced through training, mentorship on the job by senior officers, and a thorough understanding of the processes and procedures that provide understanding of SMUD's needs during a possible cyber incident. Through a constant improvement process, the need to replace our current system that is used to monitor, detect, and respond to possible events occurring throughout the SMUD enterprise was identified. Via that same process, the current security-centric policies were identified as being in need of refinement and a better communication of those policies and procedures to all SMUD employees was highlighted.

Customer Privacy

SMUD continues to see requests for SMUD customer data to be used and shared for additional purposes and programs, including customer personally identifiable information (PII). Requests for such data have come from internal programs, state agencies and vendors. SMUD's Data Sharing Policy and process are in place to provide request tracking and approval to ensure that all sharing of PII is authorized and performed using a secure transfer mechanism.

5) **Recommendation**

It is recommended that the Board accept the Monitoring Report for SD-16 Information Management Policy Monitoring Report.

6) **Appendices**

Definitions and acronyms:

NIST – National Institute of Standards and Technology

CSF – Cybersecurity Framework

RTVA – Risk, Threat, and Vulnerability Assessment

LLEA – Local Law Enforcement Agency

SRRCS – Sacramento Regional Radio Communications System

CEOP – Cybersecurity Emergency Operations Program

CIRP – Cybersecurity Incident Response Plan

SSS No. TR21-005

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date Policy – 11/17/21
Board Meeting Date November 18, 2021

TO		TO	
1.	Russell Mills	6.	
2.	Brandy Bolden	7.	
3.	Farres Everly	8.	
4.	Jennifer Davidson	9.	Legal
5.	Stephen Clemons	10.	CEO & General Manager

Consent Calendar	<input checked="" type="checkbox"/>	Yes	No <i>If no, schedule a dry run presentation.</i>	Budgeted	<input checked="" type="checkbox"/>	Yes	No <i>(If no, explain in Cost/Budgeted section.)</i>
FROM (IPR)	DEPARTMENT			MAIL STOP	EXT.	DATE SENT	
Toni Hoang	Treasury and Risk Management			B355	6532	10/25/21	

NARRATIVE:

Requested Action: Accept the monitoring report for Strategic Direction SD-17, Enterprise Risk Management.

Summary: The Enterprise Risk Management Report summarizes the activities that have occurred since the December 2020 annual report. The report includes historical risk profiles of enterprise risks which are not currently within management’s risk objectives, the 2022 mitigation strategies and a current residual risk exposure status of all identified enterprise risks.

Board Policy: *(Number & Title)* SD-17 Enterprise Risk Management. Effectively balancing and managing risk to further SMUD’s policy and business goals is a core value of SMUD. SMUD will implement and maintain an integrated enterprise risk management process that identifies, assesses, prudently manages and mitigates a variety of risks facing SMUD, including financial, supply, operational, physical and cyber security, climate change, legal, legislative and regulatory, and reputational risk.

Benefits: SD-17 Enterprise Risk Management. Effectively balancing and managing risk to further SMUD’s policy and business goals is a core value of SMUD. SMUD will implement and maintain an integrated enterprise risk management process that identifies, assesses, prudently manages and mitigates a variety of risks facing SMUD, including financial, supply, operational, physical and cyber security, climate change, legal, legislative and regulatory, and reputational risk.

Cost/Budgeted: N/A

Alternatives: N/A

Affected Parties: Board of Directors, Customers, Employees, SMUD Operations

Coordination: Enterprise Risk Management activities are closely coordinated enterprise-wide throughout SMUD.

Presenter: Toni Hoang

Additional Links:

SUBJECT Strategic Direction SD-17, Enterprise Risk Management	ITEM NO. (FOR LEGAL USE ONLY)
--	--------------------------------------

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SACRAMENTO MUNICIPAL UTILITY DISTRICT

OFFICE MEMORANDUM

TO: Board of Directors

DATE: November 9, 2021

FROM: Claire Rogers *CR 11/9/21*

**SUBJECT: Audit Report No. 28007347
Board Monitoring Report; SD-17: Enterprise Risk Management**

Audit and Quality Services (AQS) received the SD-17 *Enterprise Risk Management 2021 Annual Board Monitoring Report* and performed the following:

- A review of the information presented in the report to determine the possible existence of material misstatements;
- Interviews with report contributors and verification of the methodology used to prepare the monitoring report; and
- Validation of the reasonableness of a selection of the report's statements and assertions.

During the review, nothing came to AQS' attention that would suggest the SD Board Monitoring report did not fairly represent the source data available at the time of the review.

CC:

Paul Lau

Board Monitoring Report 2021

SD-17, Enterprise Risk Management



1. Background

Strategic Direction 17 states that:

Effectively balancing and managing risk to further SMUD’s policies and business goals is a core value of SMUD.

Therefore:

SMUD will implement and maintain an integrated enterprise risk management process that identifies, assesses, prudently manages, and mitigates a variety of risks facing SMUD, including financial, supply, operational, physical, and cyber security, climate change, legal, legislative, and regulatory, and reputational risk.

2. Executive summary

- a) SMUD strategically manages risk to proactively reduce the chance of loss, identify and take advantage of opportunities to create greater financial stability and protect our resources to support SMUD’s mission and create value for our customers.
- b) **SMUD is in compliance with the Board’s Strategic Direction 17 (SD-17) Enterprise Risk Management.**
- c) SMUD continues to maintain an integrated Enterprise Risk Management (ERM) Program. The program was evaluated by a third party and a plan is being developed to implement recommendations to support the achievement of the Board’s Strategic Directions.

SMUD’s ERM program continues to integrate risk management best practices to support decision making in key business processes. This year we have expanded the reliance on the risk framework for prioritization, planning, and budgeting.

Since the 2020 Annual Monitoring Report, staff continues to review SMUD’s portfolio of risks. The Year-on-Year Residual Risk Exposure results are summarized as follows:

			Nov. 2019	Dec. 2020	Nov. 2021
✓	“Red”:	Extremely High Residual Exposure	(0)	(0)	(0)
✓	“Orange”:	High Residual Exposure	(4)	(4)	(5)
✓	“Yellow”:	Medium Residual Exposure	(33)	(36)	(40)
✓	“Green”:	Low Residual Exposure	(40)	(38)	(38)
✓	“Blue”:	Extremely Low Residual Exposure	(0)	(0)	(0)
			(77)	(78)	(83)

Since the 2020 Board Monitoring Report, there has been 5 new risks added to the enterprise risk portfolio. Staff continues to implement risk mitigation strategies to balance residual risk exposures. Some risks, while medium or “yellow” are within the risk management goal. There are currently 46 risks, shown in the last two lines of the table, which are within the risk management goal.

Attachment A outlines the actions that will be taken to address risks that are not at target.

Current Residual Risk Exposure	Risk Management Goal	Number of Risks
Orange “high”	Yellow “medium”	5
Yellow “medium”	Green “low”	32
Yellow “medium”	Yellow “medium”	8
Green “low”	Green “low”	38

SMUD’s enterprise-wide risk exposure is a medium/high. SMUD’s ambitious 2030 goal, evolving technologies, the increasing pace of change in the utility business environment, skilled workforce scarcity, and increased legislative/regulatory requirements are key components that could impact SMUD’s risk profile in the upcoming years. Staff continues identify risks and implement initiatives to mitigate and manage risks appropriately.

3. Additional Supporting information:

a) Summary of 2021 activities

In 2021, ERM continued to support the organization with facilitating risk conversations and providing a risk framework for uniformed risk assessments across the organization. The overarching goal is to encourage the integration of risk-based thinking into decision-making at all levels, effectively balancing risks with opportunities.

ERM continues to utilize four existing committees to enhance cross-functional discussion and thorough understanding of major risk issues at the executive and operational leadership team level. One of these is an executive level oversight committee, the Enterprise Risk Oversight Committee (EROC) which includes multiple executives. The other three are the Trading Operations Risk Committee (TORC), Zero Carbon Plan Implementation Team, and the Three Lines Working Team.

2021 continues to bring changes and challenges. Despite the many challenges, staff continues to leverage the enterprise risk management framework to support enterprise-wide risk management/mitigation activities bringing positive outcomes for SMUD, our customers and the community. Some samples of these activities include:

ERM Program Evaluation

In early 2021, a third party reviewed SMUD’s ERM Program. They identified some of the program’s strengths to include far-sighted risk management vision, good program oversight, risk ownership in key business areas, risk-based planning, and information classification. Areas of opportunities identified include having more risk reward trade-off discussion, deepen understanding of risk interdependencies and viewing risks as opportunities, not just “bad risk.” Staff is currently developing a plan to implement the recommendations and work collaboratively across all areas to improve risk culture.

North American Electric Reliability Corporation (NERC) Compliance Mock Audit

SMUD conducted a mock audit of our compliance with selected NERC reliability and security standards that pose high risks to Bulk Electric System operations. The mock audit scope included NERC’s Critical Infrastructure Protection (CIP) and Operations and Planning (O&P) standards.

The exercise focused largely on how SMUD performs activities that lead to compliance with regulatory obligations, as well as identifying whether we achieved compliance. The purpose of the NERC standards is to ensure reliable operations, as merely demonstrating historical compliance is sometimes not enough. SMUD recognizes that compliance and reliability objectives are not always aligned, as the former can at times be achieved through a “check the box” approach while the latter is achieved by a job consistently well done. This mock audit was successful in helping the organization identify areas to improve. The exercise increased our ability to communicate internally and to regulatory authorities how and why our collective performance can reduce operational risks while also meeting the reliability and security standards.

Budget Risk Prioritization

Staff continues to leverage the enterprise risk management framework to optimize resource allocation to help build resiliency against future impacts and capacity for future activities in support of SMUD’s climate goals. In 2021 staff conducted a pilot effort to develop a process to facilitate decision making and prioritization at the executive level to ensure that the organization and resources are aligned to appropriately manage risks to the acceptable levels. Staff continues to refine these efforts and reinforces its importance with the hiring of an Enterprise Prioritization Manager. Staff has formed a core team to further expand upon the pilot efforts to be implemented for planning in 2022 and will continue to be refined in future years.

2030 Zero Carbon Plan

Climate change is a pressing issue facing our region and the world. On April 28, 2021, SMUD’s Board solidified SMUD’s commitment to leading the way to a clean energy future with the approval of our 2030 Zero Carbon Plan (Plan). The Plan is a flexible pathway to eliminate carbon emissions from our power supply by 2030, the most ambitious goal of any large utility in the country. The Plan demonstrates our commitment to finding innovative ways to reach our zero-carbon goal without impacting reliability, or rates, which are among the lowest in California. To pay for new technologies and make them available to customers in an equitable manner, we’ll aggressively pursue partnerships, investors, and grant funding, while keeping our rate increases at or below inflation. In 2021, staff continues to conduct and review reliability studies to ensure that reliability levels are maintained and look for ways to limit rate increases through cost offsets from operational efficiencies and grants/partnerships.

Cybersecurity

Since 2019, SMUD has strategically implemented measures to manage cyber risk to operations from a cyber-attack, disruption, and from other threats to its’ technology and information. The Enterprise Cybersecurity Emergency Operations Program was established to bolster SMUD’s ability to respond to cyber incidents. The Chief Information Security Officer appointed a dedicated Program Manager to oversee this crucial resilience capability. In May 2021, the Program Manager published an enterprise Cybersecurity Incident Response Plan and in August 2021, SMUD conducted its first enterprise-wide Cybersecurity Incident Response Exercise. In the past, SMUD only tested incident response capability for its NERC CIP regulated environment. Moving forward SMUD will conduct at least two exercises each year, one for the enterprise as a whole and one for our regulated assets to meet our NERC CIP compliance obligations.

The August 2021 exercise highlighted SMUD’s ability to utilize incident response plans and playbooks which outline specific actions to be taken during a real incident. Over 30

individuals participated in the exercise and an additional 70 observed, including multiple levels from individual contributors up to and including executives.

The Program Manager is responsible for cybersecurity incident management, including planning, coordination, communication, and oversight during an actual cyber incident. To further mitigate risk to the enterprise, this cybersecurity capability is integrated and collaborates with SMUD's enterprise Emergency Operations function.

Risk exposure monitoring and continuous updates: Staff continues to monitor and update any changes to existing and emerging risks and their impacts to residual risk. In addition, audit results and management responses are considered in the ERM assessment plan and reporting process. The audit plans are linked with the enterprise risk assessments to provide assurance that mitigation measures for critical risks are being implemented effectively and in a timely manner.

- In 2021, 6 audit reports were reviewed by the ERM Office, and none resulted in a change to the risk profile.

Noteworthy enterprise risk profile changes are included in regular Board reporting.

- Attachment A summarizes the “Year-on-Year Profile Changes,” for all enterprise risks currently not within risk management goal. The attachment includes year-on-year changes, current “risk trend,” and actions staff is taking to reach the “target”; which could be either low “green” or medium “yellow.”

- b) Benchmarking: Staff reviews available enterprise risk related information and incorporates new risk issues and/or expands existing risk issues where appropriate. North Carolina State University's (NCSU) Enterprise Risk Management Initiative and Protiviti continue to jointly publish benchmark information. The joint study, 2021 & 2030 Executive Perspectives on Top Risks, provides insight for short-term and long-term risks from 1,081 global board members and executives from across several industries. The study found that for 2021, COVID-19 was the driver of most top risks' organizations were concerned about the impact of the ongoing pandemic on government policies and regulations to their business model and operations. Overall, the top ten identified enterprise risk issues across the surveyed organizations and those specific to the Energy and Utility Industry (Utility Industry) and its trend analysis is consistent with SMUD's identified enterprise risks.

An analysis of SMUD's enterprise risks as compared to the top 10 enterprise risks identified by the study is outlined in Attachment B.

- c) Looking forward

In 2022, staff will develop and implement recommended changes to the enterprise risk management program and further integrate risk management practices into business processes to build a more risk aware culture. The following initiatives have been planned:

- Begin implementing third party recommendations to further enhance the ERM program.
- Form the Risk Champion Network (RCN), a forum of Director level risk champions to sponsor risk initiatives across the organization.
- Integrate risk into enterprise prioritization process.
- Continue to:

- Be vigilant in identifying and reporting on risks across the organization
- Leverage risk process to help build resiliency and future capacity in financial planning and prioritization; expanding upon approaches used for the 2021 budget plan
- Prioritize spending to be within limits needed to achieve no more than inflation level annual rate increases
- Support 2030 Zero Carbon Plan
- Support Enterprise Prioritization process
- Support initiatives for the management of cyber risk with vendors
- Support physical security risk assessments
- Test and strengthen SMUD's response to risk events
- Improve safety performance to meet SD-6 Safety DART goal
- Continue to improve upon wildfire mitigation activities/programs where appropriate
- Positively influence state and federal legislative/regulatory issues
- Attract and retain a skilled and innovative workforce
- Provide programs and services which reflect the customer's changing expectations
- Enhance data categorization and availability to support business and customer decisions
- Continue cyber security and privacy awareness and compliance activities
- Improve upon current physical security and public safety practices
- Increase alignment between costs and revenue collection in SMUD's rate design

4. Challenges: Global challenges posed by the ongoing COVID-19 pandemic, occurrences of wildfires throughout the region and market uncertainty continue to put strain on business operations and critical resources. The risk environment continues to challenge staff to be vigilant at making more measured risk informed decisions to achieve business objectives. By leveraging the ERM framework and existing data analytics tools, staff can better manage risks as a portfolio, rather than in silos. The result is increased awareness of SMUD's risks, the level-setting of risk tolerance across the enterprise, efficiencies in mitigation efforts as well as potential cost savings.

5. Recommendation: It is recommended that the Board accept the Monitoring Report for SD-17 Enterprise Risk Management.

Enterprise Risk Mitigations for Risks Currently not within Target

Risk Category	Risk	Year on Year Profile			Risk Trend	Target	2022 Risk Mitigation
		2019	2020	2021			
Financial	Load variation: customer owned generation						SMUD gained approval of the 2030 Zero Carbon Plan, which illustrated expected growth of behind the meter distributed generation and storage, with ranges of 500-750MW of behind the meter solar and 50-250MW of behind the meter storage. In addition, the Board approved the new solar & storage rate as a successor to NEM 1.0. The implementation of this new rate in March 2022, coupled with the launch of both a critical peak pricing offering for solar & storage as well as a virtual power plant option for solar & storage will help inform the reliability, cost-effectiveness, and resource characteristics of distributed solar & storage's contribution towards our 2030 ZCP goal.
	Project execution						The Project Portfolio Management tool, using the ServiceNow platform, went live in 2021 and was used for capturing all capital projects for the 2022 budget. This streamlined the level of effort for executive decision making and discussion, as the tool could be used to provide summary information rather than it having to be manually created. Work is continuing building reports for the tool and incorporating the data so that it can be used with PowerBI for other reporting. With the realignment, project changes need to be approved by the sponsor's executive. With the centralization of PMO's (IT & Non-IT) and the soon to be created 2030 Zero Carbon Plan PMO, staff is working with the Project Management Office's to create standards and expectations and clarification of roles as we move forward.
Operational: People	Employee safety						SMUD continues support a Safety for Life culture throughout the organization with an emphasis toward zero incidents and injuries. This year Safety updated Strategic Direction (SD)-6 to include a new metric for Days Away, Restricted Time or Job Transferred (DART) and a contractor safety emphasis. The new DART metric is a limit of 13 over the next 5 years. In addition, SMUD continues to develop and support COVID-19 standards and guidelines to protect employees, contractors, and the public. Safety is supporting Facilities for the safe re-entry of remote employees back in the building during first quarter of 2022. Safety continues to expand its contractor safety program by screening contractors providing high risk work, conducting improved onboarding, and increasing field visits. In 2022, Safety is expanding its pilot field ergonomics program;

Enterprise Risk Mitigations for Risks Currently not within Target

						expanding its Safety Management System (SMS) modules; improving public safety training for Emergency Response Personnel; updating our Safety Road Map goals with Directors for 2022; working with HR to include an improved safety goal in PAS performance evaluations; and updating our Wildfire Smoke Health program. Lastly, Safety is continuing to update and assist business units with safety standards.	
	Strategic workforce agility						<p>While some business units did conduct activities, due to pandemic, uncertain finances resulting in hiring constraints and the work required for a successful realignment, formal Strategic Workforce & Succession Planning work was paused. Q4 of 2021 work includes completion of a plan to reengage these needed programs with the organization in Q1 of 2022. Plan will include increased executive support and accountability measures.</p> <p>2022 activities include the launch of Strategic Workforce Planning and Succession Planning programs with enhanced senior leadership support, accountability measures and specific to critical roles at SMUD.</p>
	Diversity, equity, and inclusion						<p>Most significant outcome in 2021 was the realignment and establishment of Executive level diversity officer and formation of a separate Diversity, Equity, and Inclusion (DEI) function – separating it from the Human Resources department. It is anticipated a Director of DEI will be in place by the end of 2021. Other significant work included the creation of a new DEI Strategy with three focus areas: Diverse Workforce, Inclusive Culture and Community Impact. Each of these areas have strategies, tactics, and measures of success to create a detailed roadmap with finalization by end of 2021.</p> <p>To mitigate this risk the implementation of the DEI Strategic Roadmap will occur throughout 2022.</p>
Operational: Systems and IT	Cyber security						<p>In 2020, The Cybersecurity Department continued to strategically implement measures to manage cyber risk to operations from a cyber-attack, disruption, and other threats to SMUD’s technology and information. Maturing our implementation of the National Institute of Standard and Technology (NIST) Cybersecurity Framework (CSF) is the cornerstone the departments risk reduction initiatives to protect SMUD’s people, processes, and technology. Important to note, these risk measures are critical to SD-16 and encompasses Information Security and other</p>

Enterprise Risk Mitigations for Risks Currently not within Target

<p>major components such as privacy, data security, supply chain security, and business applications and cloud security.</p> <p>The department has successfully implemented planned 2020 cyber risk reduction initiatives and improved maturity across multiple CSF subcategories. In 2021 the department will:</p> <p>Continue to mature its implementation of CSF in accordance with organizational policy (AP 07.03.01). Cybersecurity Operations red team/penetration test capability will improve on how they identify and manage asset vulnerabilities with the integration of ServiceNow (Security Operations) module. This capability is aligned to the framework’s control set “Identify Risk Assessment - (ID.RA-1)”.</p> <p>The Program Manager for Enterprise Cybersecurity Emergency Operations Program in May 2021 published an enterprise Cybersecurity Incident Response Plan. August 2021, SMUD conducted its first enterprise-wide Cybersecurity Incident Response Exercise. In the past, SMUD only tested incident response capability for its NERC CIP regulated environment. In 2022 the PM will conduct at least two exercises each year, one for the enterprise as a whole and one for our regulated assets to meet our compliance obligations.</p> <p>Staffing risk for 2021 (Recruitment, Retention, and Compensation not competitive with industry) has impacted and will continue to impact the ability to mature overarching Cybersecurity Program Maturity in 2022. In 2021, the department added two new staff and promoted 2 part-time staff to full-time assets (built talent from STEM Internship program). PS&S Compensation and Class has added a 5% non-PERS premium to help with retention of current staff. Recruiting actively for four positions to help protect all SMUD’s technology and information assets; candidates have declined offer of employment due to compensation and has been a trend for the last 2 years.</p> <p>Continued to collaborate with Technology and Innovation Infrastructure and Operations & Applications departments to further implement Microsoft (MS) 365 Multifactor Authentication (MFA) on premise and to increase capability for remote patching of SMUD’s endpoints to better manage vulnerabilities and provide better protections as result of COVID-19 impacts.</p>
--

Enterprise Risk Mitigations for Risks Currently not within Target

<p>2021 policy refresh effort to mature our program and assist with implementing critical security controls across our IT and OT environments will be completed by end of year. The refresh will result in an updated set of cybersecurity policies, procedures and standards that are aligned to the NIST CSF and the NIST 800-53 Security and Privacy Control families. In 2022, enforcement of these policies will begin leveraging ServiceNow Governance, Risk, and Compliance modules and other program processes such as audit and assessments.</p> <p>In 2022 the program will continue to conduct vendor risk assessments as part of procurement processes for enterprise supply chain risk management.</p> <p>In 2021, staff began documenting cybersecurity awareness, training, and education program to support managing cyber risk across the enterprise for all staff and those in privileged technology and information management positions.</p> <p>In 2021 collaborated with the Chief Financial Officer (CFO) organization and external consultancies determine the need and ultimately landed on the determination to increase Cyber insurance coverage limit for 2022. Increased from \$40M to \$60M.</p> <p>In 2021 staff continued working to finalize system integration of two new technical solutions to mature our cybersecurity governance, risk, and compliance program and security operations program. These technologies are on track to be integrated on time. These systems will enhance SMUD's technology project and engineering practices and ensure we are implementing effective cybersecurity policy and practices to protect our information confidentiality, integrity, and availability. The GRC technology will also begin to help with attesting SMUD's control implementation in support of CFO creditor requirements, Payment Card Industry Compliance, and other business partnerships SMUD will consider for 2030 Clear Carbon goals and objectives.</p> <p>In 2022 will continue to explore implementation of the NIST Risk Management Framework (RMF) from an organizational and system-level perspective to establish the context and priorities for managing cyber and privacy risk within SMUD's notional System Development Lifecycle (includes cloud solutions and applications). The RMF will introduce repeatable processes that will enhance risk mitigation and support the Enterprise Risk Management (ERM) Program, Data Governance,</p>











Enterprise Risk Mitigations for Risks Currently not within Target

						<p>Business Strategy and Requirements, IT Strategy and Governance, and Project and Procurement Lifecycles. In 2021, worked with a consultant to help design an RMF process and how it could be implemented on our GRC technology platform.</p> <p>In 2022, the cybersecurity department will continue to champion and advocate for cyber risk reduction activities to be integrated in technical and programmatic efforts needed to support critical business capabilities (to account for items such as business continuity, disaster recover, physical security, new business application developments) and requirements. The goal is to ensure cyber, and privacy are baked in early to avoid risk to business cost, schedule, and performance of SMUD’s operational business requirements.</p> <p>IN 2022 North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standard requirements compliance Audit conducted by the Western Electricity Coordinating Council (WECC). In 2021, the department collaborated with RC&C to conduct a Mock Audit to reduce non-compliance risk for 2022 audit. The Mock Auditors observed risk to compliance and the CIP Program within the cybersecurity department has begun addressing with responsible requirement owners, e.g., Physical Security and OT Security)</p>
Privacy						<p>In 2021 SMUD continues to see demand for SMUD customer data to be used and shared for additional purposes and programs, including customer personally identifiable information (PII). Requests for such data have come from internal programs, state agencies and vendors. SMUD’s Data Sharing Policy and Process are in place to provide request tracking and approval to ensure that all sharing of PII is authorized and performed using a secure transfer mechanism.</p>
Data governance						<p>In 2021 the Data Governance Program weathered a hit due to COVID and part-time resource allocation evidenced by a continuation of the expansion for data accountability. This was achieved with the identification of new data owners and data leads within multiple business units then incorporating them in decisions for issue resolution and data sharing agreements. In support of our Strategic Directions, Management Policies, Administrative Procedures, and other risk mitigation initiatives, the data sharing process was incorporated into well-established enterprise</p>

Enterprise Risk Mitigations for Risks Currently not within Target

							<p>processes resulting in improvements in transparency for data shared with third parties and an uptick in the number and scope of requests received.</p> <p>In 2022 a full-time Data Governance Program Manager will be onboarded and leading the categorization of additional data sets, identification of owners and leads, establishing additional governance processes, and classifying data sets to be incorporated into the NIST Risk Management Framework.</p>
	Enterprise-wide documentation						<p>Records and Information Management will work with IT and the Business Units to address and implement solutions for the findings identified in completed records evaluations. The group will also continue to perform records evaluations across the remainder of business units, as well as continue refining and simplifying the evaluation process itself.</p>
	Technology systems infrastructure						<p>Hybrid Workforce Experience: Continued efforts to provide an ideal technology experience for our workforce are underway as we look towards our goal of re-entry into our SMUD facilities and a continuation of hybrid work occurring remote and on-premises.</p> <p>Disaster Recovery: While key and critical systems at SMUD have multiple safeguards in place to remain available in the event of a disaster (backups replicated to alternate sites, application failover to alternate sites), we will continue to partner with business continuity to align business continuity plans which call for technology to align with the systems availability requirements in our data centers and cloud footprints. We also are looking to have a scheduled cadence of disaster recovery drills for key and critical systems identified.</p>
Operational: Process	Gas & gas pipeline assets						<p>Staff has completed the analysis of all results from 2018's full Internal Line Inspection (ILI) of the entire pipeline system. The next ILI is due in 2025 but will be planned for 2024 at the latest.</p> <p>In 2022, SMUD staff intends to continue our program of emergency response plan exercises with first responders and outside agencies in both Sacramento and Yolo Counties; continue to perform multiple community outreach events to reduce or eliminate the number of unplanned excavations within or near SMUD's gas pipeline easements; and continue to diligently inspect and patrol the SMUD gas pipeline and all easement areas, including leak and density surveys.</p>





















Enterprise Risk Mitigations for Risks Currently not within Target

Enterprise continuity management						In 2022, staff will work to implement Enterprise Continuity Management Software (ECMS) solution to support efficient access to real-time business continuity plan information and requirements during events that pose a threat to SMUD's continuity.
Internal communications and alignment						<p>Speed of Trust: 100% of Supervisors and Managers have completed Leading at the Speed of Trust (SoT) Key Concepts class by 7/31/21. All leaders have a goal to use the SoT concepts and Huddle Guide in their teams to develop trust behaviors by 12/31/2021. 100% of SMUD Leaders complete the actions in their inclusion goal by 12/31/2021 that demonstrate commitment to an inclusive culture, where employees have a sense of belonging and can contribute and thrive. 100% of SMUD leaders complete the actions in their inclusion goal by 12/31/2021 that demonstrate commitment to an inclusive culture, where employees have a sense of belonging and can contribute and thrive.</p> <p>Engagement Survey: SMUD's engagement survey will take place in Q4 of 2021. The survey is an opportunity for leaders to listen and understand employees' experiences and how it affects engagement, as well as inclusion and belonging. One new element in the survey this year is more robust organizational-level reporting on a set of questions that will help us understand where we have meaningful differences between populations on important aspects of inclusion at SMUD, specifically: voice, growth, belonging and commitment.</p> <p>To continue work on reducing risk the most important part of the 2021 employee engagement survey will take place in 2022 which is deciding what meaningful steps SMUD and SMUD leaders can and will take, in our teams and as an organization once we review employees' feedback. We expect all leaders will use survey results to set an engagement goal as part of their 2022 workplans, which they will complete in Q1 2022.</p> <p>Communication across the organization will continue surrounding the robust CEV, activities, outcomes with regular connection to the reasons for the vision.</p> <p>To continue work on reducing risk the most important part of the 2021 employee engagement survey will take place in 2022 which is deciding what meaningful steps SMUD and SMUD leaders can and will take, in our teams and as an organization once we review employees' feedback. We</p>











Enterprise Risk Mitigations for Risks Currently not within Target

						<p>expect all leaders will use survey results to set an engagement goal as part of their 2022 workplans, which they will complete in Q1 2022.</p> <p>Communication across the organization will continue surrounding the robust CEV, activities, outcomes with regular connection to the reasons for the vision.</p>
Energy management center (EMC)						Facilities is continuing to implement key projects within the EMC that help reduce the risks to day-to-day operations
Backup control center (BCC)						The Project, Implementation of the BCC Interim Response Plan is in execution and is scheduled to be completed by Q2 2022.
Headquarter building						Per the agreement with the City of Sacramento, the project was to be implemented in 3 phases. Phase One was completed in 2021 with Phase 2 and Phase 3 schedule for execution in 2022 and 2023 respectively.
Physical asset security						Low-Impact Security requirements have been implemented and Security continues to monitor sites and works to align the security plan to the One SMUD vision. The conversion to digital security cameras at campus locations is complete and the conversion at Substations is currently scheduled to be completed in Q4 2023. SMUD Security Operations will be conducting a Risk, Threat, and Vulnerability Assessment of the Headquarters Campus via a third-party vendor to commence Q1 2022 and end Q2-Q3 2022. Recommendations from the vendor will be available to SMUD in Q3 2022. SMUD currently does not have a comprehensive physical security/asset protection program or the documentation and policy/procedure guidance in place to articulate successful protection of physical assets. It is recommended that SMUD mitigate this by ensuring adequate protection measures are implemented under the guidance of a new risk-based assessment program to demonstrate active and ongoing protection of defined assets.
Transmission and distribution substation assets						Staff is on track with its multi-year replacement plan for T&D substation assets which include circuit breakers, transformers, and switchgears. Critical assets were identified and prioritized for replacement. The 2022 budget and capital portfolio include projects to replace two distribution transformers, three transmission circuit breakers and eight 69kV circuit breakers.

Enterprise Risk Mitigations for Risks Currently not within Target

Operational excellence						<p>The expected OpEx Program outcomes will be used to mitigate financial risks. Staff will focus on:</p> <ul style="list-style-type: none"> • Identifying and execute cost savings to fund strategic investment areas; • Increasing efficiency and productivity across the enterprise; • Developing and managing an enterprise-wide portfolio of OpEx initiatives and results; and • Building organizational competencies for continuous improvement
Pricing rate design implementation						<p>The SMUD Board unanimously voted on Sept. 16, to approve the rate package which included rate increases for all customers in the amount of 1.5% effective March 1, 2022, and 2.0% effective January 1, 2023, a new solar and storage rate for new solar customers who generate energy on-site and/or store energy and an optional critical peak pricing rate for residential customers to help when the grid is most stressed. The rate package also included \$25M in supporting programs to accelerate the adoption of storage. Staff is also working on a new Virtual Solar Program (VNEM) for under-resourced multi-family dwelling communities effective June 1, 2022. As of the date of this update, the implementation work is on track with minimum risk to meet the adopted deadlines.</p>
CPUC General Orders						<p>A project to automate processes for time-based compliance work will go into production and be implemented in 2022.</p> <p>The SAP/GIS interface updates will continue. Once the necessary work is completed, we will take the necessary steps to transition to using SAP Maintenance Plans for time-based maintenance of line assets.</p>
NERC/FERC Standards						<p>Staff continues to ensure compliance with the Federal Energy Regulatory Commission (FERC) mandated North American Electric Reliability Corporation (NERC) and Western Electricity Coordinating Council (WECC) Reliability Standards through internal coordination. SMEs review upcoming and approved Reliability Standards and update associated procedures, processes, and tools to ensure compliance. In addition, staff continues to execute the Internal Controls Evaluation (ICE) Program for both Operating & Planning and CIP Reliability Standards.</p>

Enterprise Risk Mitigations for Risks Currently not within Target











Meter to cash						<p>The current 2022-2023 rate proposals include significant system work including, Solar + Storage, VNEM, CPP, and multiple price changes per year. IT, CCS, Strategy, and 2030 Zero Carbon leadership and staff have partnered to build robust planning, implementation, and QA/QC teams to ensure successful deployments of all changes. While the “Yellow” risk rating accurately reflects the level of change and effort to manage the change, advanced testing gives staff the opportunity to identify areas of concern before the customer experience is impacted. Should an error be identified after a customer’s bill has been impacted, SMUD Rate, Rules, and Regulations provide the latitude to rebill as needed to resolve the concern.</p>
Supply chain						<p>In 2021, staff continues to focus on the acquisition of Personal Protective Equipment (PPE), sanitation, and other critical supplies to help manage SMUD’s response to COVID-19. The effects of prioritizing this response and implementing social distancing and other protocols for essential employees was an unexpected but unavoidable shift in focus on top of existing responsibilities to manage supply chain risk.</p> <p>Wildfire was another emergency event that impacted supply chain availability. With the nature and volume of the fires in 2021, there were regional impacts to material availability (delays in shipment and arrival) due to the impacts from transportation and logistics demands in the region. Staff managed these risks in the moment and have included it in our planning for the future.</p> <p>In addition to impacts of COVID-19 and the wildfire season, staff experienced an increase in construction demand along with material price increases which were somewhat related to COVID-19 responses, wildfire, and other natural disasters across the United States.</p> <p>In 2021, supply chain risk management continued to focus on strengthening SMUD’s material and equipment supply chain through partnering with critical suppliers, focusing on contract management, and working with key stakeholders on process improvements.</p> <p>In 2021 supply chain has an increased focus on material forecasting, managing supplier performance, and further implementing risk assessment reviews because of new risk element definitions completed in 2021. Staff continues this effort into 2022.</p>

Enterprise Risk Mitigations for Risks Currently not within Target

	59 th Street reuse						Risk reduction efforts underway include the following: 1) Lobbying efforts with the state, local agencies, and development organizations to support an agency developed attenuation factor that balances science and health risk to support risk-based cleanup level; 2) Development of a due diligence agreement with SKK/BlackPine to support off-ramps and land reuse options should SMUD be unable to remediate PCE in soil to residential cleanup standards; 3) Purchase of an insurance document to reduce liability and risk from future offsite and onsite health exposure/liability claims; 4) Ongoing research and investigation to delineate the solvent plume and evaluate remedial action technologies for use at the site; and 5) Planned soil removal of the "hot spot" area and continued soil vapor extraction at 59th Street.
Strategic	Innovation						Our 2030 Zero Carbon Plan will rely heavily on being innovative, leveraging both business and technological innovations to meet our goal. It was determined a dedicated innovation team would be created during realignment, July 2021. The Innovation team will propel us towards our 2030 zero carbon goal by balancing diverse emerging technologies and ideas across the organization that drive operational efficiencies and competitive advantage with a centralized team that can champion breakthrough innovations. The Innovation team launched IDEAHub, September 30, 2021. The IDEAHub is designed to play a central role in supporting the 2030 Zero Carbon Plan, inspire a culture of innovation at SMUD, allow for increased organizational agility and offer an easy intake process that's inclusive and transparent.
	Energy efficiency						The 2030 Zero Carbon Plan includes energy efficiency (including building electrification) that supports meeting/exceeding the statewide goal of doubling of energy efficiency. Given COVID, the original 5-year glidepath to transition to a largely building electrification portfolio for energy efficiency was accelerated and we have largely reached our "maintain" level for traditional energy efficiency in lieu of building electrification. Moving forward, efficiency in support of decarbonization will be the key, aligned to our revised SD metric.
	Changing customer expectations						In 2021, staff continued to improve digital self-service tools for customers including launching a pilot of a new solution for commercial customers with our partner, SEW. As we prepare to launch new 2030 ZCP strategies and



Enterprise Risk Mitigations for Risks Currently not within Target

						<p>programs, we have been integrating customer insights and leveraging customer-focused design-thinking and journey mapping to ensure the optimum customer experience. Strategic Account representatives have been working closely with our commercial accounts to ensure they are aware of and prepared for upcoming structural changes to rates and the recently approved rate increases. Uncertainty around customer perceptions regarding the new rates expected to launch in 2022 (Critical Peak Pricing, Solar and Storage Rate, Virtual Net Energy Metering) could impact customer experience. In addition, the anticipated restart of collections and disconnections in early 2022 are expected to negatively impact customer VFP and create bleed-over to other areas of customer satisfaction.</p>
Competitive workforce total rewards						<p>To mitigate this risk, 2021 activities included establishing a strategy with Procurement and Benefits Team to build the healthcare cost containment roadmap using the GOST framework. Six Strategies with associated tactics were identified. Several of the strategies have been implemented and proven successful in recent renewal including building stronger relationships with carriers and more heavily leveraging AON along with assertive negotiations. The roadmap is on schedule to be completed by Q4. The outcomes for 2021 are negotiating initial renewal of 10.5% from United Healthcare (UHC) recommending a 10.5% to 7.6% (CalPERS renewal with UHC was 8.26%). Our final renewal with Kaiser landed at 6.56% down from initial of 8.56%</p> <p>Additional work in 2021 includes beginning the assessment of SMUD's paid leave programs to evaluate both offerings (an ask from Parents ERG) and the financial components.</p> <p>Complete assessment of SMUD's paid leave programs, decide on any changes in 2022 and implement for 2023 Open Enrollment.</p> <p>In 2022 staff will execute on six strategies and associated tactics from finalized healthcare premium roadmap.</p> <p>Complete assessment of SMUD's paid leave programs, decide on any changes, and implement for 2023 Open Enrollment.</p>
Renewable portfolio standards (RPS)						<p>SMUD achieved the 2020 RPS requirements for Compliance Period 3 2017-2020, achieving a 33% RPS in 2020. The next compliance period is being planned for Compliance Period 4, 2021-2024, the next RPS target</p>

Enterprise Risk Mitigations for Risks Currently not within Target

							statute is a 44% RPS in 2024. Low risk in achieving this goal as we have several renewable projects in the pipeline and some surplus REC's.
	Underserved Community Engagement			●	➔	●	In order to reduce this risk, SMUD is developing a collaborative low income/underserved community strategy document that will focus developing consist process to gain intake information regarding customer concerns in hard to reach demographics, provide avenues for diverse customer education on programs and implementation, identify alternate low-income/underserved community funding sources via grants and federal sources to address inclusive 2030 adoption alignment for underserved populations, and develop community pilots to catalyze equitable electrification onboarding.
	2030 Zero Carbon Plan			●	➔	●	Staff continues to conduct and review reliability studies to ensure that reliability levels are maintained and look for ways to limit rate increases through cost offsets from operational efficiencies and grants/partnerships.
External	Economic business agility	●	●	●	➔	●	In the 2022 Rate process, staff introduced a 1 1/2% rate increase for 2022, as well as start the Commercial Rate Restructure in Q4 2021 as well as implement the Solar & Storage Rate. This helps protect SMUD in the long term to ensure more stable revenue as well as encourage the adoption of batteries, which will improve reliability for the grid. The CEO and CFO have shown fiscal prudence and have kept the budget within financial limits, which is an improvement. Executive review of all hiring continues, and the exec team has spent a lot of time looking at vacant and limited term positions to give the organization better clarity around staffing. There will be continued work for 2023 and 2024. We have begun work to streamline our budget process and look at risks relative to priorities. The next step will be to incorporate the prioritization framework that is being developed into the planning process. As we get further insight into the programs and items included in the 2030 Zero Carbon Plan, we are getting a better insight into the cost and financial concerns. Our models continue to be synced up and that work will continue. As part of the realignment, an Operational Excellence team was created. They are partnering with areas in the business, and we're starting to see the benefits of that work.
	CEC: Integrated resource planning (IRP)						In 2021, SMUD staff delivered the 2030 Zero Carbon Plan (ZCP) to the Board and the Public. The Board adopted SMUD's Zero Carbon Plan in



Enterprise Risk Mitigations for Risks Currently not within Target






late April 2021. Staff now is focused on day two work and analysis including:

- In depth reliability assessment of McClellan and Campbells retirements which will identify additional investments needed to support these retirements.
- Issue an RFP for new renewable resources to support Proven Clean Technology Growth supporting GHG reduction and the thermal transition plan.
- NTUA 100 MW Solar online in 2021 and local Hedge Battery Storage 4 MW online in 2021.
- Receive Board approval to execute power purchase agreements for the Sacramento Valley Energy Center and King's Country Solar+Battery projects.
- Continued development of Country Acres project.
- Continued development of Solano 4 wind project - received SMUD Board approval to proceed with the project. 91 MW of clean wind.
- Development of DER pilots that will test various customer programs in VPP and Demand Response.
- Continued exploration and study of Utility Scale Clean Energy options that address the remaining 10% of GHG in 2030, including but not limited to pumped hydro, long duration energy storage technologies, various alternative clean fuels that we could use at thermal sites, carbon capture and sequestration, and green hydrogen production.
- Continue to identify future locations for local solar and battery storage projects in support of SMUD's renewable goals and green programs such as Neighborhood Solar Shares.
- Continue work on grid modernization efforts including the Automated Distribution Management System (ADMS) and continuing work on the Distributed Energy Resource Management System (DERMS), both of which lay the foundation for integration of DERs such as solar, energy storage, flexible demand, and electric vehicles.
- Revisit low income and underserved community offerings with 2030 ZCP lens.

Enterprise Risk Mitigations for Risks Currently not within Target

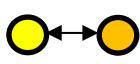


						<p>-New local system upgrades to be completed in 2021, including the completion of a transmission line upgrade project (Hurley Proctor Reconductoring Project) that will increase SMUD’s ability to serve customer demand.</p> <p>-Begin to track and report SMUD’s progress towards achievement of our 2030 ZCP goal by incorporating carbon savings attributed to energy efficiency, and the electrification of buildings and transportation - develop ZCP Dashboard and project tracking report.</p>
Post 2020 carbon markets						<p>SMUD continues to be engaged in the stakeholder process with the California Air Resources Board (CARB) as they look to reallocate carbon allowances based on the new 60% RPS (SB100). Staff has been providing analysis and comment to CARB and with the Joint Utilities Group to achieve greatest value for SMUD customers. CARB is planning to open the rule making process in 2021 and will likely reallocate allowances based on the new 60% RPS (at a minimum - other adjustments may be made based on electrification projects which could mean more allowances for SMUD, but this topic may be addressed in later proceedings).</p>
Wildfire						<p>The 2022 budget includes projects to continue the implementation of SMUD’s Wildfire Mitigation Plan. In 2021, staff continued the installation of non-expulsion equipment on distribution facilities in higher risk areas. Due to negative impact of labor resources, this work is expected to be completed by 2025. High resolution imagery of SMUD’s transmission assets located in high fire threat district (HFTD) Tiers 2 and 3 were collected via drones and are being analyzed to identify deficiencies with these assets. The project identified previously unknown mechanical defects, and in one instance, avoided a potential wire down during fire season. The corrective maintenance activities resulting from the drone pilot will be prioritized based on severity. This project will be concluded by the end of 2021 and may lead to a new program in the future.</p>
Climate Change						<p>Climate readiness analysis completed in 2021 but given the development and adoption of the 2030 Zero Carbon Plan, need to look at the frame of the Climate readiness and adaptation work relative to the 2030 Zero Carbon Plan before developing an updated Action Plan. This work will be done with consideration of enterprise prioritization during 2022.</p>

Enterprise Risk Mitigations for Risks Currently not within Target







<p>Pandemic</p>						<p>During 2021, SMUD Safety, Emergency Planning (EP), and Workforce, Diversity, and Inclusion (WDI), herein referred to as the COVID response team, continued to provide COVID-19 prevention guidance to its employees and contractors. During the first half of the year, the team initiated a vaccination campaign for employees that included the coordination of vaccination schedules with the County and designated health care agencies. In addition, staff continued to track COVID-19 regulatory changes with the Centers for Disease Control (CDC), California Department of Public Health, and Cal-OSHA, as well as participation in utility roundtables that discussed COVID-19 controls and remote work re-entry planning. Regulatory and roundtable information was used to update COVID-19 prevention guidance, limited facility openings (e.g., lobby opening), community event planning, customer service support, and travel/training protocols. More recently, staff has been able to provide COVID-19 antigen testing at its onsite medical service center with confirmation molecular testing at a third-party test laboratory. Strong contact tracing, contractor COVID-19 prevention guidance, remote work, and wellness/exposure updates have assisted SMUD in providing reliable power and quality customer service while protecting our employees and the public during the pandemic.</p> <p>In 2022, the SMUD's COVID response team will continue to track regulatory changes and update guidance as needed. In addition, the team will be working with Facilities to support the re-entry plan of its remote work employees. The re-entry plan outlines a phased employee return over 4 to 5 months starting in January 2022. Re-entry controls to ensure the safety of our employees include mandatory on-line re-entry training; more frequent sanitation of work areas; conference room scheduling/cleaning; adoption of a hybrid work schedules; Personal Protective Equipment usage, and social distancing. Facilities and Safety is currently piloting an air ionization plan that may be installed in buildings prior to initiating the re-entry program. Lastly, Safety will continue to work with hybrid staff to ensure that they have ergonomic workstations at home and work.</p>
-----------------	---	---	---	---	---	---

**TOP 10 ENTERPRISE RISKS COMPARED TO SMUD'S ENTERPRISE RISK CATEGORIES
Specific to Energy and Utilities Industry**


Benchmarking Information indicates that SMUD's risks are consistent with other energy and utilities; one indicator that we are aligned in our understanding of risks facing our industry.

North Carolina State ERM Initiative and Protiviti Top 10 Enterprise Risks		SMUD's Corresponding Risks	SMUD's Current Residual Risk Exposure
Specific to Energy and Utilities Industry			
1	Pandemic related policies and regulation impact business performance.	Operational risk: Regulatory compliance Strategic risk: Demand response Distributed energy Energy efficiency Electrification of the transportation sector Innovation Carbon emissions Renewable Portfolio Standards CEC: Integrated Resource Planning External risk: Legislative & regulatory Climate change Pandemic Wildfire	The current residual risk exposure ranges from medium to high 
2	Economic conditions constrain growth opportunities.	Strategic risk: 2030 Zero Carbon Plan Innovation External risk: Business agility	
3	Pandemic-related market conditions reduce customer demand	Financial risk: Budget planning and rate setting Capital availability/cashflow Operational risk: Meter to cash Strategic risk: 2030 Zero Carbon Plan Changing customer expectations External risk: Economic business agility Pandemic	

**TOP 10 ENTERPRISE RISKS COMPARED TO SMUD’S ENTERPRISE RISK CATEGORIES
Specific to Energy and Utilities Industry**

4	Adoption of digital technologies may require new skills or significant efforts to upskill/reskill existing employees	Operational risk: Change Management Strategic Workforce Agility Data governance Data availability Cyber security Privacy	The current residual risk exposure ranges from medium to high 
5	Privacy/identity management and information security protection	Operational risk: Cyber security Privacy	
6	Cyber threats	Operational risk: Cyber security Privacy	
7	Impact of regulatory change and scrutiny on operational resilience, products, and services	Operational risk: Regulatory compliance Strategic risk: Demand response Distributed energy Energy efficiency Electrification of the transportation sector Innovation Carbon emissions Renewable Portfolio Standards CEC: Integrated Resource Planning External risk: Legislative & regulatory Climate change Pandemic Wildfire	The current residual risk exposure ranges from medium to high 
8	Succession challenges, ability to attract and retain top talent	Operational risk: Strategic workforce agility Competitive workforce total rewards Diversity, Equity, Inclusion and Belonging Change Management	
9	Resistance to change operations and business model	Operational risk: Strategic workforce agility Operational excellence Diversity, Equity, Inclusion and Belonging Change Management Strategic risk: Innovation 2030 Zero Carbon Plan	

**TOP 10 ENTERPRISE RISKS COMPARED TO SMUD’S ENTERPRISE RISK CATEGORIES
Specific to Energy and Utilities Industry**

<p>10</p>	<p>Ability to compete with “born digital” and other competitors</p>	<p>Operational risk: Technology system infrastructure Grid operational system & support Strategic risk: Innovation External risk: Business agility</p>	
-----------	---	---	---

SSS No. LEG 2021-0121

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date Policy – 11/17/21
Board Meeting Date November 18, 2021

TO				TO			
1.	Jennifer Davidson	6.					
2.	Stephen Clemons	7.					
3.	Brandy Bolden	8.					
4.	Farres Everly	9.	Legal				
5.		10.	CEO & General Manager				
Consent Calendar	<input checked="" type="checkbox"/> Yes	No <i>If no, schedule a dry run presentation.</i>		Budgeted	<input checked="" type="checkbox"/> Yes	No <i>(If no, explain in Cost/Budgeted section.)</i>	
FROM (IPR) Laura Lewis		DEPARTMENT Executive Office			MAIL STOP B308	EXT. 6123	DATE SENT 11/11/21

NARRATIVE:

Requested Action: Make determination pursuant to Assembly Bill 361 (AB 361) to continue meetings via virtual (online/teleconference) meeting for the next 30 days.

Summary: Pursuant to Executive Order N-29-20 issued on March 17, 2020, and Executive Order N-35-20 issued on March 21, 2020, as well as the Emergency Board Meeting Procedures adopted by this Board via Resolution No. 20-06-08 on June 18, 2020, this Board has conducted regular Board meetings and other public meetings via remote (online/teleconference) meetings.

Executive Order N-08-21 was issued on June 11, 2021, to phase out various Executive Orders issued in response to the COVID-19 (coronavirus) pandemic, including the temporary authority allowing local agency bodies to hold remote meetings under N-29-20. Under this Order, the temporary authority expired on September 30, 2021.

On September 16, 2021, Governor Newsom signed Assembly Bill 361 (AB 361), which became effective immediately upon signature, containing language similar to the Governor’s previous Executive Orders that eased Brown Act requirements to allow local agencies to meet remotely. AB 361 allows meetings to continue to be conducted by teleconference, similar to the process used during the current COVID-19 pandemic, but only when there is a declared state of emergency that makes it unsafe to meet in person.

On July 29, 2021, the Sacramento County Public Health Officer issued an Order, effective July 30, 2021, finding the significantly more transmissible Delta variant of the SARS-CoV-2 virus has become the predominant strain in the County of Sacramento, and directing all individuals in the County to wear a face covering indoors in workplaces and public settings regardless of vaccination status. This Order is currently in effect.

On September 28, 2021, the Sacramento County Public Health Office issued a Teleconferencing Recommendation for public meetings stating it is an effective and recommended social distancing measure to facilitate participation in public affairs and encourage participants to protect themselves and others from COVID-19.

It would be impractical to ensure all public meeting attendees are vaccinated and have appropriate face coverings that are worn correctly.

Staff’s recommendation is to continue to hold regular Board meetings and other public meetings via solely virtual (online/teleconference) meeting and continue to monitor developments related to the COVID-19 pandemic. Pursuant to Government Code section 54953(e), this Board must make findings every 30 days that conditions warrant continuing to meet virtually instead of in-person.

Board Policy: Governance Process GP-3, Board Job Description – j) Take such other actions as may be required by law.
(Number & Title)

Benefits: Making the determination to continue remote meetings will allow for efficient conduct of SMUD business.

Cost/Budgeted: Contained in Business Unit budget for internal labor.

Alternatives: Take no action and comply with all original Brown Act requirements.

Affected Parties: SMUD, Board of Directors, Public

Coordination: Executive Office, Board Office, Legal Department, Information Technology, Communications

Presenter: Laura Lewis, Chief Legal & Government Affairs Officer

Additional Links:

SUBJECT

Make Determination to Continue Online/Teleconference Meetings

ITEM NO. (FOR LEGAL USE ONLY)

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No. BOD 2021-001

BOARD AGENDA ITEM STAFFING SUMMARY SHEET

Committee Meeting & Date Policy 2021
Board Meeting Date 2021

TO	TO
1. Jennifer Davidson	6.
2. Stephen Clemons	7.
3.	8.
4.	9. Legal
5.	10. CEO & General Manager

Consent Calendar		Yes	<input checked="" type="checkbox"/>	No <i>If no, schedule a dry run presentation.</i>	Budgeted		Yes	No <i>(If no, explain in Cost/Budgeted section.)</i>
FROM (IPR) Nancy Bui-Thompson / Donna Lofton	DEPARTMENT Board Office				MAIL STOP B307	EXT. 5079	DATE SENT 12/22/2020	

NARRATIVE:

Requested Action: Enable the Board of Directors and Executive Staff an opportunity to review the Board Work Plan.

Summary: The Board President reviews the Board Work Plan at the Policy Committee meeting to ensure a genda items support the work of the Board.

Board Policy: This review of the work plan supports GP-6 Role of the Board President which states that the Board President shall give progress reports on the Board's work plan.
(Number & Title)

Benefits: Reviewing the Work Plan allows the Board members and Executive staff to make changes to the Work Plan and Parking Lot items as necessary.

Cost/Budgeted: N/A

Alternatives: Not review the Work Plan at this time

Affected Parties: Board and Executive staff

Coordination: Donna Lofton

Presenter: Nancy Bui-Thompson, Board President

Additional Links:

SUBJECT Board Work Plan	ITEM NO. (FOR LEGAL USE ONLY)
----------------------------	-------------------------------

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No. BOD 2021-004

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date Policy 2021
Board Meeting Date N/A

TO	TO
1. PaulLau	6.
2. JenniferDavidson	7.
3.	8.
4.	9. Legal
5.	10. CEO & General Manager

Consent Calendar	<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	No	<i>If no, schedule a dry run presentation.</i>	Budgeted	<input type="checkbox"/>	Yes	No	<i>(If no, explain in Cost/Budgeted section.)</i>
-------------------------	--------------------------	------------	-------------------------------------	-----------	--	-----------------	--------------------------	------------	-----------	---

FROM (IPR) Heidi Sanborn / Donna Lofton	DEPARTMENT Board Office	MAIL STOP B307	EXT. 5079	DATE SENT 12/22/20
--	----------------------------	-------------------	--------------	-----------------------

NARRATIVE:

Requested Action: Provide a summary of committee direction from the Board to Staff.

Summary: During a Board discussion at the January 2017 Policy Committee, the Board requested having an on-going opportunity to do a wrap up period at the end of each committee meeting to summarize various Board member suggestions and requests that were made at the meeting in an effort to make clear the will of the Board. The Committee Chair will summarize Board member requests that come out of the committee presentations for this meeting.

Board Policy: GP-4 Agenda Planning states the Board will focus on the results the Board wants the organization to achieve.
(Number & Title)

Benefits: Having an agendized opportunity to summarize the Board’s requests and suggestions that arise during the committee meeting will help clarify what the will of the Board.

Cost/Budgeted: N/A

Alternatives: Not summarize the Board’s requests at this meeting.

Affected Parties: Board of Directors and Executive Staff

Coordination: Donna Lofton, Special Assistant to the Board

Presenter: Heidi Sanborn, Policy Committee Chair

Additional Links:

SUBJECT Summary of Committee Direction	ITEM NO. (FOR LEGAL USE ONLY)
---	-------------------------------

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.