Board Policy Committee Meeting and Special SMUD Board of Directors Meeting

Date: Wednesday, November 15, 2023

Time: Scheduled to begin at 6:00 p.m.

Location: SMUD Headquarters Building, Auditorium
6201 S Street, Sacramento, CA

Powering forward. Together.

SMUD®

AGENDA
BOARD POLICYCOMMITTEE MEETING
AND SPECIAL SMUD BOARD OF DIRECTORS MEETING

Wednesday, November 15, 2023
SMUD Headquarters Building, Auditorium
6201 S Street, Sacramento, California
Scheduled to begin at 6:00 p.m.

This Committee meeting is noticed as a joint meeting with the Board of Directors for the purpose of 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:

Virtual Viewing or Attendance:
Live video streams (view-only) and indexed archives of meetings are available at: http://smud.granicus.com/ViewPublisher.php?view_id=16

Zoom Webinar Link: Join Board Policy Committee Meeting Here
Webinar/Meeting ID: 160 750 5422
Passcode: 802571
Phone Dial-in Number: 1-669-254-5252 or 1-833-568-8864 (Toll Free)

Verbal Public Comment:
Members of the public may provide verbal public comment by:

- Registering in advance of a meeting by sending an email to PublicComment@smud.org, making sure to include the commenter's name, date of the meeting, and topic or agenda item for comment. Microphones will be enabled for virtual or telephonic attendees at the time public comment is called and when the commenter's name is announced.
- Completing a sign-up form at the table outside of the meeting room and giving it to SMUD Security.
- Using the "Raise Hand" feature in Zoom (or pressing *9 while dialed into the telephone/toll-free number) during the meeting at the time public comment is called. Microphones will be enabled for virtual or telephonic attendees when the commenter's name is announced.

Written Public Comment:
Members of the public may provide written public comment on a specific agenda item or on items not on the agenda (general public comment) by submitting comments via email to PublicComment@smud.org or by mailing or bringing physical copies to the meeting. Comments will not be read into the record but will be provided to the Board and placed into the record of the meeting if received within two hours after the meeting ends.

DISCUSSION ITEMS

1.	Antiwon Jacobs Kelsey McFadyen	Accept the monitoring report for **Strategic Direction SD-16, Information Management and Security.** Presentation: 15 minutes Discussion: 5 minutes
2.	Russell Mills	Accept the monitoring report for **Strategic Direction SD-17, Enterprise Risk Management**. Presentation: 15 minutes Discussion: 10 minutes
3.	Dave Tamayo	Board Monitoring: **Governance Process GP-8, Board Committee Principles; Governance Process GP-12, Board Compensation and Benefits; Governance Process GP-15, Board Travel and Training Reimbursement**. Presentation: 2 minutes Discussion: 3 minutes
4.	Dave Tamayo	Annual Review of Standing Committees. Presentation: 2 minutes Discussion: 3 minutes
5.	Heidi Sanborn	Discuss **Election of Officers for 2024** (President and Vice President) for the SMUD Board of Directors. Discussion: 10 minutes

INFORMATIONAL ITEMS

6.	Heidi Sanborn	Board Work Plan. Discussion: 5 minutes
7.	Public Comment	
8.	Dave Tamayo	Summary of Committee Direction. Discussion: 1 minute

ANNOUNCEMENT OF CLOSED SESSION AGENDA

1. **Threats to Public Buildings, Services and Facilities**.

   Pursuant to Section 54957 of the Government Code:

   Consultation with: Laura Lewis, Chief Legal & Government Affairs Officer; Suresh Kotha, Chief Information Officer; Antiwon Jacobs, Director, Cybersecurity and Rob Lechner, Director, Facilities, Security & Emergency Operations.

Members of the public shall have up to three (3) minutes to provide public comment on items on the agenda or items not on the agenda, but within the jurisdiction of SMUD. The total time allotted to any individual speaker shall not exceed nine (9) minutes.

Members of the public wishing to inspect public documents related to agenda items may click on the Information Packet link for this meeting on the smud.org website or may call 1-916-732-7143 to arrange for inspection of the documents at the SMUD Headquarters Building, 6201 S Street, Sacramento, California.

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 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 1-916-732-7143, no later than 48 hours before this meeting.

SSS No.
GM 23-189

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date
Policy, November 15, 2023
Board Meeting Date
November 16, 2023

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

Consent Calendar	X	**Yes**		**No** *If no, schedule a dry run presentation.*	**Budgeted**		**Yes**	X	**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
David Bitter	Cybersecurity	K112	6901	10/24/2023

NARRATIVE:

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

Summary: Present the 2022-2023 Board Monitoring Report for SD-16, Information Management and Security.

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

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: Costs contained in internal labor budget.

Alternatives: Receive information via memo or written report.

Affected Parties: All SMUD Departments

Coordination: Cybersecurity

Presenter: Antiwon Jacobs, Director, Cybersecurity

Additional Links:

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

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SACRAMENTO MUNICIPAL UTILITY DISTRICT

OFFICE MEMORANDUM

TO: Board of Directors **DATE:** November 1, 2023

FROM: Claire Rogers CR 11/1/23

SUBJECT: **Audit Report No. 28007613**
Board Monitoring Report; SD-16: Information Management and Security

Internal Audit Services (IAS) received the SD-16 *Information Management and Security* 2023 Annual Board Monitoring Report and performed the following:

- Selected a sample of statements and assertions in the report for review.
- Interviewed report contributors and verified the methodology used to prepare the statements in our sample.
- Validated the reasonableness of the statements in our sample based on the data or other support provided to us.

During the review, nothing came to IAS' attention that would suggest the items sampled within 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 2023
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 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) SMUD's Information Security, Physical Security, Customer Privacy, and Records Management programs and initiatives align directly with the "Safety and Reliability" Core Values of SMUD's 2030 Clean Energy Plan. 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	Security controls and processes are 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	Minor changes (around why SMUD collects personal information)
Customer Privacy: Ensure security where data is shared	System Security Plans and SOC 2 audit report requirements	Evaluate the information practices and security controls of third parties	Confidence that vendors have implemented robust cybersecurity programs to protect SMUD information	
Customer Privacy: Maintain a process that identifies purposes for information collection and dissemination	Data Sharing Policy, Data Sharing Request/Approval Process	Track NDAs, the data being shared, and the business justification for sharing	Formal data sharing process is being observed and maintained	
Records Management: Identify and manage records and information	Records Evaluations and Information Migration	Evaluate, classify and migrate records and ensure retrieval, disposal and protection.	Completed the 5-year records evaluation plan and kicked off the first wave of business area information migrations	
Records Management: Ensure all information systems are compliant with	Information System Evaluations	Review of software tools housing SMUD data and information.	Evaluate software tools for information management compliance	IMC has been added to software purchase process

IMC requirements and best practices.				
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	Completed operational component of project to facilitate direct radio contact with local law enforcement agencies	Policy and procedures documentation was also updated to accommodate the new radios
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-industry best practices	Security Operations personnel continue to provide security evaluations for SMUD real properties	Third-party Risk, Threat, and Vulnerability Analysis tentatively scheduled to begin Q1 2024

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 Information Officer's (CIO) 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 controls through SMUD policies to enhance and govern 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.

Security Operations has successfully implemented the full integration of the Sacramento Regional Radio Communications System (SRRCS) into our Security Control Centers as well as with Supervisors and key leadership personnel. This integration will facilitate interoperability directly with local and regional law enforcement agencies during emergencies. Security

Operations has also been working on a Risk, Threat, and Vulnerability Assessment (RTVA) request for proposal, which is complete and out for bid. This project will provide a comprehensive, third-party assessment of nearly all of SMUD's facilities in order for us to identify and mitigate risks to our personnel and assets.

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.

Security Operations has been involved in the effort to replace the enterprise-wide Physical Access Control System (PACS). This project to upgrade and modernize the PACS is well underway and has been progressing successfully. Security Operations is also working on the implementation of additional complementary technologies to increase our ability to detect and assess unauthorized intruders at critical substations. Once the pilot program is complete, it should lead to a wider implementation of the new technologies.

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 language in the notice was updated this year to be more straightforward about why we collect customer information and that it is disposed of when no longer necessary. 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. Additionally, our data sharing policy and process (discussed below) align to this requirement.

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 policy and process were audited last year by SMUD's Internal Audit Services (IAS) department. IAS noted no high-risk observations, although they did identify ways to improve both the data sharing policy and the associated process. Responses to all audit observations were completed on schedule and were confirmed by IAS to be closed in November 2022.

Records 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 Information Management and Compliance (IMC) program has achieved our 5-year plan of completing record evaluations for all business areas. We have implemented information management procedures for each completed business area. The completion of these evaluations and procedures gives us a high level of confidence that SMUD records will be managed appropriately.

The IMC Program in collaboration with the Enterprise Content Management (ECM) team launched a mass content migration (Enterprise Shared Drive Migration) project at the beginning of 2023. Using completed IMC records evaluations, this effort has kicked off for 13 of the 33 business areas in scope for this project. The project will identify, organize, and ultimately migrate content for each business area from non-approved records repositories into approved record repositories. This will allow this content to be managed in accordance with SD-16.

The IMC 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. IMC has been added to the purchase approval process to support this effort.

The IMC Program continues to collaborate with the Enterprise Content Management 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

The "Shields Up" declaration from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) from last year has never been rescinded, reflecting continued geopolitical tension and nation state cyber actors targeting critical infrastructure. Cybersecurity continued to work with numerous IT teams to follow this guidance to help manage the cyber risk. Ongoing internally facing awareness campaigns have been helpful in reminding staff of the risks we're facing and the role they play in keeping our systems and data protected. In addition to the technical controls put in place, cybersecurity also continued to partner with other departments to ensure our cyber insurance coverage is maintained.

SMUD's Payment Card Industry (PCI) card payment transaction volume once again increased, although SMUD remains a Level 2 Merchant. SMUD is again compliant with the PCI Data Security Standard (PCI DSS) this year as determined by an independent third-party PCI Qualified Security Assessor. Our required assessment documents were submitted to Chase Paymentech in June. This year we also introduced new processes and controls required by the upcoming PCI DSS version 4. Although our mature cybersecurity practices have prepared us well for the updated standard's requirements, these minor improvements were necessary and will be complete by the time the new standard takes effect in March of 2024.

The Cybersecurity team continues to work hard to ensure compliance with the NERC Critical Infrastructure Protection (CIP) standards. Additional standards become enforceable in 2024 and subsequent years, which SMUD is currently not adequately staffed to implement. Over the next few years standards related to Bulk Electric System Cyber System Information (BES CSI or BCSI) in the cloud, monitoring vendor remote access, and several standards changes related to supporting virtualization will all become enforceable. Additionally, the Solano Phase 4 project and the upgrade of SMUD's Energy Management System (EMS) will both require significant resources to ensure compliance.

Ransomware continues to be a threat facing many organizations today, and as a result SMUD Cybersecurity has continued to mature our Cybersecurity Emergency Operations Program (CEOP), performing annual exercises to ensure our teams understand the plan and are prepared to execute it in the event of a security incident. The exercises have highlighted areas of concern and risks that need to be addressed, which we are in the process of doing. Some of these need to be addressed at an enterprise level, which makes them more challenging. Additional risks and challenges will be discussed in the upcoming closed session.

SMUD Cybersecurity continues to execute a multi-year plan to execute a Zero-Trust Strategy and implement its principles to better position SMUD to secure sensitive data, systems, and services. A Zero-Trust architecture will drastically improve SMUD's Cybersecurity risk. Zero-Trust architectures are data-centric and allows the concept of least-privileged access to be applied for every resource access decision. Much progress has already been made in recent years, hastened by the enablement of remote work for our employees, and we will continue to move in this direction aligned to our IT Strategy.

Also in support of the larger IT Strategy, we will continue to enhance our necessary Vulnerability Response and Management capability and technology to ensure Information Technology delivers secure and reliable infrastructure by utilizing automation for patch management, engineering vulnerability mitigations, and maturing the implementation of cybersecurity's vulnerability management plan.

Physical Security

Physical Security is a first line of defense against any unauthorized intrusions at all of our facilities. With our current 'open campus' concept for the Headquarters Campus, and other locations, we are going to continue to regularly discover persons not authorized to be on SMUD property. This may result in increased security risks unless additional resources are deployed to prevent those incursions. This issue is also reflected at our substations as unauthorized intrusions remain a regular occurrence. Reinvesting in additional personnel and technology resources will help mitigate these issues.

As SMUD continues to grow our infrastructure footprint and provide power to an ever-expanding customer base, this necessitates additional investment in Security Operations in order to properly provide the requisite physical security protections called for by both regulatory compliance and industry best-practices. The resource profile for Security Operations has not been changed or evaluated for change since 2014. Since then, both the infrastructure profile and the population it serves have increased significantly. As with the reevaluation that occurred with Cybersecurity that resulted in their organization and staffing changing markedly, the same reevaluation and reinvestment into physical security is necessary to continue to keep pace with the increases in vulnerable assets and customers served.

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). As in years past, 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 that transmission is performed using an approved and secure transfer mechanism.

Records Management

The IMC program continues to integrate information management best practices into SMUD's daily operations. Business areas are actively collaborating with IMC in the creation of information management and recordkeeping polices/procedures specific to their day-to-day operational needs. SMUD's continued development of the IMC program further reduces the risk of potential multi-million-dollar fines and reputational damage associated with lack of records management controls.

The Enterprise Shared Drive Migration project which launched at the beginning of 2023 is a large undertaking that will involve the mass organization and migration of content from Enterprise shared drives to approved SMUD information repositories. IMC in collaboration with the ECM team is working diligently to ensure completion of the project tasks by business areas and ease the learning curve that comes with these implemented changes. We have created documentation that helps with the classification of the records as well as training to ease the transition into using a new repository. This project will ensure SMUD stays in line with information management industry best practices, create an environment of purposeful organization and generate information management symmetry across SMUD.

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
SRRCS – Sacramento Regional Radio Communications System
CISA – Cybersecurity and Infrastructure Security Agency
PCI – Payment Card Industry
PCI DSS – Payment Card Industry Data Security Standard
CIP – Critical Infrastructure Protection
BES – Bulk Electric System
BESCSI – Bulk Electric System Cyber System Information
BCSI – BES Cyber System Information
CEOP – Cybersecurity Emergency Operations Program
CIRP – Cybersecurity Incident Response Plan

2

SSS No.
TR 23-003

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date
Policy Committee November 15, 2023
Board Meeting Date
November 16, 2023

TO		TO	
1.	Russell Mills	6.	Claire Rogers
2.	Jennifer Davidson	7.	
3.	Suresh Kotha	8.	
4.	Brandy Bolden	9.	**Legal**
5.	Farres Everly	10.	**CEO & General Manager**

Consent Calendar		**Yes**		**No** *If no, schedule a dry run presentation.*	**Budgeted**		**Yes**		**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
Russell Mills	Treasury & Risk Management	B355	6532	10/20/2023

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 November 2022 annual report. The report includes historical risk profiles of top of mind enterprise risks for 2023-2024, mitigation strategies, and a current residual risk exposure status of identified enterprise risks.

Board Policy: *(Number & Title)* Strategic Direction 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: Provides Board members information regarding SMUD's Enterprise Risk.

Cost/Budgeted: Costs contained in internal labor budget.

Alternatives: Provide a written report to the Board.

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

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

Presenter: Russell Mills, Director, Treasury & Treasurer, Corporate Financial & Administrative Services

Additional Links:

SUBJECT	ITEM NO. ***(FOR LEGAL USE ONLY)***
SD-17, Enterprise Risk Management Board Monitoring Report	

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SACRAMENTO MUNICIPAL UTILITY DISTRICT

OFFICE MEMORANDUM

TO: Board of Directors **DATE:** November 1, 2023

FROM: Claire Rogers CR 11/1/23

SUBJECT: **Audit Report No. 28007614**
Board Monitoring Report; SD-17: Enterprise Risk Management

Internal Audit Services (IAS) received the SD-17 *Enterprise Risk Management* 2023 Annual Board Monitoring Report and performed the following:

- Selected a sample of statements and assertions in the report for review.
- Interviewed report contributors and verified the methodology used to prepare the statements in our sample.
- Validated the reasonableness of the statements in our sample based on the data or other support provided to us.

During the review, nothing came to IAS' attention that would suggest the items sampled within 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 2023
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, SD-17 Enterprise Risk Management.**

c) SMUD continues to maintain an integrated Enterprise Risk Management (ERM) Program.

SMUD's ERM program continues to integrate risk management best practices to support decision making in key business processes. This year the risk framework was used to support decision making during the enterprise prioritization, planning and budget process.

Since the 2022 Annual Monitoring Report, staff continues to review SMUD's portfolio of risks. Two risks were consolidated into one risk, one risk title was changed, and three new additional risks were added to the portfolio.

- Consolidated risk: System adequacy and Operational adequacy combined to Grid infrastructure and operational adequacy
- Changed: Electrification of transport sector to Transportation sector electrification/Unmanaged electrification
- New risk: Utility scale technology
- New risk: Renewables projects
- New risk: Severe weather

The Year-on-Year Residual Risk Exposure results are summarized as follows:

			Nov. 2021	Nov. 2022	Nov. 2023
✓	**"Red":**	Extremely High Residual Exposure	(0)	(0)	(0)
✓	**"Orange":**	High Residual Exposure	(5)	(6)	(5)
✓	**"Yellow":**	Medium Residual Exposure	(40)	(39)	(40)
✓	**"Green":**	Low Residual Exposure	(38)	(38)	(40)
✓	**"Blue":**	Extremely Low Residual Exposure	(0)	(0)	(0)
			(83)	**(83)**	**(85)**

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 47 risks, shown in the last two lines of the table, which are within the risk management goal.

Current Residual Risk Exposure	Risk Management Goal	Number of Risks
Orange "high"	Yellow "medium"	5
Yellow "medium"	Green "low"	33
Yellow "medium"	Yellow "medium"	7
Green "low"	Green "low"	40

Building Resiliency in a Changing Risk Landscape
SMUD's enterprise-wide risk exposure is medium/high. SMUD's risk landscape continues to change. Escalating inflation, increasing cyber events, challenges brought by energy transition, rapid changes in technology, ongoing supply chain challenges exacerbated by global unrest, and unprecedented weather events brought about by climate change are a few of the factors causing the changes in our risk environment. In addition, a hardened insurance market with reduced coverage capacity makes it more difficult for SMUD to protect itself from financial losses resulting from a risk event. As a result, SMUD is focusing on leveraging its enterprise risk management framework in building a resilient organization that can monitor uncertainties and trends, adapt to changing operating environments, and recover from significant impacts in a shifting risk landscape. Staff has worked to further enhance risk input into the enterprise prioritization and business planning processes, focused on better understanding risk interdependencies, and have identified the key risks that have the potential to impact SMUD's performance in the upcoming year. Staff continues identify risks and implement initiatives to mitigate and manage the risks appropriately.

3. Additional Supporting information:

a) Summary of 2023 activities
In 2023, ERM continued to support the organization by facilitating risk conversations, supporting projects, aligning risk practices, 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 utilizes five 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. Another is the newly developed

Risk Champion Network (RCN), a director led risk team focused on championing risk practices across SMUD and discussing top risk priorities. The other three are the Trading Operations Risk Committee (TORC), Zero Carbon Plan Implementation Team, and the Three Lines Working Team.

Since the 2022 Board update, SMUD was faced with unprecedented challenges with recurring storms, operational difficulties, and increased commodity costs to name a few. 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:

Risk Focus Areas for 2023-2024
In 2023, staff worked with leaders across SMUD to identify the top risk focus areas for 2023-2024. This is a list of the top risk areas that if additional controls/mitigations aren't appropriately allocated, have a high potential to impact the achievement of SMUD's goals and strategic objectives in the upcoming year. Understanding these risks better allows senior leaders to make risk informed decisions on the investments they need to make and the actions that are required to achieve SMUD's goals and strategic objectives. These risks were integrated into our enterprise prioritization process to help align our 2024 resource plan to areas of high risk and strategic value.

Attachment A outlines the risk focus areas for 2023-2024 and the actions that will be taken to address these risks.

Risk Champion Network
The Risk Champion Network (RCN) is a director level led committee responsible for championing risk practice across SMUD and identifying and discussing risks that have the potential to impact SMUD and its operations. In 2023, the Risk Champion Network worked to identify the interdependencies between the risk focus areas for 2023-2024. This process identifies where risks are shared across SMUD helping to identify opportunities for optimizing risk response activities. This work also lays the foundation to strategically look at the impacts of these risks SMUD-wide instead of in risk silos allowing staff to better manage and communicate risks.

Environmental and Safety Risk Mitigation
SMUD's Environmental, Health Safety (EH&S) and Real Estate department continues to support risk mitigation efforts throughout the organization. SMUD continues to expand our use of the of the safety management software to improve contractor oversight, risk mitigation compliance, and business partnership. As contractors work through our robust Procurement and Sourcing vendor screening program that assesses and qualifies them to perform future contract work at SMUD, they submit various critical risk mitigation program elements of their EH&S program. After being risk ranked scored, and selected high risk contractors performing work scopes for SMUD complete various pre-task assessments to ensure that key compliance or other project risks are sufficiently mitigated. Once work begins, EH&S staff partner with other SMUD teams to ensure that daily pre-job briefings are conducted and that required project specific risk mitigation measures are routinely performed. SMUD personnel partner with these contractors to ensure that all affected personnel and the public are not negatively impacted by work activities.

Managing Commodity Market Volatility
SMUD has various Board approved directives that dictate guidelines for commodity procurement, limiting the amount of risk tolerance and variability to commodity costs for supplying our customers. These directives serve as guardrails for reliability and affordability.

Commodities Risk Management (CRM) staff monitors and reports regularly on our risk exposure and performance of commodity procurement operations against budgeted costs within our rate case.

2022 and 2023 proved to be challenging in managing commodity costs affordably. This was. primarily because of the outage at Cosumnes Power Plant (CPP), but also because of extraordinary commodity market prices in the later part of 2022 and the beginning of 2023. However, our directives requiring Energy Trading and Contract (ET&C) to respond to an outage by procuring the replacement power and capacity required to satisfy our guidelines and to hedge exposure to gas market risk helped mitigate risk to further cost increases and to any blackouts by having enough power to serve our customers reliably.

The western natural gas markets endured three months of extreme volatility from Dec 2022 through Feb 2023. Prices at northern California's main pricing hub, PG&E Citygate spiked as high as $57 per MMBtu during this period. Our hedging program and directives ensured we were insulated from most of the cost increase, providing large cost offsets through positive settlement revenues of from these hedges. Having gas in storage also assists with this, by allowing SMUD to pull gas that was purchased at much lower prices from the ground instead of paying expensive market prices during periods of volatility.

The commodity budget was severely impacted during the outage period but was insulated from even higher costs and potential for emergency rate increases due to our risk management practices and directives on hedging.

Hazard Mitigation Plan
In 2023, SMUD received a grant from the Federal Emergency Management Agency (FEMA) to update its Hazard Mitigation Plan (HMP). The HMP is a plan that is updated every 5 years and is a requirement to receive mitigation grant funding from FEMA under Disaster Mitigation Act (DMA) 2000. SMUD's Board adopted its first HMP in 2018 and expires in June 2024. New requirements in this update includes an emphasis on vulnerable communities, climate change, and high hazard dams.

The HMP is a collaborative process which include input from the public, various stakeholders and community groups and internal subject matter experts to identify natural and human-made hazards that could potentially impact SMUD's plan area. SMUD's plan area includes all the counties where SMUD owns, partially owns, or operates its infrastructure in. Staff conducted a risk assessment and identified gaps in mitigation by leverage existing SMUD processes to prioritize any additional mitigation actions for future funding opportunities. Some risks included in the plan includes wildfire, floods, drought, severe weather, cyber threats, physical attacks, and oil spill to name a few. This plan allows SMUD to identify policies and actions that can be implemented over the long term to reduce risk and future losses. Furthermore, by having a Hazard Mitigation Plan, SMUD is eligible to apply for future CalOES and FEMA grants to help offset a portion of mitigation project costs.

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. Staff incorporates audit results and management responses ERM assessment planning 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.

- Since the 2022 SD-17 report, 8 audit reports were reviewed by the ERM Office, and none resulted in a change to the risk profile.

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, 2023 & 2032 Executive Perspectives on Top Risks, provides insight for short-term and long-term risks from 1,304 global board members and executives from across several industries. The study states that the level of uncertainty in today's global marketplace and the velocity of change continue to produce a multitude of potential risks that can disrupt an organization's business model and strategy on very short notice. The study found that for 2023, risks are the highest in more than a decade, risk scores for almost all risk domains have increased. People and culture continue to be top of mind for many leaders as it becomes increasingly challenging to attract and retain talent to address needs across organizations. Economic uncertainties as well as massive disruptions in the global supply chain and innovative disruptions continue to impact strategic initiatives for many organizations. 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 risks identified by the study is outlined in Attachment B.

c) Looking forward
   In 2023, ERM's goal is to build a more risk aware culture by leveraging the Risk Champion Network and frequent risk communications and learning modules. Staff will continue to implement programmatic changes, align risk practices SMUD-wide, and fine tune risk management practices within business processes. The following initiatives have been planned:

   - Develop risk appetite statements and risk awareness trainings,
   - Enhance risk input into enterprise prioritization and strategy process,
   - Finalize SMUD's Hazard Mitigation Plan,
   - Continue to support SMUD's wildfire safety program,
   - Positively influence state and federal legislative/regulatory issues,
   - Identify a strategy to attract workforce for critical roles,
   - Provide programs and services which reflect the customer's changing expectations,
   - Support SMUD's Environmental and Safety initiatives,
   - Continue cyber security and privacy awareness and compliance activities,
   - Improve upon current physical security and public safety practices, and
   - Test and enhance our operational response plans through tabletop exercises and coordinated meetings.

4. Challenges: The risk environment is changing more rapidly than ever before. With technology innovations increasing, there brings both opportunities and exacerbates existing risks. Supply chain issues, decarbonization trends, a hardened insurance market, workforce capabilities, and reliability and resiliency requirements all add to the challenging risk environment, making it more difficult to manage risks. SMUD's ERM framework allows staff to better manage risks as a portfolio, rather than in silos. The result is increased awareness of SMUD's risks, 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.

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
Operational: Process	Business continuity and disaster recovery						In 2023, staff worked to implement the 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. In 2024, staff will continue to focus on increasing business continuity capabilities through the continued roll-out of the ECMS solution with training and change management support. Staff will also begin partnering with IT to initiate enhancements to the IT Disaster Recovery Program.
Financial	Commodity costs: energy commodity						Additional directives were put in place to monitor fluctuations in commodity risks. The TORC will continue to monitor changes and report to the EROC as appropriate.
Operational: Process	Control center						Staff is currently in the beginning stages of acquiring property to build a new control center that will meet SMUD's current and future needs.
Operational: System	Cybersecurity						The cybersecurity program has continued to mature year-after-year and in line with SD-16, cyber has implemented strategies and technical solutions to manage SMUD's cyber, privacy, legal, regulatory and compliance risk. In 2023, Cybersecurity has focused on: • Encouraging Information Technology (IT) and the business to embrace a Zero-Trust Strategy and Principles to better position SMUD to secure sensitive data, systems, and services. A Zero-Trust architecture will drastically improve SMUD's Cybersecurity risk. Zero-Trust architectures are data-centric and allows the concept of least-

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							privileged access to be applied for every resource access decision. In 2024, collaborating within IT and the business, cyber will continue to introduce and implement their strategic road map to implement a Zero-Trust architecture. • Continued to deploy Vulnerability Response and Management Strategy and Plan to support the delivery of secure information technology. In 2024, Cybersecurity will continue to strategically mature this capability by encouraging automation, where technically feasible, for patch management. • Continued implementing cybersecurity controls, information management processes, and technical solutions to enforce cybersecurity policies, procedures and standards aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework Security and Privacy Control families. • Continued building on the momentum and experience from achieving 100% pass rate for consecutive North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance audits. Cybersecurity's CIP Program Manager and team continued to ensure the implementation of new mandatory and enforceable regulatory standards, best practices, and internal controls while collaborating across multiple stakeholders to mature technology and process compliance implementations.
Operational: System	Data Privacy						SMUD continues to see demand for SMUD customer data to be used and shared for additional purposes and

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							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.
Operational: Process	Grid infrastructure T&D						Staff continues to implement ongoing T&D asset maintenance and multi-year replacement strategies using a risk-based approach, considering the assets' impacts to safety, load serving capability, reliability and regulatory compliance requirements. The 2024 Capital Portfolio includes completion of multi-year projects that are in flight and the start of projects to replace or upgrade substation transformers, circuit breakers and switchgear. The portfolio also includes funding for our ongoing pole replacement and cable replacement programs.
Operational: Process	Physical asset security						Security Operations continues its work to develop, update, and modernize security plans, policies, and procedures affecting the entire SMUD enterprise. Security Operations is also continuing to pursue implementation of additional physical security measures throughout our critical asset portfolio, such as installation/implementation of the following: thermal imaging cameras to detect intrusion at substations, ballistic protection for transformers within critical substations, enhancement and hardening of perimeters at both campus and substation locations, and expansion of the video management systems memory to preserve footage for a greater amount of time. In addition,

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							Security Operations is currently working towards providing recommendations for security risk mitigation in the UARP, as well as down selecting a leading security contractor firm in order to develop a comprehensive risk profile of all SMUD locations where personnel are located in order to better protect them.
Operational: Process	Power generation asset reliability						Staff has established processes to manage unexpected disruption to power generation and/or non-performance from power & gas contractual assets that threaten to cause partial or complete cessation of the day-to-day bulk power operations of SMUD. Staff continues to assess the reliability of SMUD's assets and performs standard maintenance and rebuilds where necessary to meet SMUD's current and future needs. In addition, staff continues to identify appropriate renewables resources in support of SMUD's zero carbon goals. See renewables projects for additional information.
External	Regulatory/legislative mandates						Staff continues to monitor and stay apprised of all regulatory/legislative mandates that have the potential to impact SMUD. Staff works through a formalized process to respond to these
Strategic	Renewables projects						In 2024 staff will continue to work to identify appropriate resources to meet SMUD's needs and move SMUD closer towards the achievement of its zero carbon goals. SMUD staff performed significant analysis and outreach, numerous studies, and a competitive solicitation of the market to identify future projects that meet SMUD's needs. Planned diversification of proven clean technologies and new technologies and business model evaluations ensure that the right projects and programs are selected to meet SMUD's goals in a

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
		[redacted]	[redacted]				reliable and affordable manner. In addition, SMUD staff participate in industry discussions and studies with regard to the development and implementation of new and updated Reliability Standards to ensure grid reliability and resiliency with the increased penetration of inverter-based resources into the grid. SMUD staff continue to plan and perform Capital and Operations and Management projects and work to ensure the reliability of existing and new generation assets and infrastructure supported by proven procedures, policies, and strategies as a part of SMUD's Asset Management Program.
Operational: Process	Safety: loss of life						Within SMUD Operations, the health & safety of our employees, contractors continue to be a primary focus. Integrated into our work processes are various mitigations that help SMUD reduce both the frequency and severity of incidents. We continue to ensure that we follow the guidance laid out in the Cal-OSHA Injury Illness & Prevention Program (IIPP). Key areas of risk mitigation measures that SMUD performs include safety responsibility awareness, OSHA regulatory compliance, safety communications, hazard assessments, accident/exposure investigations, hazard correction, safety training instruction, and recordkeeping. In addition, SMUD continues to operate an industry leading, behavior-based safety program called SCORCH. In the past year SMUD has continued to further integrate safety software solutions that has improved employee access to critical safety information, enhanced the ability to capture near miss reporting, and employee safety suggestions and concerns. SMUD continues to leverage best practices among the Utility

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							industry to drive down risk and improve operational performance.
External	Severe weather (incl wind, heat, lightning, capacity)						Climate change increases the frequency, intensity, and impacts of extreme weather events. These impacts have a high potential to impact SMUD's goals and operations. SMUD has conducted lessons learned after events and used those lessons to make process changes and plan for future events. Staff continues to conduct tabletop exercises for a number of hazard events such as storms, wildfires, heat waves, and gas pipeline to name a few. Doing so helps SMUD proactively identify gaps and address them, preparing SMUD for future events.
Operational: People	Strategic workforce planning: critical positions						In 2023 SMUD leadership began implementing action plans for each of the 59 roles identified as key through our Strategic Workforce Planning Program. These action plans encompass 110 different strategies that mitigate current and future risks associated with the key positions, as well as outlines steps to create new classifications that will be required to support work in the next 3-5 years. Directors and executives drive the action plans, which often require stakeholder partnerships and significant touchpoints in People Services and Strategies. Staff monitors progress and report status of action plans quarterly; due to the action plans being strategic and long-range in nature, staff will continue execution and tracking through 2024. Staff will also ask senior leaders to identify significant changes that require reassessing key roles. In 2024 staff expects to accomplish several impactful plans, such as creating a Data Scientist classification series and a Field Leader Training

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							Program. While the Data Scientist classification will facilitate getting new and important work done, it also helps attract new talent with diverse experiences and expands career opportunities and helps retain current employees. The Field Leader Training Program is another way SMUD is investing in its employees and maximizes employees chances of being successful in leading a team to accomplish core operational work. As background, staff assess all roles through Strategic Workforce Planning against several criteria: impact on strategy, turnover, cost of turnover, level of effort to backfill, operational impact, customer service impact, and performance variability. Leaders also describe positions that don't yet exist, but that would be needed for new types of work 3-5 years in the future. In 2022 the top 2% (59) of highest scoring roles based on these criteria were designated as "key" and reasons for the challenges or future anticipated challenges were captured. Action plans were created to identify how staff can address challenges, mitigating risk to the organization.
Operational: Process	Supply chain						Supply chain risk management (SCRM) efforts continues to mature in 2023. Staff has continued with weekly integrated business planning to manage supply and demand forecasts for key equipment supporting the new business pipeline, primarily distribution transformers. Internal coordination has continued to include the Chief Operating Officer (COO) and Chief Financial Officer (CFO) for inventory levels and risk of customer or project delays due to supply chain. In 2023, for the third year in a row, staff completed an annual SCRM risk assessment for all categories

2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							(materials/equipment, services/technology, and construction), the overall risk score for materials and equipment has gone down by 32%. Staff has reduced risk scores in 2023 by adding secondary suppliers, increasing safety stock values, increasing inventory on-hand, and by managing supplier performance. The new goal for 2023 is to establish more senior leadership involvement in managing critical third-party relationships, estimated to include the top 10 to 20 suppliers that are 60 to 80% of SMUD's spend and provide mission critical material, equipment, services, and technology has begun to develop with a few key relationships being managed at the executive level at least 1x per year including; distribution transformers, large power transformers, fleet vehicles/equipment, meters, and wood poles, this goal will continue in 2024.
Strategic	Transportation sector electrification/Unmanaged electrification						SMUD has been looking at the question of what electrification of buildings and transport will do to our grid for more than a decade. We continually improve our assessment approach as new data, forecasts, and technology change. This assessment process helps us plan for expected growth in a manageable way, to reduce the risk of us delaying connection of new electric loads. In addition, the assessment process enables us to have a clear picture of the potential impacts in an unmanaged and a managed world. Beyond assessment, we are actively piloting different approaches to managing charging to make sure that we can flatten out large new electric loads and accommodate as much of this new load as possible on our existing grid. In 2022 we launched a large-scale pilot of managed charging with three large OEMs and we've

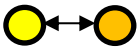
2023-2024 Risk Focus Areas

Attachment A

Risk Category	Risk	Year on Year Changes 2021	2022	2023	Risk Trend	Target	Risk Mitigation Activity(ies)
							expanded that in 2023 to continue to explore approaches to managing charging of light duty vehicles. We are also testing charge management and vehicle to grid functionality with school bus fleets and expect to expand our efforts in the broader commercial fleet space in 2024. With managed charging we anticipate being able to significantly reduce impacts to our grid, but at the same time recognize that we will need to also expand our grid's capacity to accommodate even a future where managed charging is widespread.
External	Wildfire						In 2023 staff continues to assess wildfire risks to SMUD and completed its triennial update of its Wildfire Mitigation Plan. The 2024 Capital and O&M budget include funds to continue implementation of SMUD's Wildfire Mitigation Plan.

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.

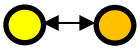
North Carolina State ERM Initiative and Protiviti Top 10 Enterprise Risks Specific to Energy and Utilities Industry		SMUD's Corresponding Risks	SMUD's Current Residual Risk Exposure
1	Rising threat associated with natural disasters and weather phenomena	**External risk:** Climate change Global pandemic Wildfire Severe weather	The current residual risk exposure ranges from medium to high 
2	Uncertainties in supply chain including the viability of key suppliers, scarcity of supplies, volatile shipping and delivery options, or stable prices in the supply chain ecosystem may make it difficult to deliver services	**Operational risk:** Supply chain	
3	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	

Attachment B

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

North Carolina State ERM Initiative and Protiviti Top 10 Enterprise Risks Specific to Energy and Utilities Industry		SMUD's Corresponding Risks	SMUD's Current Residual Risk Exposure
4	Changes in the overall work environment including shifts to hybrid work	**Operational risk:** Strategic workforce agility Operational excellence Diversity, equity, inclusion and belonging Change management Employee safety	
5	Organization's approach to managing ongoing demands on or expectations of a significant portion of workforce to "work remotely" or increased expectations for a transformed, collaborative hybrid work environment may negatively impact our ability to retain talent as well as the effectiveness and efficiency of how we operate our business.	**Operational risk:** Strategic workforce agility Operational excellence Diversity, equity, inclusion and belonging Change management Employee safety **Strategic risk:** 2030 Zero Carbon Plan Innovation	
6	Resistance to change in our culture may restrict our organization from making necessary adjustments to the business model and core operations	**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

North Carolina State ERM Initiative and Protiviti Top 10 Enterprise Risks Specific to Energy and Utilities Industry		SMUD's Corresponding Risks	SMUD's Current Residual Risk Exposure
7	Economic conditions (including inflationary pressures) in markets we currently serve may significantly restrict growth opportunities, impact margins, or require new skill sets for our organization	**Financial risk:** Interest rate Commodity Project execution **Operational risk:** Strategic workforce agility **External risk:** Legislative and regulatory Economic business agility	
8	The current interest rate environment may have a significant effect on the organization's capital costs and operations.	**Financial risk:** Interest rate Energy commodity Capital availability/cashflow Liquidity Wholesale credit default	The current residual risk exposure ranges from medium to high 
9	The adoption of digital technologies in the marketplace and in our organization may require new skills that either are in short supply in the market for talent or require significant efforts to upskill and reskill our existing employees.	**Operational risk:** Strategic workforce agility Operational excellence Diversity, equity, inclusion and belonging Change management **Strategic risk:** Innovation	
10	Anticipated increases in labor costs may affect our opportunity to meet targets	**Operational risk:** Strategic workforce agility Total rewards Change management **Strategic risk:** Innovation	

3

SSS No.
BOD 2023-012

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date
Policy – November 15, 2023
Board Meeting Date
N/A

TO		TO	
1.	Jennifer Davidson	6.	
2.	Suresh Kotha	7.	
3.	Brandy Bolden	8.	
4.	Farres Everly	9.	**Legal**
5.		10.	**CEO & General Manager**

Consent Calendar		**Yes**	x	**No** *If no, schedule a dry run presentation.*	**Budgeted**	x	**Yes**		**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
Dave Tamayo / Karen Wilfley	Board Office	B304	6154	10/22/23

NARRATIVE:

Requested Action: Allow the Board of Directors an opportunity to monitor existing policies: Governance Process GP-8, Board Committee Principles; Governance Process GP-12, Board Compensation and Benefits; Governance Process GP-15, Board Travel and Training Reimbursement**.**

Summary: A schedule to monitor Board policies was agreed upon by the Policy Monitoring Ad Hoc Committee. Monitoring established policies creates a better understanding of the policies and gives the Board an opportunity to make corrections, additions, or changes, if necessary.

Board Policy: *(Number & Title)* This monitoring supports GP-2 Governance Focus which states that the Board will direct, evaluate, and inspire the organization through the establishment of written policies which reflect the Board's values.

Benefits: Monitoring policies helps ensure the policies are current and in keeping with the current will of the Board.

Cost/Budgeted: Included in budget

Alternatives: Not review these policies at this time.

Affected Parties: Board of Directors

Coordination: Karen Wilfley, Senior Administrative Assistant to the Board Office

Presenter: Dave Tamayo, Policy Chair

Additional Links:

SUBJECT	ITEM NO. ***(FOR LEGAL USE ONLY)***
Board Monitoring of GP-8, GP-12, and GP-15	

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No.
BOD 2023-013

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date
Policy – November 15, 2023
Board Meeting Date
N/A

TO		TO	
1.	Jennifer Davidson	6.	
2.	Suresh Kotha	7.	
3.	Brandy Bolden	8.	
4.	Farres Everly	9.	**Legal**
5.		10.	**CEO & General Manager**

Consent Calendar		**Yes**	x	**No** *If no, schedule a dry run presentation.*	**Budgeted**	x	**Yes**		**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
Karen Wilfley for Dave Tamayo	Board Office	B304	6154	10/22/23

NARRATIVE:

Requested Action: Allow the Board of Directors an opportunity to discuss the four standing committees, Policy, Energy Resources and Customer Services, Strategic Development and Finance and Audit, and review committee charters.

Summary: The Board committees are Finance and Audit, ERCS, Strategic Development and Policy. By this discussion the Board will determine if these committees should continue as they currently stand.

Board Policy: *(Number & Title)* Reviewing the committee charters and standing committees on an annual basis gives the Board the opportunity to make any necessary changes to the charters and committees.

Benefits: This discussion supports Board policy GP- 8 Board Committee Principles (e) which states that the Board will review standing committees annually to determine whether they should continue as they currently stand.

Cost/Budgeted: N/A

Alternatives: Not review the committees or charters at this time.

Affected Parties: Board of Directors

Coordination: Crystal Henderson, Special Assistant to the Board

Presenter: Dave Tamayo, Policy Chair

Additional Links:

SUBJECT	ITEM NO. *(FOR LEGAL USE ONLY)*
Annual Review of Standing Committees	

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No.	Committee Meeting & Date
BOD 2023-014	Policy – 11/15/23
	Board Meeting Date: November 16, 2023

BOARD AGENDA ITEM
STAFFING SUMMARY SHEET

TO		TO	
1.	Jennifer Davidson	6.	
2.	Suresh Kotha	7.	
3.	Brandy Bolden	8.	
4.	Farres Everly	9.	**Legal**
5.		10.	**CEO & General Manager**

Consent Calendar		**Yes**	x	**No** *If no, schedule a dry run presentation.*	**Budgeted**	x	**Yes**		**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
Karen Wilfley for Dave Tamayo	Board Office	B304	6154	10/22/23

NARRATIVE:

Requested Action: Allow the Board of Directors an opportunity to discuss Board Officer positions for 2024.

Summary: The directors will discuss and make recommendations for Board President and Vice President for January through December of the upcoming year.

Board Policy: *(Number & Title)* Governance Process GP-5, Election of the Board President and Vice President states that "[t]he Board shall elect each year a president and vice president to preside over it…." This discussion supports the governance process.

Benefits: Having this discussion will allow the directors a forum to voice their choices for President and Vice President for the upcoming year.

Cost/Budgeted: N/A

Alternatives: Not select Board Officers at this time.

Affected Parties: Board of Directors

Coordination: Crystal Henderson, Special Assistant to the Board

Presenter: Heidi Sanborn, Board President

Additional Links:

SUBJECT	ITEM NO. ***(FOR LEGAL USE ONLY)***
Board Officers for 2024	

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No.
BOD 2022-014

BOARD AGENDA ITEM
STAFFING SUMMARY SHEET

Committee Meeting & Date
Policy Committee 11/15/23
Board Meeting Date
N/A

TO		TO	
1.	Jennifer Davidson	6.	
2.	Suresh Kotha	7.	
3.	Brandy Bolden	8.	
4.	Farres Everly	9.	**Legal**
5.		10.	**CEO & General Manager**

Consent Calendar		**Yes**	x	**No** *If no, schedule a dry run presentation.*	**Budgeted**		**Yes**		**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
Heidi Sanborn / Crystal Henderson	Board Office	B307	5079	12/22/2022

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 agenda items support the work of the Board.

Board Policy: *(Number & Title)* 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.

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: Costs included in budget.

Alternatives: Not review the Work Plan at this time

Affected Parties: Board and Executive staff

Coordination: Special Assistant to the Board

Presenter: Heidi Sanborn, Board President

Additional Links:

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

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No.
BOD 2022-018

BOARD AGENDA ITEM
STAFFING SUMMARY SHEET

Committee Meeting & Date
Policy Committee 11/15/23
Board Meeting Date
N/A

TO		TO	
1.	Jennifer Davidson	6.	
2.	Suresh Kotha	7.	
3.	Brandy Bolden	8.	
4.	Farres Everly	9.	**Legal**
5.		10.	**CEO & General Manager**

Consent Calendar		**Yes**	x	**No** *If no, schedule a dry run presentation.*	**Budgeted**		**Yes**		**No** *(If no, explain in Cost/Budgeted section.)*

FROM (IPR)	DEPARTMENT	MAIL STOP	EXT.	DATE SENT
Dave Tamayo / Crystal Henderson	Board Office	B307	5079	12/27/22

NARRATIVE:

Requested Action: A summary of directives provided to staff during the committee meeting.

Summary: The Board requested 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 Policy Committee Chair will summarize Board member requests that come out of the committee presentations for this meeting.

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

Benefits: Having an agenized 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: Included in budget

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

Affected Parties: Board of Directors and Executive Staff

Coordination: Special Assistant to the Board

Presenter: Dave Tamayo, Policy Chair

Additional Links:

SUBJECT	ITEM NO. ***(FOR LEGAL USE ONLY)***
Summary Of Committee Direction - Policy	

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.