

Board Policy Committee Meeting and Special SMUD Board of Directors Meeting

Date: Wednesday, November 12, 2025

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

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

Powering forward. Together.



AGENDA BOARD POLICY COMMITTEE MEETING AND SPECIAL SMUD BOARD OF DIRECTORS MEETING

**Wednesday, November 12, 2025
SMUD Headquarters Building, Auditorium
6201 S Street, Sacramento, California
scheduled to begin at 6:00 p.m.**

**Remote Telephonic Location:
33 East Nationwide Boulevard
Columbus, OH 43215**

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 Policy Committee's recommendation on the below agenda item(s):

Virtual Viewing or Attendance:

Live video streams (view-only) and indexed archives of meetings are available at:
<https://www.smud.org/Corporate/About-us/Company-Information/Board-Meetings/Watch-or-Listen-online>

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

Webinar/Meeting ID: 161 216 5830

Passcode: 327217

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:

- 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. Email is not monitored during 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. Steve Kustin
Kirsten DePersis
Kelsey McFadyen Discuss the monitoring report for **Strategic Direction SD-16, Information Management and Security**.
Presentation: 10 minutes
Discussion: 10 minutes
2. Jillian Rich Discuss the monitoring report for **Strategic Direction SD-17, Enterprise Risk Management**.
Presentation: 12 minutes
Discussion: 5 minutes
3. Gregg Fishman Discuss **Election of Officers for 2026** (President and Vice President) for the SMUD Board of Directors.
Discussion: 3 minutes
4. Heidi Sanborn Annual Review of Standing Committees.
Discussion: 1 minute

INFORMATIONAL ITEMS

5. Gregg Fishman Board Work Plan.
Discussion: 3 minutes
6. Public Comment
7. Heidi Sanborn Summary of Committee Direction.
Discussion: 1 minute

ANNOUNCEMENT OF CLOSED SESSION AGENDA

1. Threats of Public Buildings, Services and Facilities.

Pursuant to Section 54957 of the Government Code:

Consultation with: Suresh Kotha, Chief Information Officer;
Jose Bodipo-Memba, Chief Diversity Officer; Laura Lewis, Chief Legal &
Government Affairs Officer; Steve Kustin, Interim Director, Cybersecurity;
and Kirsten DePersis, 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 25-145

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date

Policy – 11/12/25

Board Meeting Date

November 20, 2025

TO					TO								
1.	Claire Rogers				6.	Farres Everly							
2.	Steve Kustin				7.								
3.	Scott Martin				8.								
4.	Suresh Kotha				9.	Legal							
5.	Brandy Bolden				10.	CEO & General Manager							
Consent Calendar		X	Yes	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	
David Bitter				Cybersecurity				K112		6901		10/21/25	
NARRATIVE:													
<p>Requested Action: Accept the monitoring report for Strategic Direction SD-16, Information Management and Security.</p> <p>Summary: Present the 2024-2025 Board Monitoring Report for SD-16, Information Management and Security.</p> <p>Board Policy: Strategic Direction SD-16, Information Management and Security (Number & Title)</p> <p>Benefits: Provides an update to the Board of Directors on the progress and status of Information Security, Privacy, and Records Management programs.</p> <p>Cost/Budgeted: Costs contained in internal labor budget.</p> <p>Alternatives: Receive information via memo or written report through the Chief Executive Officer and General Manager.</p> <p>Affected Parties: All SMUD Departments</p> <p>Coordination: Cybersecurity, Facilities, Security & Emergency Operations, and Information Management & Compliance</p> <p>Presenter: Steve Kustin, Interim Director, Cybersecurity Kirsten DePersis, Director, Facilities, Security & Emergency Operations Kelsey McFadyen, Program Manager, Information Management & Compliance</p>													

Additional Links:

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

SACRAMENTO MUNICIPAL UTILITY DISTRICT

OFFICE MEMORANDUM

TO: Board of Directors

DATE: October 29, 2025

FROM: Claire Rogers *CR 10/29/25*

**SUBJECT: Audit Report No. 28007875
Board Monitoring Report; SD-16: Information Management and
Security**

Internal Audit Services (IAS) received the SD-16 *Information Management and Security* 2025 Annual Board Monitoring Report and performed the following:

- Selected a sample of statements and assertions in the report for review.
- Compared sample to the corresponding supporting documentation to identify potential discrepancies.

All items sampled within the SD Report aligns with the supporting documentation provided at the time of review.

CC:

Paul Lau

Board Monitoring Report 2025

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) **Cybersecurity:** SMUD will protect customer, employee and third-party information, and SMUD technology 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 or employee 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 and employee information.
- d) **Information Management:** SMUD will maintain the efficient and systematic control of the creation, capture, identification, receipt, maintenance, use, disposition, and destruction of SMUD information, in accordance with legal requirements and Board policies.

2) Executive summary

- a) SMUD's Cybersecurity, Physical Security, Customer Privacy, and Information 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 technology systems, cyber and physical security, privacy, and information 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
Cybersecurity: protect systems and information from unauthorized access	Cybersecurity 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: Notify customers about use of information	Annual notice of privacy practices	Notify customers of our privacy practices	Notice sent in the May bill package	Changes this year explain information use and the purpose of the notice
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 robust cybersecurity programs to protect SMUD information	
Customer Privacy: Identify 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	
Information Management: Identify and manage records and information	Records Evaluations and Information Migration	Evaluate, classify and migrate records, and ensure retrieval, disposal and protection.	Migration of 35 out of 40 total business areas with expected completion of 40 by end of 2025, for an estimated 7 million documents migrated and classified.	
Information Management: Ensure all information systems are compliant with IMC best practices and requirements	Data Loss Prevention	Implementation of tools and policies in information repositories	Creation of a sustainable model for SMUD to classify/label documents and prevent inappropriate distribution and access.	
Physical Security:	- Annual Workplace Violence Training	Proactively equip employees and	Increased employee awareness and	Despite improvements,

Safeguard employees while at work	<ul style="list-style-type: none"> - Situational Awareness Training for Field Crews & Awareness Campaign - Civil Standby by Law Enforcement - Beakon Threat Awareness Tool - Mandatory ballistic vests for Officers 	visitors to recognize, report, and respond to workplace threats, ensuring security at SMUD facilities.	preparedness significantly reduce the risk and impact of workplace violence, fostering a culture of safety & vigilance at all SMUD sites.	workplace violence risks persist; ongoing training and law enforcement collaboration remain essential.
Physical Security: Safeguard customers & visitors at SMUD facilities	<ul style="list-style-type: none"> - CSC Lobby Improvements - Security Presence in Public Lobbies - Risk Threat Vulnerability Assessment (RTVA) - Event Metal Detection - Board Meeting Security - VOA Partnership 	Create a welcoming yet secure environment for customers & visitors by mitigating risks related to physical safety, theft & privacy at SMUD facilities.	Enhanced security controls & physical modifications ensure customer & visitor safety, minimize incidents & maintain trust in SMUD's commitment to protect its interests.	Security improvements reduce risks, but challenges with disgruntled customers and the unhoused require ongoing vigilance and adaptive measures.
Physical Security: Protect overall operation from unauthorized access or disruption	<ul style="list-style-type: none"> - Design & Budgeting of Folsom Administrative Office Building - Perimeter Intrusion Detection Systems at Critical Impact Protection Sites - UARP Technology - No Findings for NERC Audit - Physical Access Control System (PACS) 	Ensure uninterrupted operations by preventing unauthorized access and disruptions at critical sites using advanced security technology and compliance.	Implementation of robust physical access controls & detections systems results in higher operational resilience, regulatory compliance & reduced risk of operational disruptions.	Controls reduce vulnerabilities but evolving threats require continuous assessment and updates.

3) Additional supporting information

Cybersecurity

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

SMUD's Cybersecurity program continues to evolve and mature to keep pace with the evolving cyber threats we face and to manage our cyber, privacy, legal, regulatory and compliance risk. This includes the adoption of a Zero Trust Architecture strategy, aligned to the Technology and security excellence objective of SMUD's 2025 Enterprise Strategy. The program aligns to 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 six core functions of the CSF (Identify, Protect, Detect, Respond, Recover, and Govern) 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

SMUD is committed to safeguarding the safety and well-being of its employees, customers, and visitors across all facilities. Recognizing the various risks—including workplace violence, disgruntled customers, civil unrest, and challenges posed by an open campus—SMUD has implemented comprehensive initiatives to create a secure environment. For employees, mandatory annual workplace violence and situational awareness training equip staff to recognize and respond to potential threats, while campaigns like “See Something, Say Something” and “Power of Hello” promote vigilance and communication. Asset protection officers are now equipped with ballistic vests, and partnerships with law enforcement provide civil standbys and threat intelligence support through tools such as Beakon. For customers and visitors, security enhancements focus on high-traffic, customer-facing areas with measures such as lobby redesigns for improved visibility, increased security presence, and metal detection for large or high-risk events. Ongoing Risk Threat Vulnerability Assessments guide targeted improvements, and visible security presence at Board meetings ensures public safety. Collaboration with community partners like Volunteers of America further strengthens social support and security around facilities, particularly addressing vulnerabilities related to unhoused populations. Through these combined efforts, SMUD fosters a vigilant, prepared, and welcoming environment for all who work at and visit its premises, while maintaining ongoing vigilance to address emerging threats.

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.

Protecting electric system infrastructure is essential to SMUD’s mission of reliable power delivery. Substations, control centers, and transmission sites face threats such as theft, vandalism, trespassing, and terrorism. SMUD applies stringent security standards, advanced surveillance technologies—including mobile trailers, thermal radar, Perimeter Intrusion Detection Systems (PIDS), and CCTV—and landscape hardening with enhanced fencing to secure these sites. Integration with Computer Aided Dispatch (CAD) and Letters of Agency with local law enforcement ensure swift incident response and information sharing. Ongoing technology upgrades, such as those addressing security gaps at the Upper American River Project, align with FERC and internal recommendations. SMUD’s zero-findings 2025 NERC audit validates the effectiveness of current controls, though continuous monitoring and innovation remain critical to counter evolving threats.

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 clearer about its purpose and to be easier to understand. The notice continues to include plain language regarding SMUD's collection, use, and release of customer sensitive and confidential information, the business purposes for which it 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.

Where business requires sensitive and confidential information to be shared with a third party, Cybersecurity's risk management team evaluates third party artifacts, attestations, and independent reports to ensure that robust information practices are in place sufficient to protect customer information. The American Institute of CPAs (AICPA) Service Organization Control 2 (SOC 2) Type 2 continues to be our 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. This year the request form was updated to require clear declaration when a request is for non-SMUD business purposes.

Information Management

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

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 migrated content from 35 business areas out of 40, with expected completion of 40 by end of 2025, for an estimated total of 7 million documents classified and migrated. The project has identified, organized, and migrated content for each business area from non-approved records repositories into approved record repositories. This allows content to be managed in accordance with SD-16.

Information Management & Compliance is partnering with Cybersecurity and Organizational Change Management to implement a Data Loss Prevention (DLP) program. This initiative establishes a sustainable governance model to classify and protect sensitive information, monitor at-risk activities, and reduce the risk of data breaches. It is critical for ensuring regulatory compliance, safeguarding our reputation, and protecting the organization from potential financial and operational impacts. 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

Cybersecurity

Industry and federal partners and agencies all continue to warn SMUD and the industry of the heightened geopolitical tension and associated nation state cyber actors targeting critical infrastructure. Cybersecurity takes these warnings seriously, ingesting threat intelligence and taking precautions to protect against known attacks and threat actors. Mandatory annual training and year-round awareness activities keep employees informed of the risks we face and their role in keeping things secure. Additionally, Cybersecurity participated once again in efforts to ensure we maintain cybersecurity insurance.

AI has brought a new set of risks and challenges this year. The Cybersecurity team has been involved to ensure that the risks associated with AI are appropriately understood and managed.

SMUD's current Payment Card Industry (PCI) card payment transaction volume continues to classify SMUD as a PCI Level 2 Merchant. Each year SMUD engages a third-party Payment Card Industry Professional (PCIP) to validate our compliance. All required assessment documents attesting to our compliance were submitted to Chase Paymentech in June.

The Cybersecurity team continues to work hard to ensure compliance with the NERC Critical Infrastructure Protection (CIP) standards. This year was our triennial CIP compliance audit, where we not only had zero findings, but received two positive observations. The CIP team is now preparing for additional standards which become enforceable in 2026 and beyond, requiring additional resources not only from the Cybersecurity team but from others as well.

Our Zero-Trust Cybersecurity Strategy remains a core part of IT work, and positions SMUD to secure sensitive data, systems, and services. IT continues to make progress in this area, working with Cybersecurity to ensure upcoming projects and efforts align to this strategy.

Physical Security

Physical Security remains SMUD's frontline defense for its people, facilities, and infrastructure. A current comprehensive Risk Threat Vulnerability Assessment (RTVA) is identifying gaps in staffing, technology, access controls, and processes needed to address evolving threats such as unauthorized access and sophisticated disruptions. Early findings highlight vulnerabilities in perimeter security, remote site protection, and response capabilities, especially within the open campus environment and substations. Since 2014, SMUD's growth has outpaced security enhancements, necessitating a critical reassessment similar to recent cybersecurity investments. The RTVA will guide improvements in resources, technology, and operations to ensure regulatory compliance and industry best practices, enabling SMUD to effectively safeguard its assets, people, and business continuity amid increasing risks and complexity.

Customer Privacy

We continue to receive SMUD customer data sharing requests for regulatory, compliance, municipal collaboration, and internal program needs related to SMUD business purposes. In rare cases data is requested to be shared for purposes that are not considered primary or core SMUD business, and in those situations the data is aggregated or de-identified before sharing so it is no longer considered personally identifiable information (PII).

Information 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 policies/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 DLP program is now in the pilot phase, testing the solution's sensitivity labels with selected teams, gathering feedback to refine technical rules, training, and communications. This work will reduce the risk of data breaches, reputational harm, and costly regulatory fines, while building a sustainable governance model for information protection 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

AICPA – American Institute of CPAs

SOC 2 – Service Organization Control 2

IMC – Information Management & Compliance

ECM – Enterprise Content Management

DLP – Data Loss Prevention

PCI – Payment Card Industry

PCIP – Payment Card Industry Professional

CIP – Critical Infrastructure Protection

CEOP – Cybersecurity Emergency Operations Program

RTVA – Risk Threat Vulnerability Assessment

SSS No. CFO 25-015

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date

Policy – 11/12/25

Board Meeting Date

November 20, 2025

TO					TO				
1.	Claire Rogers				6.				
2.	Scott Martin				7.				
3.	Brandy Bolden				8.				
4.	Farres Everly				9.	Legal			
5.	Suresh Kotha				10.	CEO & General Manager			

Consent Calendar	X	Yes	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
Jillian Rich	Enterprise Strategy & Planning	B356	6454	10/17/25

NARRATIVE:

Requested Action:

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

Summary:

The Enterprise Risk Management Report summarizes activities that have occurred since the November 2024 annual report. It includes historical risk profiles for the enterprise risk focus areas of 2024-2025, mitigation strategies, and the current residual risk exposure status of identified enterprise risks.

Board Policy:

Strategic Direction SD-17, Enterprise Risk Management

Board Policy:

(Number & Title)

Benefits:

Provide the scheduled monitoring report as requested by the Board of Directors and Executive staff. The report provides an opportunity to make recommendations or policy revisions, as necessary.

Cost/Budgeted:

Costs are contained within the budget for internal labor.

Alternatives:

Provide via written report through the Chief Executive Officer and General Manager.

Affected Parties:

Board of Directors, Executive Office

Coordination:

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

Presenter:

Jillian Rich, Manager, Enterprise Strategy & Risk

Additional Links:

SUBJECT	Strategic Direction SD-17, Enterprise Risk Management Monitoring Report	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: October 29, 2025

FROM: Claire Rogers *CR 10/29/25*

**SUBJECT: Audit Report No. 28007876
Board Monitoring Report; SD-17: Enterprise Risk Management**

Internal Audit Services (IAS) received the SD-17 *Enterprise Risk Management* 2025 Annual Board Monitoring Report and performed the following:

- Selected a sample of statements and assertions in the report for review.
- Compared sample to the corresponding supporting documentation to identify potential discrepancies.

All items sampled within the SD Report aligns with the supporting documentation provided at the time of review.

CC:

Paul Lau

Board Monitoring Report 2025

SD-17 Enterprise Risk Management



1) Background

Strategic Direction 17 states: 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

SMUD is in compliance with SD-17, Enterprise Risk Management.

In 2025, staff modernized our Enterprise Risk Management (ERM) framework in response to a 2024 maturity assessment conducted by KPMG, a global consulting firm. The refreshed framework is now complete and will be used as the basis for risk monitoring, reporting and decision-making going forward.

SMUD's new risk framework:

- provides a cross-functional, top-down view of risk that allows staff, executives and the Board to discuss risk more holistically before examining details;
- increases alignment to SMUD's Strategic Direction;
- includes detailed risk definitions and an enhanced rating system to more clearly communicate risk; and,
- conveys the impact of mitigations and controls by tracking our risk environment level (inherent risk) separately from remaining risk (residual risk).

While the risk refresh was in process, SMUD continued to strategically manage risk in a way that proactively reduced the chance of loss. For example, action at the Federal level caused several risks to escalate in the first half of the year, including those related to renewable energy projects, the economy, grants and supply chain. SMUD increased its monitoring and communication around these risks and introduced additional mitigations and safeguards where possible.

Our new risk framework is a baseline against which future changes will be compared. The changes we made in our former risk framework to supply chain, economic, grant, and renewable project risk are included in the new risk levels outlined below. Our strategic risks have the following residual ratings:

Strategic Risk	Residual Risk Level
Safety & Security: Risks related to safety and security events involving our people, community and critical assets.	Medium-High
Financial: Risk related to our affordable rates.	Medium-High
Environmental: Risks related to our clean energy goals and environmental stewardship.	Medium
Reliability: Risk related to keeping the lights on.	Medium
Process & Technology: Risk related to our operational support systems, processes, and technologies.	Medium
Customer & Community: Risks related to SMUD's engagement with customers and the community.	Low
Our People: Risk related to building an inclusive, engaged and future-ready workforce.	Low

These risk ratings account for the potential impact of the risk, the likelihood of it occurring, and how quickly SMUD would have to respond should the risk occur. A low risk rating does not mean low priority. If anything, it means that the risk has fewer influences outside of our control. For instance, we cannot influence global politics that may impact supply chain and cybersecurity risk, but we have significant influence over our employee experience.

Moving forward, SMUD will continue to monitor bottom-up risk and communicate it through our new risk framework. Our 2026 work plan will focus on further improving our risk-aware culture, launching new training and tools for business area leaders to identify, manage and communicate risk consistent with our new framework.

3) Additional supporting information

a) 2025 ERM Program Highlights

In 2025, SMUD's ERM program:

- finished a refresh of the enterprise risk framework to better communicate, anticipate, and accommodate our changing risk landscape,
- continued to support the organization in the facilitation of risk conversations and embedding risk into our decision-making, such as prioritization decisions,
- enhanced cross-functional governance and thorough understanding of major risk issues by leveraging six committees: the Enterprise Risk Oversight Committee (EROC), Risk Champions Network (RCN), Trading Operations Risk Committee (TORC), Reliability committee, and Zero Carbon Plan Steering Committee, and Three Lines of Defense Working Team,
- made several updates to risk levels and took corresponding action, largely in response to new Federal policy changes,
- updated our uniform risk rating rubric to include more specific key risk indicators, and



- created new dashboards, reports and tools to better communicate, monitor, compare, rate and update risks.

Attachment A provides further details about our 7 Strategic Risks, which are broken down into 26 sub-risks or Enterprise Risks. The attachment includes:

- Risk definitions & Strategic Direction (SD) alignment
- Risk scores: Subject matter experts and senior leaders rated each risk based on the potential cross-functional impacts, the likelihood of the risk occurring, and the speed at which SMUD would have to respond should the risk occur. There are two ratings per risk: the risk environment (inherent risk) if SMUD did nothing to control or mitigate the risk and remaining risk (residual risk) after SMUD mitigations and controls are considered. We use the following scale:

Level	Risk Level	ERM significance (residual risk)
L	Low	Risk is mitigated to a low level. ERM reviews periodically.
M	Medium	Risk is moderately mitigated. ERM reviews periodically.
MH	Medium High	Risk is moderately mitigated. ERM monitors regularly.
H	High	Considered a focus area for risk mitigation. ERM monitors regularly.
EH	Extremely High	Risk is immediate and substantial resources are needed to mitigate risk.

- Risk forecast: Anticipated trend for the coming year based on key risk indicators and subject matter expert opinion:

Risk level may increase	Risk level expected to be maintained	Risk level may decrease
	=	

b) 2025 Risk Management Highlights

SMUD completed several efforts in 2025 that either reduce the impact of risk or demonstrate that our current controls and mitigations are performing as expected. Highlights of those efforts are provided below.

2025 Risk Highlight	Strategic Risk(s)	Description
Prudent fiscal management	Financial	In 2025, we took several actions to preserve our strong financial health including securing a \$91M direct Investment Tax Credit payment and setting aside funds in reserves and stabilization funds to ensure funding availability and mitigate any rate impacts for customers.

2025 Risk Highlight	Strategic Risk(s)	Description
Enhanced field safety	Safety & Security	We improved field safety by deploying advanced communication technologies, including radio repeaters and Starlink satellite connectivity. These enhancements ensure reliable and continuous communication for field crews, especially in remote or disaster-affected areas, supporting safer and more efficient operations.
Rate case below inflation	Customer & Community	With SMUD's approved rate changes for 2026-2027, our rates remain among the lowest in California, which positively impacts our risks related to customer affordability and inclusive economic development.
Western Electricity Coordinating Council (WECC) audit	Reliability	We successfully completed the 2025 WECC audit with no non-compliance findings, demonstrating strong adherence to reliability standards and effective operational controls.
Innovative technologies	Process & Technology	We piloted new robotics to assist substation maintenance workers with daily tasks such as sulfur hexafluoride (SF6) gas monitoring, infrared inspections, and partial discharge testing.

c) Global Risk Trends & Benchmarking

SMUD's ERM program actively monitors global risk trends and compares our risk landscape to that of others in the energy industry to stay ahead of potential changes.

Global risk trends impacting SMUD in 2025-2026:

- **Affordability:** Rising costs and uncertainty driven by supply chain disruptions, inflation, tariffs and escalating labor expenses put additional financial pressure on utilities. This heightens the risk of continuing to meet our affordability goal and may increase cost of living pressures for our customers in general, particularly those in vulnerable communities.
- **Supply Chain Disruptions:** Delays in delivery times, changing expectations for service agreements and increased costs for equipment – including transformers, materials and technology – affect the way the utility industry approaches grid modernization and expansion of clean energy resources.
- **Regulatory and Policy Uncertainty:** Rapidly changing policy decisions such as those related to Federal funding priorities pose significant challenges for long-term planning and capital investment decisions. These uncertainties can lead to unexpected costs and potential delays in project execution.
- **Climate change and weather-related impacts:** Climate change continues to be a major driver of uncertainty for utilities. Increased frequency and severity of wildfire, heatwaves and severe storms poses a threat to grid resiliency and

critical assets. Additionally, the costs associated with structure hardening, vegetation management and advanced monitoring systems is driving the need for greater risk-based decision-making for the replacement and maintenance of our assets.

- **Technology Integration:** The integration of new, cloud-based technologies and distributed energy resources introduces great opportunity for utilities and also several challenges. Challenges include changing cybersecurity vulnerabilities and the need for standards development to address the regulatory and compliance implications of integration.

These global risk trends are also impacting our peers in the energy industry. As in previous years, SMUD relied on the North Carolina State University's (NCSU) Enterprise Risk Management Initiative and Protiviti [2025 & 2035 Executive Perspectives on Top Risks](#) for a benchmark of short-term and long-term risks from 1,215 global board members and executives.

Attachment B compares SMUD's top enterprise risks to the top 10 Energy and Utility risks identified in NCSU and Protiviti study. Overall, SMUD's refreshed risk framework aligns to the industry benchmarking and will allow us to make productive comparisons with our peers moving forward.

d) Looking forward

In 2026, ERM will work with leaders to continue to mature ERM at SMUD based on the KPMG recommendations of standardization, prioritization, aggregation and interconnectedness of risks. Staff will facilitate executive leadership in the development of risk tolerances and key risk indicators to enhance decision-making and greater understanding of strategic priorities. We will also provide staff with tools, education, and escalation processes to increase risk awareness and reporting.

4) Challenges

Today's risk environment is increasingly becoming more complex, interconnected and fluid. In response, the refreshed enterprise risk management framework looks holistically across the organization to identify and mitigate risk cross-functionally. Moving to an approach that identifies and manages risk both from a top-down and bottom-up perspective will improve risk governance across the enterprise, our ability to identify and manage emerging risks, and provide management with improved quantitative tools to make resource decisions.

5) Recommendation

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

6) Appendices

Attachment A: New Strategic and Enterprise Risks

See Section 3a of this report for the legend. For risks with a positive or negative forecast, we include a rationale in the last column entitled “forecast notes”.

Strategic Risk <i>Enterprise Risk</i>	2025 risk rating			2025 mitigation and control accomplishments
	Inherent	Residual	Forecast	
Safety & Security (SD-6; SD-16) Risks related to safety and security events involving our people, community and critical assets.	H	MH		<ul style="list-style-type: none"> Increased employee/supervisor safety interactions, which are preventative communications to help identify and remove barriers to safe work Enhanced safety training qualifications for contractors Invested in enhanced ergonomics and safety tools such as car mounts for navigation devices and improved tower grounding safety gear Implemented Privileged Access Management improving permissions for critical systems Continued implementation of our Zero Trust cybersecurity strategy and program aligned to National Institute of Standards & Technology (NIST) Initiated third-party risk management process enhancements including the acquisition of a third-party risk management application, additional monitoring and reporting tools, and a new third-party and cybersecurity governance committee
Safety There is a risk that the safety of our employees, contractors, and public will be compromised.	H	L	=	
Physical Security There is a risk that SMUD-owned property and assets will be accessed by unauthorized individuals.	H	M	=	
Cybersecurity There is a risk that SMUD's data, information assets, systems and networks will be accessed by unauthorized individuals or groups.	EH	H	=	
Third-Party There is a risk that a third party will fail to represent SMUD's interests, standards or expectations.	H	MH	=	

Strategic Risk <i>Enterprise Risk</i>	2025 risk rating			2025 mitigation and control accomplishments
	Inherent	Residual	Forecast	
Reliability (SD-4; SD-14) Risk related to keeping the lights on.	H	M		<ul style="list-style-type: none"> On track to meet 2025 System Average Interruption Frequency Index (SAIFI) and System Average Interruption Duration Index (SAIDI) reliability limits Completed the North American Electric Reliability Corporation (NERC) audit with no findings Introduced a new compliance tracking interface for Power Generation assets Inspected transmission line towers, including an advanced assessment of towers in the High Fire Threat District in the Upper American River Project (UARP) Patrolled thousands of miles of transmission and distribution overhead lines Continued to improve storm response, including more accurate estimations and enhanced communication Enhanced vegetation management with new data collection applications to improve patrol efficiency and geospatial tracking Trimmed tens of thousands of trees to reduce wildfire and storm risk Completed and received approval from Federal Emergency Management Association (FEMA) for the 2024-2028 Hazard Mitigation Plan Updated the Wildfire Mitigation Plan Enhanced remote monitoring solutions at thermal plants
Resource Adequacy There is a risk that SMUD's electricity load could exceed available supply.	H	M	=	
System Adequacy There is a risk that SMUD's transmission and distribution equipment could be insufficient for current and future capacity requirements.	H	M	=	
Operational Adequacy There is a risk that SMUD's asset capabilities could be insufficient or our resources too inflexible to reliably operate SMUD's system or interact with the interconnected grid.	H	MH	=	
Grid Resiliency There is a risk that SMUD's critical infrastructure may not be resilient to hazards such as wildfire, extreme weather or other natural and man-made disruptions.	H	M	=	
Reliability Compliance There is a risk that SMUD's internal controls are inadequate, that SMUD is unable to evolve with changing regulatory requirements, and that SMUD may not comply with applicable laws and regulations.	H	L	=	

Strategic Risk <i>Enterprise Risk</i>	2025 risk rating			2025 mitigation and control accomplishments
	Inherent	Residual	Forecast	
Environmental Risk (SD-7; SD-9) Risks related to our clean energy goals and environmental stewardship.	H	M		<ul style="list-style-type: none"> Continued progress on multiple utility-scale projects including Country Acres, Coyote Creek, Curry Creek, Grace, Hatchet Ridge, Oveja Ranch, Sunzia, and Terra-Gen Completed Sloughhouse Solar Finished the Cosumnes Power Plant turndown project Implemented a new customer facing online residential electrification tool to support education and awareness of building decarbonization technologies Reached a major building electrification milestone with 20,000 heat pump heating ventilation and air conditioning (HVAC) systems incentivized to date Advanced the Energy Management System (EMS) upgrade project enabling enhanced renewable integration, system monitoring, and control supporting our transition to clean energy resources Implemented the Habitat Conservation Plan focused on endangered species protection <p>Forecast notes:</p> <ul style="list-style-type: none"> Staff anticipates that Clean Energy Resources and Community Decarbonization risks will increase as we adjust to the changing priorities of Federal funding like tax credits and grants.
Clean Energy Resources There is a risk that the transition to clean energy resources could be delayed or be insufficient to meet regulatory requirements.	H	MH	↑	
Community Decarbonization There is a risk that our customer programs may not effectively decarbonize buildings and vehicles in the region.	H	MH	↑	
Environmental Stewardship There is a risk that inadequate environmental stewardship or non-compliance with environmental rules and regulations could occur.	MH	M	=	
Climate Change There is a risk that the escalating impacts of climate change, including extreme weather events, rising temperatures, and loss of snowpack could impact our operations and infrastructure.	H	MH	=	

Strategic Risk <i>Enterprise Risk</i>	2025 risk rating			2025 mitigation and control accomplishments
	Inherent	Residual	Forecast	
Customer & Community Risk (SD-5; SD-12; SD-13; SD-15) Risks related to SMUD's engagement with customers and the community.	M	L		<ul style="list-style-type: none"> Extensive market research and customer preference testing prior to launching new customer messaging or offerings like the new smud.org going live in 2026 Executed our Community Impact Plan to support energy efficiency and electrification for communities that need it most Expanded lobby days to encourage customers to enroll in our Customer Assistance offerings like the Energy Assistance Program Rate (EAPR) and Medical Equipment Discount (MED) rate Launched our new Solar & Storage for Nonprofits program Maintained high customer satisfaction and Value for What You Pay Delivered educational courses, hosted community events, and supported extensive volunteer and tree planting activities Deployed the Smart Energy and Water (SEW) Enterprise Portal for commercial customers Received Catalyst grant funding to conduct feasibility study on regional utility worker training program Funded Shine awards and supported Sustainable Communities partners Held the 2025 Meet the Buyers & Business Resource Expo to promote local business participation in our operations
Customer Experience There is a risk of not meeting customer expectations.	MH	L	=	
Reputational There is a risk of lost credibility with the community, industry partners, board and/or governmental entities.	MH	M	=	
Inclusive Energy Transition There is a risk under-resourced populations may bear an undue burden of the zero carbon transition.	M	L	=	
Inclusive Economic Development There is a risk Sacramento's regional economy may not thrive or may not benefit all communities equally.	L	L	=	
Customer Affordability There is a risk customers may be unable to reduce their electric energy bill burden.	M	L	=	

Strategic Risk <i>Enterprise Risk</i>	2025 risk rating			2025 mitigation and control accomplishments
	Inherent	Residual	Forecast	
Financial Risk (SD-2; SD-3; SD-11; SD-19) Risk related to our affordable rates	H	MH		<ul style="list-style-type: none"> Planned for future risks and market volatility to ensure rate stability for customers by fully funding insurance reserves and stabilization funds Received \$91.7 million investment tax credits for Solano 4 Wind project Supported our grant strategy, securing funding for our efforts despite shifts in focus for Federal funding Issued the nation's first green commercial paper by a municipal utility Received Fitch (AA) and Moody's (Aa2) rating affirmations maintaining low borrowing costs Reduced costs by consolidating the SMUD Financing Authority (SFA)
<i>Economic Conditions & Financial Management</i> There is a risk of rising costs and unpredictable economic fluctuations.	H	M	=	
<i>Commodity Management</i> There is a risk of increasing volatility in commodity prices or supply.	H	MH	=	
Process & Technology Risk (SD-10; SD-16) Risk related to our operational support systems, processes, and technologies.	H	M		
<i>Technology Systems</i> There is a risk that technology systems may not meet the current and future needs of the organization.	H	M	↑	
<i>Data Governance & Privacy</i> There is a risk of data integrity and and/or unauthorized access, disclosure, or misuse of personal or sensitive information.	H	M	↓	
<i>Supply Chain</i> There is a risk of supply chain disruptions and unavailability of resources.	H	M	=	

Forecast notes:

- Staff anticipates that Technology Systems will increase in the coming year with the implementation of multiple technology upgrade projects, including an enterprise-wide transformational effort SAP S/4HANA

Strategic Risk <i>Enterprise Risk</i>	2025 risk rating			2025 mitigation and control accomplishments
	Inherent	Residual	Forecast	
Artificial Intelligence (AI) & Emerging Technologies There is a risk of effective integration of Artificial Intelligence into SMUD's business models.	M	L	↑	<ul style="list-style-type: none"> Data Governance & Privacy risk will decrease in the coming year with the completion of our Data Loss Prevention Project AI & Emerging Technology risk at SMUD is well controlled, but staff anticipates an increase in risk exposure as new and emerging technologies are incorporated into SMUD's existing systems and business models Expanded summer internships Launched new Paid Family Leave and enhanced disability insurance benefits Updated job descriptions and conducted analysis to align compensation and broader market trends Enhanced our efforts to ensure a pipeline of talented leaders for now and the future Launched a new employee recognition platform
Our People Risk (SD-8; SD-12) Risk related to building an inclusive, engaged and future-ready workforce	H	L		
Talent Management There is a risk of attracting or retaining talent with the skillsets to meet business needs.	H	L	=	
Employee Experience There is a risk of employee turnover and disengagement.	M	L	=	
Strategic Workforce There is a risk that the skills and talent of the current workforce may not align with future business objectives.	H	L	=	

Attachment B: Risk Benchmarking

Below is a comparison of SMUD's new risk framework to industry benchmarking provided by North Carolina State University (NCSU) and Protiviti in the [2025 & 2035 Executive Perspectives on Top Risks](#).

Overall, the study found that risks are becoming increasingly interrelated and pose significant challenges to current business models and the ability of modern organizations to be resilient and agile. Energy and utility executives are increasingly concerned that climate-related trends and evolving policies are significantly reshaping the energy and utilities industry, presenting both risks and opportunities. Key worries include the financial impact of transitioning to clean energy resources, costs tied to infrastructure upgrades for grid resiliency tied to wildfire and extreme weather events, and uncertainties stemming from shifting regulatory landscapes.

Nationwide, Executives recognize the need to accelerate decarbonization efforts and grid modernization while managing affordability and reliability for customers. There is also a strong focus on leveraging new technologies and business models to capitalize on emerging opportunities, but concerns remain about supply chain constraints, cybersecurity threats, and the pace of policy changes that could affect long-term planning and investment decisions. Climate change is seen as a driving force requiring adaptable strategies to ensure sustainable, reliable, and cost-effective energy delivery.

NCSU ERM Initiative and Protiviti Top 10 near-term risks, Energy & Utilities, abbreviated and ranked	SMUD corresponding enterprise risks and residual risk level	
1. Climate change	Climate Change	MH
2. Regulatory changes and scrutiny	Reliability Compliance	L
3. Catastrophic natural disasters and weather	Grid Resiliency	M
4. Increasing labor costs	Economic Conditions & Financial Management	M
5. Supply Chain	Supply Chain	M
6. Geopolitical shifts, regional conflicts and instability	Supply Chain	M
7. Economic Conditions	Economic Conditions & Financial Management	M
8. Talent and labor availability	Talent Management	L
9. Global markets and trade policies	Supply Chain	M
10. Third-party risks	Third-party	MH

SSS No. BOD 2025-015

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date

Policy – 11/12/25

Board Meeting Date

November 20, 2025

TO				TO			
1.	Farres Everly			6.			
2.	Suresh Kotha			7.			
3.	Brandy Bolden			8.			
4.				9.	Legal		
5.				10.	CEO & General Manager		
Consent Calendar		<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	Budgeted		<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<i>If no, schedule a dry run presentation.</i>				<i>(If no, explain in Cost/Budgeted section.)</i>			
FROM (IPR)		DEPARTMENT		MAIL STOP		EXT.	
Heidi Sanborn / Crystal Henderson		Board Office		B307		6155	
						DATE SENT	
						10/14/25	
NARRATIVE:							
<p>Requested Action: Discuss, with possible action, Election of Officers for 2026 (President and Vice President) for the SMUD Board of Directors.</p> <p>Summary: The Directors will discuss and make recommendations for Board President and Vice President for January through December of the upcoming year.</p> <p>Board Policy: Governance Process GP-5, Election of the Board President and Vice President states in pertinent part that, (Number & Title) “[t]he Board shall select each year a president and vice president to preside over it...” This discussion supports the governance process.</p> <p>Benefits: Having this discussion will allow the directors a forum to voice their choices for President and Vice President for the upcoming year.</p> <p>Cost/Budgeted: There is no budgetary impact for this item.</p> <p>Alternatives: Not select Board Officers at this time.</p> <p>Affected Parties: Board of Directors</p> <p>Coordination: Board Office</p> <p>Presenter: Gregg Fishman, Board President</p>							

Additional Links:

SUBJECT

Election of 2026 Board Officers

ITEM NO. (FOR LEGAL USE ONLY)

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SSS No. BOD 2025-016

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

Committee Meeting & Date Policy – November 12, 2025
Board Meeting Date N/A

TO				TO						
1.	Farres Everly			6.						
2.	Suresh Kotha			7.						
3.	Brandy Bolden			8.						
4.				9.	Legal					
5.				10.	CEO & General Manager					
Consent Calendar		Yes	x	No <i>If no, schedule a dry run presentation.</i>		Budgeted	x	Yes	No <i>(If no, explain in Cost/Budgeted section.)</i>	
FROM (IPR)				DEPARTMENT				MAIL STOP	EXT.	DATE SENT
Heidi Sanborn / Crystal Henderson				Board Office				B307	5424	10/14/25

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 of Directors

Presenter: Heidi Sanborn, Committee Chair

Additional Links:

SUBJECT	Annual Review of Standing Committees	ITEM NO. <i>(FOR LEGAL USE ONLY)</i>
---------	--------------------------------------	--------------------------------------

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

FINANCE AND AUDIT COMMITTEE

CHARTER

- The Committee assists the Board in its ongoing work by gathering information, monitoring SMUD's performance, considering implications, preparing alternatives and/or recommending policies related to financial practices and metrics, access to credit markets, audit practices, employee benefits and risk management.
- The Committee considers and makes recommendations to the Board regarding the annual budget and the issuance of debt.
- The Committee considers audits prepared by SMUD's Internal Auditor and the independent outside auditor. The Committee provides direction to the Internal Auditor on the annual audit plan.
- The Committee considers and makes recommendations to the Board regarding operational matters, including contracts related to the Committee's charter.
- The Committee may also consider any other matter placed on its agenda where there is a business need for timely consideration.

ENERGY RESOURCES AND CUSTOMER SERVICES COMMITTEE

CHARTER

- The Committee assists the Board in its ongoing work by gathering information, monitoring SMUD's performance, considering implications, preparing alternatives and/or recommending policies related to customer relations and initiatives, reliability, energy resources, and transmission and distribution matters.
- The Committee considers and makes recommendations to the Board regarding operational matters, including contracts related to the Committee's charter.
- The Committee may also consider any other matter placed on its agenda where there is a business need for timely consideration.

POLICY COMMITTEE

CHARTER

- The Committee assists the Board in its ongoing work by gathering information, monitoring SMUD's performance, considering implications, preparing alternatives and/or recommending policies related to governance, economic development, community outreach and communications, safety, rates, procurements, legislation, information management and other policy development issues.
- The Committee may also consider any other matter placed on its agenda where there is a business need for timely consideration.

STRATEGIC DEVELOPMENT COMMITTEE

CHARTER

- The Committee assists the Board in its ongoing work by focusing on mid and long term strategic issues. The Committee will educate itself, gather information and consider the implications regarding industry trends, emerging technologies, shifting business models, competitive threats and opportunities, and risks associated with shifting legislative and regulatory paradigms.
- The Committee may also consider any other matter placed on its agenda where there is a business need for timely consideration

SSS No.

BOD 2025-001

BOARD AGENDA ITEM
STAFFING SUMMARY SHEET

Committee Meeting & Date
POLICY - 2025
Board Meeting Date
N/A

TO					TO							
1.	Suresh Kotha				6.							
2.	Brandy Bolden				7.							
3.	Farres Everly				8.							
4.					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) Gregg Fishman / Crystal Henderson					DEPARTMENT Board Office					MAIL STOP B307	EXT. 5424	DATE SENT 12/20/24
NARRATIVE:												
<p>Requested Action: Enable the Board of Directors an opportunity to review the Board Work Plan.</p> <p>Summary: The Board President reviews the Board Work Plan to ensure agenda items support the work of the Board.</p> <p>Board Policy: This review of the Work Plan supports Governance Process GP-4, Board/Committee Work Plan and Agenda Planning, which states that the Board will develop each year a list of topics and issues that it wishes to explore in the coming years and maintain a work plan that will be regularly reviewed by the Board or a standing committee. Governance Process GP-6, Role of the Board President, states that the Board President shall ensure that the Board’s agendas meet the goals of the annual work plan.</p> <p>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.</p> <p>Cost/Budgeted: Included in the budget for internal labor.</p> <p>Alternatives: Not review the Work Plan at this time.</p> <p>Affected Parties: Board of Directors and Executive Office</p> <p>Coordination: Crystal Henderson, Special Assistant to the Board</p> <p>Presenter: Gregg Fishman, Board President</p>												

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 2025-002

BOARD AGENDA ITEM
STAFFING SUMMARY SHEET

Committee Meeting & Date
POLICY - 2025
Board Meeting Date
N/A

TO					TO							
1.	Brandy Bolden				6.							
2.	Farres Everly				7.							
3.	Suresh Kotha				8.							
4.					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) Heidi Sanborn / Crystal Henderson					DEPARTMENT Board Office					MAIL STOP B307	EXT. 5424	DATE SENT 12/20/24

NARRATIVE:

Requested Action:

A summary of directives is provided to staff during the committee meeting.

Summary:

The Board requested an ongoing 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 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:

Governance Process GP-4, Board/Committee Work Plan and Agenda Planning states the Board will focus on the results the Board wants the organization to achieve.

Benefits:

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

Cost/Budgeted:

Included in budget for internal labor.

Alternatives:

Not to summarize the Board’s request at this meeting.

Affected Parties:

Board of Directors, Board Office and Executive Office

Coordination:

Crystal Henderson, Special Assistant to the Board

Presenter:

Heidi Sanborn, Policy Committee Chair

Additional Links:

SUBJECT
Summary of Committee Direction – Policy Committee

ITEM NO. (FOR LEGAL USE ONLY)

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.