Board Energy Resources & Customer Services Committee Meeting and Special SMUD Board of Directors Meeting

Date: Wednesday, December 9, 2020

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

Location: Virtual Meeting (online)

Powering forward. Together.

SMUD®

AGENDA
BOARD ENERGY RESOURCES & CUSTOMER SERVICES COMMITTEE MEETING
AND SPECIAL SMUD BOARD OF DIRECTORS MEETING

Wednesday, December 9, 2020
Scheduled to begin at 5:30 p.m.
Zoom Webinar Link: Join SMUD Energy Resources & Customer Services Committee Meeting
Webinar ID: 161 097 9651
Password: 043027
Phone Dial-in Number: 1-669-254-5252

In accordance with the Governor's Executive Order N-29-20 and the Emergency Board Meeting Procedures adopted by the SMUD Board of Directors, the regular Board meeting and other public meetings are closed to the public to align with state, local, and federal guidelines and social distancing recommendations for the containment of the coronavirus.

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

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

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

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

This Committee meeting is noticed as a joint meeting with the Board of Directors for 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 Energy Resources and Customer Services Committee will review, discuss and provide the Committee's recommendation on the following:

DISCUSSION ITEMS

1. Mark Rawson

   a. Adopt a resolution stating SMUD's intent to exercise the authority in Section 12773 of the California Municipal Utility District Act, where SMUD may hold nonstock security in a corporation or other private entity if such security is acquired as part of a procurement of goods or services from that entity, provided no separate funding is expended solely for the nonstock security, and not more than three nonstock security acquisitions are made during the period starting January 1, 2020, to January 1, 2025.

   b. Adopt a pilot program and policy governing the acquisition of nonstock security.

   c. Authorize the Chief Executive Officer and General Manager to operate the **Nonstock Security Pilot Project Program**.

   Presentation: 10 minutes
   Discussion: 5 minutes

2. Antiwon Jacobs

   Accept the monitoring report for **Strategic Direction SD-16, Information Management and Security**.
   Presentation: 12 minutes
   Discussion: 5 minutes

INFORMATIONAL ITEMS

3. Public Comment

4. Brandon Rose

   Summary of Committee Direction.
   Discussion: 1 minute

ANNOUNCEMENT OF CLOSED SESSION AGENDA

1. Threat to Public Services or Facilities

Pursuant to Section 54957 of the Government Code:

Consultation with: Laura Lewis, Chief Legal Officer; Stephen Clemons, Chief Information Officer; Antiwon Jacobs, Director, Information Technology Security; and Rob Lechner, Director of Facilities & Security Operations.

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

Members of the public may make either a general public comment or comment on a specific agenda item by submitting comments via email. Comments may be submitted to PublicComment@smud.org. Comments will be provided to the Board and placed into the record of the Committee meeting if it is received within two hours after the meeting ends.

Members of the public that are listening or watching the live stream of a Board meeting and wish to comment on a specific agenda item as it is being heard, may submit their comments, limited to 250 words or less, to PublicComment@smud.org. The Board Chair may read the comments into the record, in her discretion, based upon such factors as the length of the agenda or the number of email comments received. Comments will be provided to the Board and placed into the record of the Committee meeting if it is received within two hours after the meeting ends.

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

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

SSS No. LEG 2020-0160

BOARD AGENDA ITEM
STAFFING SUMMARY SHEET

Committee Meeting & Date
ERCS Committee – 12/09/20
Board Meeting Date
December 10, 2020

TO		TO	
1.	Scott Martin	6.	
2.	Jennifer Davidson	7.	
3.	Frankie McDermott	8.	
4.	Brandy Bolden	9.	**Legal**
5.	Stephen Clemons	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
Gigi Capuyan	Office of the General Counsel	B308	5670	11/23/20

NARRATIVE:

Requested Action:

a. Adopt a resolution stating SMUD's intent to exercise the authority in Section 12773 of the California Municipal Utility District Act, where SMUD may hold nonstock security in a corporation or other private entity if such security is acquired as part of a procurement of goods or services from that entity, provided no separate funding is expended solely for the nonstock security, and not more than three nonstock security acquisitions are made during the period starting January 1, 2020, to January 1, 2025.

b. Adopt a pilot program and policy governing the acquisition of nonstock security.

c. Authorize the Chief Executive Officer and General Manager to operate the Nonstock Security Pilot Project Program.

Summary: SMUD has long worked with companies to innovate products and services to enhance affordability and reliability of electrical energy service. In 2018 the Board adopted an Integrated Resource Plan ("IRP"), with an ambitious goal of carbon neutrality by 2040, which will require several billions of dollars of investments in renewable power resources, other assets, and programs. In 2020 the Board adopted a climate emergency declaration in which the Board committed to work toward carbon neutrality by 2030 and to collaboratively find creative solutions to eliminate GHG emissions until a safe atmosphere is restored. Substantial investment will be needed in new technologies, grid modernization, energy resources, and electric transportation to meet SMUD's and California's carbon reduction and clean energy goals.

Recognizing the need for greater flexibility and innovative approaches to business partnerships and business models, SMUD worked with legislators on Assembly Bill 689 ("AB 689"). AB689 was signed into law last year and codified in Section 12773 of the California Public Utilities Code ("Municipal Utility District Act"), which authorizes SMUD to operate a pilot project, effective until January 1, 2025, under which it may hold nonstock security in a corporation or other private entity, if such security is acquired as part of a procurement of goods or services from that entity, provided no separate funding is expended solely for the nonstock security. Under the pilot project, SMUD may acquire up to three (3) nonstock security instruments wherein the value of each security (e.g., number of units multiplied by the unit price) at the time of acquisition by SMUD does not exceed three (3) percent of SMUD's annual revenue in the fiscal year of the acquisition. Prior to SMUD's exercising the authority to implement the pilot project, the Board must adopt a policy governing the acquisitions to provide, at a minimum, conflicts of interest, an approval process, and procedures to ensure the security acquisition does not unduly affect the price of the underlying goods and services, and assuring that SMUD receives a reasonable return for any underlying use of its intellectual property or other SMUD resources.

Board Policy: *(Number & Title)* SD-10, Innovation; SD-13, Economic Development; and SD-19, Diversified Business

Benefits: Acquiring nonstock security in a corporation or other private entity will help: (1) promote carbon reduction, clean energy and other technologies that will help foster a better environment for the Sacramento community and beyond; (2) fairly compensate ratepayers for their community investment in development of such technologies by creating a revenue stream that may potentially offset future rate increases; and (3) attract businesses to the SMUD service area, which in turn may lead to job growth in the Sacramento region.

Cost/Budgeted:	No costs are required to exercise the authority in Section 12773 of the MUD Act because SMUD is allowed to hold the nonstock security only if acquired as part of a procurement of goods or services from the same company, and provided no separate funding is expended solely for such security.
Alternatives:	Forego the potential to receive a financial return on the community's investment in companies that SMUD partners with to develop or improve products and services that enhance affordability and reliability of electrical energy service for the benefit of SMUD ratepayers.
Affected Parties:	Resource and New Business Strategy; Treasury and Accounting; Legal
Coordination:	This pilot project would be coordinated by Resource and New Business Strategy in consultation with Treasury & Accounting and Legal.
Presenter:	Mark Rawson, Manager: Resource and New Business Strategy

Additional Links:

SUBJECT	ITEM NO. ***(FOR LEGAL USE ONLY)***
Nonstock Security Pilot Project	

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

DRAFT

Nonstock Security Pilot Project Program
Sacramento Municipal Utility District

Pilot Project Program Description

1. **Purpose:** To provide an opportunity for a return on investment from SMUD's contribution to the development of goods or services procured from a corporation or private entity, consistent with Strategic Directives (SD-10: Innovation, SD-13: Economic Development, and SD-19: Diversified Business).

2. **Definitions:**

   Acquisition – An act of obtaining an asset.

   Nonstock Security – A "security," as defined in Section 25019 of the California Corporations Code, that is not a stock.

   Stock – A distinct type of security that specifically includes an ownership interest in a corporation, where the owner is entitled to participate in: (i) the company's management (e.g., has a voting right); (ii) a proportionate share of profits; and (iii) distribution of assets upon dissolution of the company. Its unit of measurement is the share.

3. **Conflict of interest:** To avoid any potential conflict or perceived conflict of interest and to prevent violations of applicable conflict of interest rules including Cal. Gov't Code § 1090, et seq.; the Political Reform Act (Cal. Gov't Code § 81000, et seq.); and the Fair Political Practices Commission Regulations (Cal. Code of Regulations § 18700, et seq.), SMUD shall not enter into an agreement to acquire a nonstock security interest in a corporation or private entity under any of the following situations:

   a. A board member, or spouse or dependent child of the board member, has a financial interest in the corporation or private entity.

   b. A board member, or spouse or dependent child of the board member, has a personal or familial relationship with any officer or employee of the corporation or private entity.

   c. An executive officer of SMUD, or spouse or dependent child of the officer, has a financial interest in the corporation or private entity.

Board members and certain other SMUD staff are each to file annually a Statement of Economic Interests (Form 700) to ensure that those public agency officials are disclosing certain financial interests in a manner that is transparent. It also serves as a reminder for public agency officials and employees to abstain from participating in decisions, including agreements, that could enhance their personal finances in a manner that is inconsistent with law or policy.

Prior to entering into an acquisition agreement, SMUD shall review Board members' most recent financial disclosure filing for potential financial conflicts of interest related to the acquisition.

Further, existing federal and state laws prohibit individuals from purchasing or selling a security when that individual knows material, non-public information about a company which would significantly affect the market price of the security in that company (e.g., company stock price). To avoid any appearance or accusation of insider trading, non-public information received by SMUD may not be used to make decisions concerning the acquisition or sale of the security issued to SMUD.

4. **Determination of how much of nonstock security to accept:** Prior to SMUD's acquiring any nonstock security, the Busines Unit initiating the procurement of the underlying goods or services shall, in consultation with New Business Development and Treasury Departments, ensure that:

    a. SMUD, overall, receives a reasonable return for SMUD's investment, considering, at a minimum, the value of the following: (i) use of any SMUD intellectual property; (ii) SMUD's investment of staff time; and (iii) use of SMUD facilities for field testing; and

    b. The value of the nonstock security acquisition does not unduly influence the amount paid for the associated goods and services.

5. **Payment of associated goods or services:** SMUD may only hold nonstock security in a corporation or private entity if acquired as part of a procurement of goods or services from that entity. The price paid for such goods or services should not be increased due to the availability of acquiring nonstock security in that corporation or private entity. SMUD is not "purchasing" the nonstock security, so no cash will be exchanged solely for the acquisition of the nonstock security. Any acquisition of nonstock security is incidental to the procurement of goods or services.

6. **Approval for acquisition:** The Chief Executive Officer and General Manager shall seek Board approval prior to entering into an acquisition agreement.

7. **Reporting to the Board:** Staff shall report annually to the Board on the status of this Pilot Project Program and any related acquisitions.

8. **Management of Security:** All decisions and administrative actions concerning the management of any security issued to SMUD by a corporation or other private entity shall be recommended by the Chief Financial Officer or her delegee and approved by the Board. This includes decisions on when the security will be exercised or converted to cash. The Chief Financial Officer shall carry out this function consistent with her delegated investment authority.

9. **Distribution of Security Interest:** Upon such time that SMUD's security interest is sold for cash, the proceeds will be received and recorded by SMUD accounting, indicating the source of funds. SMUD's subsequent use of any cash proceeds shall be in accordance with SMUD policies and to benefit SMUD ratepayers.

10. **Related Reference:** SD-10 Innovation; SD-13 Economic Development; SD-19 Diversified Business; BL-8 Procurement; BL-14 Products, Services and Programs

2

SSS No.	BOARD AGENDA ITEM	Committee Meeting & Date
CIO 20-003	**STAFFING SUMMARY SHEET**	December 9, 2020
		Board Meeting Date
		December 10, 2020

TO		TO	
1.	Frankie McDermott	6.	Rob Lechner
2.	Brandy Bolden	7.	
3.	Stephen Clemons	8.	
4.	Antiwon Jacobs	9.	**Legal**
5.	Joe Schofield	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
Angie Christina	Cybersecurity	E114	6770	11/20/2020

NARRATIVE:

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

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

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

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

Cost/Budgeted: N/A

Alternatives: N/A

Affected Parties: SMUD

Coordination: Cybersecurity

Presenter: Antiwon Jacobs

Additional Links:

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

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.

SACRAMENTO MUNICIPAL UTILITY DISTRICT

OFFICE MEMORANDUM

TO: Board of Directors **DATE:** December 1, 2020

FROM: Claire Rogers CR 12/01/20

SUBJECT: **Audit Report No. 28007215**
Board Monitoring Report; SD-16: Information Management and Security

Audit and Quality Services (AQS) received the SD-16 *Information Management and Security* 2020 Annual Board Monitoring Report and performed the following:

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

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

CC:

Paul Lau

Board Monitoring Report 2020
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) The Information Security, Physical Security, Privacy, and Records and Information Management programs and initiatives align directly with the "Value Our Customers and Community" and "Operational Excellence" points on SMUD's North Star. These programs work towards ensuring that SMUD continues to be a good steward over customer information, physical security, privacy, and records in accordance with our customers' high expectations.

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

c) Summary:

SD Requirement	Program/ initiative/policy	Purpose	Outcome	Notes
Information Security: Protect systems and information from unauthorized access	Information security program; AP 07.03.01 Information Security Concepts and Roles	Protect systems and information; provide policy supporting the cybersecurity program	Closed door briefing to be held in December	Discuss security technologies and business processes to protect information
Customer Privacy: Annually notify customers about use of information	Annual notice of privacy practices	Notify customers of our privacy practices	Notice sent June 2020	Language updated to clarify SMUD does not sell personal information
Customer Privacy: Ensure security where data is shared	System Security Plans and SOC 2 audit reports requirement	Evaluate the information practices and security controls of third parties	High confidence that vendors are using best practices to protect SMUD sensitive and confidential information	

Customer Privacy: Maintain a process that identifies purposes for information collection and dissemination	Data sharing policy, data sharing request/approval process	Track NDAs, the data being shared, and the business justification for sharing	Data Sharing process is being observed and maintained	
Records Management: Identify and manage records and information	Records evaluations	Evaluate and classify records and ensure retrieval, disposal and protection	On-track to meet 5-year plan of completing for entire enterprise	
Records Management: Education	Ongoing enterprise training and Records Custodian Forums	Provide training to all of SMUD, with focused efforts on the Records Custodians	Provided annually to all employees, with supplemental support, as needed; also quarterly focused support for Records Custodians	
Physical Security: Safeguard employees, customers, and visitors	AP 06.03.01 Increase interoperability with local law enforcement during critical incidents	Protect SMUD employees and those who visit SMUD facilities	Completed project to facilitate direct radio contact with local law enforcement agencies	SMUD Security Operations supervisors and dispatchers communicate in the field and via dispatch 24/7
Physical Security: Protect SMUD facilities	AP 06.03.01 Physical security assessment 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 scheduled to begin Q4 2020

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 Cybersecurity group (formerly Information Security) in line with policy AP 07.03.01 adopted the National Institute of Standards and Technology (NIST) Cybsersecurity Framework (CSF) to establish prudent and reasonable measures to effectively manage information and security risk. The CSF has five core functions (Identify, Protect, Detect, Respond, and Recover) which comprise both administrative and technical controls to manage risk to SMUD's information security, physical security, customer privacy, and records management. The Chief Information Officer's (CIO) cybersecurity group is actively collaborating with the Chief Legal Officer's (CLO) records management group and Chief Workforce Officer's (CWO) physical security group to implement the CSF measures to enhance information management and security risk management practices and processes in support of SD-16. Cybersecurity will highlight capabilities provide an update to the board for SD-16 during a closed session.

Physical Security

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

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

SMUD will also protect its facilities and functions that support the reliability of the electric system and overall operation of the organization from unauthorized access or disruption of business operations.

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

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

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

Customer Privacy

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

SMUD sent out our annual privacy notice via email and as a bill insert to customers during the June bill cycle. The notice was updated this year to add a bullet explicitly stating that we will not sell personal information. 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.

As part of a 2020 Supply Chain Risk Management project, Cybersecurity worked with Procurement to identify, establish, and formalize a supply chain risk management process. As part of that process SMUD continues to use a mandatory procurement requirement for vendors to allow the Cybersecurity team to evaluate the security posture of a proposed vendor solution. The American Institute of CPAs (AICPA) Service Organization Control 2 (SOC 2) Type 2 continues to be our procurement standard as it is an independent assessment focused on a solution's security controls which includes tests of the security controls' efficacy. SOC 2 Type 2 reports provide staff confidence that vendor security controls are robust and sufficient to protect SMUD information. Contract and non-disclosure agreement language is used to provide assurance that SMUD provided sensitive and confidential information will not be used for any unapproved purposes.

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

MP 07.03.01.122 - Data Sharing requires an approved data sharing request prior to sharing information with a third party for SMUD business purposes. The request form requires the identification of the data categories to be shared and the business justification that requires the sharing of data. This facilitates an approval process which includes the requester's management, Supply Chain, the Data Governance Program Manager, the data owner(s), and Cybersecurity.

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 RIM Program is making continued progress toward our 5-year plan of completing record evaluations for all business areas; currently in year 2, and projecting completion by year 5. Through this process we have a high level of confidence that SMUD records will be identified and managed appropriately once complete.

We are also driving implementation of a SMUD-wide eCommunication policy around management of emails, chats and electronic recordings. Chats and electronic

recordings changes have been implemented as of Q4-2020, with email being managed per the policy beginning Q1-2021. Extensive training and communications are being performed now in support of the new policy.

The RIM program is actively partnering with IT to review and support new software integrations to ensure they meet records policies and information best practices. We have created a cross-functional governing body to review and approve Microsoft Office 365 tools to ensure their implementations are also in alignment with records policies. We are also actively partnering with Cybersecurity, CIP Program, Data Governance, and other business partners on document management efforts to ensure alignment.

4) Challenges

Information Security

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

In 2019 our PCI compliance related transaction volumes continue to increase, although SMUD is still a Level 2 Merchant. SMUD is again compliant this year as determined by an independent third-party PCI Qualified Security Assessor. Our required assessment documents were submitted to Chase Paymentech in September.

The Cybersecurity team continues to ensure compliance with updated Critical Infrastructure Protection (CIP) standards as well. This year saw new standards become enforceable related to supply chain risk management and CIP designated low impact facilities. The team worked with internal and external stakeholders to ensure our ability to demonstrate compliance prior to the enforcement dates for these standards.

In addition to the compliance related work that results from the breaches in the news, SMUD Cybersecurity has also continued to mature our Incident Response capabilities. New policy has been drafted and an enterprise wide incident response plan has been drafted and exercised as well.

Physical Security

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

Nevertheless, Physical Security continues working to limit unauthorized physical access to SMUD. Efforts to mitigate tailgating, both pedestrian and vehicle, into SMUD facilities continued this year, including making changes to gate opening timers, posting additional signage, and educating employees via the internal Employee News Network.

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

Customer Privacy

The California Consumer Privacy Act (CCPA) went into effect this year aimed at protecting the privacy of California citizens. Due to SMUD's existing policies and processes already having been aligned to privacy best practices, new policies and procedures were not necessary to become compliant with this law. Our transparency around these policies and practices (starting with SD-16), has helped SMUD build a level of trust with our customers that resulted in a relatively small amount of inquiries and requests related to the CCPA.

As tracked by SMUD's Enterprise Risk group, we continue to operate at a high level of residual risk in the categories of Cybersecurity and Privacy. In order to help address this, SMUD Cybersecurity has begun the process of tailoring the NIST Risk Management Framework (RMF) to our environment. Aligned with the Cybersecurity Framework (CSF) this will ensure our governance and cybersecurity risk management process appropriately address cybersecurity risks as well as facilitate informed decisions by Director-data owners and system owners regarding the management of the cybersecurity risk of their data and systems.

Records Management

Due to access restrictions related to COVID-19, we were unable to complete our standard physical content reviews as part of our records evaluation process. We implemented new processes to accommodate these restrictions and have partnered with the business areas to ensure physical content is inventoried and managed appropriately as part of our record evaluations going forward, even in light of continuing remote work.

We have implemented corrective action in response to Audit and Quality Services' audit 28006022, Finding #02, which stated that SMUD needed to ensure record destruction features are working appropriately. A recently purchased tool provides the required records management and destruction over four different document repository systems. The tool is being used in a systematic manner to destroy documents as part of record evaluations completed this year. In addition, in 2021 we will use it to apply retention for record evaluations completed in previous years.

5) Recommendation

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

6) Appendices

Acronyms used in this report:

NIST – National Institute of Standards and Technology
CSF – Cybersecurity Framework
CCPA – California Consumer Privacy Act
RMF – Risk Management Framework
RTVA – Risk, Threat, and Vulnerability Assessment
LLEA – Local Law Enforcement Agency
SRRCS – Sacramento Regional Radio Communications System

3

SSS No.	Committee Meeting & Date
LEG 2019-0004	ERCS 2020
	Board Meeting Date

BOARD AGENDA ITEM

STAFFING SUMMARY SHEET

TO		TO	
1.	Frankie McDermott	6.	
2.	Nicole Howard	7.	
3.	Stephen Clemons	8.	
4.		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
Laura Lewis	Legal Department	A311	6123	

NARRATIVE:

Requested Action: Committee discussion and consensus on any directives provided to staff during the Committee meeting.

Summary: 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. Energy Resources & Customer Services Committee Chair, Brandon Rose, 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 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: N/A

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

Affected Parties: Board of Directors and Executive Staff

Coordination: Donna Lofton, Special Assistant to the Board

Presenter: Brandon Rose, Chair, Energy Resources & Customer Services Committee

Additional Links:

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

ITEMS SUBMITTED AFTER DEADLINE WILL BE POSTPONED UNTIL NEXT MEETING.