COUNTY of VENTURA
Grand Jury

800 South Victoria Avenue
Ventura, CA 93009
Tel (805) 477-1600
Fax (805) 658-4523
grandjury.countyofventura.org

This response was given using the 2020-2021 Ventura County Grand Jury Report form. The form should have reflected the Ventura County Grand Jury Report form 2021-2022.

We regret any confusion this may cause.

Sincerely,

Keith Frost
Foreperson
Ventura County Grand Jury (2022-2023)

CALLEGUAS MUNICIPAL WATER DISTRICT

web site: www.calleguas.com

2100 OLSEN ROAD • THOUSAND OAKS, CALIFORNIA 91360-6800 805/526-9323 • FAX: 805/522-5730

August 31, 2022

RECEIVED
SEP 2 2022
Ventura County
Grand Jury

Ms. Carrie Landon, Foreperson
Ventura County Grand Jury
800 S. Victoria Avenue
Ventura, CA 93003

Dear Ms. Landon,

On behalf of Calleguas Municipal Water District (Calleguas, District), please find the enclosed response to various findings and recommendations in the Grand Jury's Report entitled *Cybersecurity of Water Providers in Ventura County*, dated May 11, 2022.

I appreciate the opportunity to provide a response on behalf of Calleguas. At your request, I am available to discuss any of the following information in further detail at (805) 579-7138 or TGoff@calleguas.com.

Sincerely,

Anthony Goff
General Manager

cc: Board of Directors, Calleguas Municipal Water District

COUNTY of VENTURA
Grand Jury

800 South Victoria Avenue
Ventura, CA 93009
Tel (805) 477-1600
Fax (805) 658-4523
grandjury.countyofventura.org

Response to Ventura County Grand Jury Report Form

Report Title: *Cybersecurity of Water Providers in Ventura County*

Responding Entity: *Calleguas Municipal Water District*

FINDINGS

- I (we) agree with the Findings numbered: F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, and F-09.

- I (we) disagree wholly or partially with the Findings numbered: _____
  (Attach a statement specifying any portions of the Findings that are disputed; include an explanation of the reasons.)

RECOMMENDATIONS

- Recommendations numbered R-01, R-02, R-03, R-04, R-06 have been implemented.
  (Attach a summary describing the implemented actions.)

- Recommendations numbered R-05 have not yet been implemented but will be implemented in the future.
  (Attach a summary indicating the timeframe for implementation.)

- Recommendations numbered _____ require further analysis.
  (Attach an explanation to include: scope and parameters of the analysis or study and timeframe for the matter to be prepared for discussion with the agency or department head. The timeframe shall not exceed six months from the date of publication of the report.)

- Recommendations numbered _____ will not be implemented because they are not warranted or are not reasonable.
  (Attach an explanation.)

Date: August 31, 2022

Signed: _____

Number of pages attached: 3

Title: General Manager

Response to Recommendations

Recommendation R-01. The Grand Jury recommends that the investigated public water providers regularly assess their cybersecurity, addressing both IT and SCADA, consistent with EPA and CISA recommended best practices. (F-01, F-02, F-03, F-05)

Response to R-01: Calleguas has established a cybersecurity program in alignment with EPA and CISA best practices, and continues to implement new and innovative security measures and recommendations as they become available. The following points briefly summarize cybersecurity protocols that are currently implemented at Calleguas:

- Segregated IT and SCADA networks are equipped with up-to-date monitoring systems, vulnerability scanners, antivirus and antimalware software, and firewalls. These protections work together to mitigate cybersecurity risks, defend business and operations systems, and prevent malicious actors or inadvertent intruders from infiltrating networks.
- System updates and security patches recur as scheduled, and as needed, in accordance with identified vulnerabilities and recommendations from service providers, vendors, contractors, and government organizations and authorities.
- Access control policies are applied to ensure network systems are only accessible through secure channels, from both mobile devices and equipment at remote facilities. Current access security protocols include detailed password protection, multi-factor authentication, physical security of network equipment, and intrusion alerts.
- Redundant back-ups for data servers and critical network systems are in place and readily available, as needed.

Recommendation R-02. The Grand Jury recommends that the investigated public water providers regularly share and exchange information regarding cybersecurity threats, attacks, protections and remedies, and provide training, using such forums as the AWAVC. (F-01, F-02, F-03, F-04, F-06, F-07)

Response to R-02: Water providers in Ventura County, including Calleguas, have informally exchanged information regarding cybersecurity threats, prevention methods, protections, and remedies with other agencies in the past. However, forums for information sharing and collaboration, as well as timely distribution of data, information and resources pertaining to cyberthreats, attacks, protections and remedies, have been established and optimized by cybersecurity agencies, networking groups and organizations at federal and state levels. Calleguas maintains active membership and standing on distribution lists with several federal and state entities that directly issue cybersecurity alerts, threat information, protection and mitigation actions, resources, and remedies, including:

- California Governor's Office of Emergency Services' (Cal OES') California Cybersecurity Integration Center (Cal-CSIC).
- CISA's National Cyber Awareness System (NCAS) and Computer Emergency Readiness Team (CERT).
- FBI Cyberhood Watch Program and Infragard Program.
- Department of Homeland Security's (DHS') Homeland Security Information

Network (HSIN).
- Joint Regional Intelligence Center (JRIC).
- Multi-State Information Sharing and Analysis Center (MS-ISAC).

Membership with these organizations, and standard monitoring of the information and resources that are distributed to members or made available in their forums, is an effective way for public water providers to receive timely information and maintain situational awareness on critical cybersecurity issues. Calleguas has advocated for all public water providers in Ventura County to register for alerts and become active members with the listed entities in order to receive information and resources directly.

In addition, Calleguas has coordinated cybersecurity training for staff and water sector professionals in Ventura County through channels such as the AWAVC, including an educational program held on March 23, 2022 via AWAVC's Channel Counties Water Utilities Committee (CCWUC) entitled "Cybersecurity for the Public Sector". At this event, cybersecurity experts and advisors from CISA and Cal-CSIC presented information regarding cyber-related threats, risks, types of attacks, preparedness measures, and response tactics, in addition to describing the services their respective agencies provide and answering questions from attendees. Through participation in AWAVC, Calleguas expects to continue advocating and collectively participating in efforts to provide additional cybersecurity training to the water sector in Ventura County.

Recommendation R-03. The Grand Jury recommends that the investigated public water providers use free federal and state expert assistance to enhance cybersecurity. (F-01, F-02, F-03, F-05, F-06, F-07, F-08)

Response to R-03: In addition to receiving and implementing applicable cybersecurity information, alerts, and updates, Calleguas also uses free services and resources from agencies and programs listed in the Response to R-02.

Recommendation R-04: The Grand Jury recommends that the investigated public water providers regularly conduct cybersecurity awareness training. (F-01, F-02. F-03, F-04)

Response to R-04: Calleguas provides monthly training to all employees on various cybersecurity topics through a third-party contractor. This monthly training is designed to increase staff awareness of basic cybersecurity issues and provide them with a better understanding of how they can protect network systems and devices, both in the workplace and in their personal lives. Additionally, the District employs a third-party contractor to perform penetration tests on both IT and SCADA networks at least once every three to five years. Other staff with cybersecurity responsibilities are assigned to attend or participate in further detailed training opportunities throughout each year at the discretion of their supervisor or manager.

Recommendation R-05: The Grand Jury recommends that the investigated public water providers address recovery from cybersecurity incidents in their business recovery plans. (F-01, F-02, F-03, F-09)

Response to R-05: Calleguas currently addresses response and recovery from all hazards, both natural and manmade, in planning documents including the Emergency Response Plan and Business Continuity Plan. The District expects to complete a comprehensive Cybersecurity Response and Recovery Plan within the next year, which will describe the recovery process specifically during a cybersecurity incident.

Recommendation R-06: The Grand Jury recommends that each investigated public water provider establish a CISA-compliant internal protocol for reporting cyber incidents. (F-01, F-02, F-03, F-06)

Response to R-06: Calleguas has established internal response and reporting protocols during a cybersecurity incident that are compliant with existing CISA requirements and consistent with current recommendations. The District's reporting protocols will evolve as additional reporting mechanisms become available and new regulatory requirements are introduced, including those previewed in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).