2021 - 2022
Ventura County Grand Jury

COUNTY *of* **VENTURA**

Final Report

Cybersecurity of Water Providers in Ventura County

May 11, 2022

This page intentionally blank

Cybersecurity of Water Providers in Ventura County

SUMMARY

Cyber-attacks are a serious threat to the public drinking water supply. Recent cyber-attacks around the United States have resulted in community water supplies being poisoned or their suppliers' business operations being held hostage by ransomware. In recognition of this critical threat, the 2021-2022 Ventura County Grand Jury (Grand Jury) investigated the cybersecurity of Ventura County public water providers.

The Grand Jury investigated two primary areas of cyber vulnerability in the water sector: the Information Technology (IT) used to bill consumers and record usage, and the Operational Technology (OT) used to control and monitor treatment and delivery of the water supply. Malicious actors can take advantage of network vulnerabilities and/or weak user access controls in either IT or OT to disrupt the business and the water service, and potentially degrade public safety.

The Grand Jury found that Ventura County relies on a complex network of public and private water wholesalers and retailers. The investigation encompassed those public water providers who supply 76% of Ventura County water users and concluded that there is considerable opportunity for improvement of cybersecurity policies and procedures.

The Grand Jury recommends that Ventura County water providers seek out and utilize free Federal and State expert support for implementing cybersecurity best practices, such as regular vulnerability assessments and cyber training for all employees. The Grand Jury further recommends that water providers utilize forums such as water agency associations to share information concerning cybersecurity threats, attacks, protections and remedies.

The Grand Jury recommendations can serve as a model to strengthen the cybersecurity of all Ventura County water providers.

METHODOLOGY

The Grand Jury obtained information from the following:

- Environmental Protection Agency (EPA) website
- Cybersecurity & Infrastructure Security Agency (CISA) website
- American Water Works Association (AWWA) website
- Water Information Sharing and Analysis Center (WaterISAC) website
- Internet research to gather information from a variety of authoritative sources
- Audio-visual presentation entitled "Water Supply Conditions and Drought Update" to the Simi Valley City Council, October 11, 2021
- Interviews with officials who have knowledge of the IT and OT of the community water systems in Ventura County

BACKGROUND

The Cyber Threat

In 2021, there were two well-publicized attempts by malicious actors to poison water supplies in Oldmar, Florida and the San Francisco Bay area. (Ref-01, Ref-02) In March 2019, a hacker gained unauthorized access to a public water plant in Kansas. (Ref-03) Ransomware attacks against water providers occurred in various locales, including Nevada, Maine, New Jersey, and California between September 2020 and August 2021. (Ref-04) These cyber-attacks involved the IT systems supporting the providers, such as customer account information and billing, as well as the OT systems that operate the water provider's physical plant. (Ref-01, Ref-04, Ref-05) The Grand Jury investigation addressed the vulnerability of Ventura County water providers to similar cyber-attacks, which could disrupt clean water availability and/or provider business operations, potentially threatening public health and safety. (Ref-02)

In 2019, the AWWA declared that "[c]yber risk is the top threat facing business and critical infrastructure in the United States." They also reported that "given the very real threat and significant consequences, it is critical that organizations prioritize cybersecurity and take reasonable steps to prevent, detect and respond to cyber incidents." The AWWA further observed that "optimistic reliance on sovereign immunity defenses or insurance policies, or an unconfirmed expectation that someone else within the organization is 'handling' cybersecurity issues, are not sufficient to protect an organization or its leaders from the repercussions of a cyber-attack…." (Ref-06) In response, CISA has published best practices for enhancing cybersecurity, including but not limited to risk assessments, user training, data backup and multi-factor authentication for remote access. (Ref-07)

In January 2022, the Biden-Harris Administration announced a new Water Sector Action Plan to secure water systems from cyberattacks. (Ref-08) The action plan, sponsored by the EPA and its federal partners, encourages the water sector to adopt technology which will enable early detection of cyber threats. (Ref-09) The plan will also boost information sharing about cyber threats between water utilities and the federal government. (Ref-08, Ref-09)

Ventura County Water Infrastructure

According to EPA's Water Systems Summary for Quarter 4 2021, there are 64 community water systems that supply drinking water to the residents of Ventura County. (Ref-10) About 98% of the county water is supplied by the 25 largest systems. The Grand Jury investigation focused on public water providers, as almost 80% of the county water agencies are operated by the County, its cities, and special districts. The Grand Jury investigation addressed 95% of these community water systems, corresponding to 76% of Ventura County water users. (Att-01)

More than half of the water delivered to Southern California homes and businesses is imported from Northern California by the Metropolitan Water District of Southern California (MWD) through the State Water Project and from the Colorado River. (Ref-11) The MWD allocates a portion of this water to Ventura County. (Ref-05) As shown on the Ventura County Water Purveyors map, two wholesale water

providers, Calleguas Municipal Water District and United Water Conservation District, are primarily responsible for distribution of this imported water to Ventura County communities. As shown on the Ventura County Water Purveyors map, these water districts provide water to every city in Ventura County except the City of Ojai, which is served by Casitas Municipal Water District. (Att-02) The water that comes from the MWD is already filtered and treated; the water from local sources is filtered and treated locally. (Ref-05, Ref-12, Ref-13) Some imported water is re-treated if it has been stored for any length of time prior to its delivery to the end user. (Ref-05) Each of these points of distribution and treatment is a potential target of a cyber-attack. (Ref-04, Ref-05)

Limitations to Scope

In many cases, the IT support for municipal water systems was housed within the respective city IT division rather than dedicated to the water department. As the cybersecurity of the cities' IT divisions was addressed in a recent Grand Jury report, the 2021-2022 Grand Jury elected not to make it our primary focus. (Ref-14) Although the Grand Jury did not interview all of Ventura County water providers, the Grand Jury recommendations could serve as a model to strengthen the cybersecurity of all.

The Grand Jury also considered that this report's findings and recommendations could potentially provide useful information to a malicious actor, as could the responses of the various water providers to this report. Therefore, this report does not make overly specific assertions of vulnerabilities or recommended remedies.

DISCUSSION

For each water provider, the chemical treatment, filtration, storage and distribution of water are controlled by OT, which is remotely accessed and managed by an industrial control system identified as the Supervisory Control and Data Acquisition (SCADA) system. (Ref-05, Ref-15) Hereafter this report will focus on SCADA as the cyber vulnerable component of OT. SCADA operators are trained in manual operation of pumps, valves and other equipment as backup in the event of SCADA failure or interruption. Additionally, each provider employs enterprise IT systems that support their workforce and provide customer interface', including usage tracking and billing for services rendered. Both the IT and SCADA systems have inherent cyber vulnerabilities, being dependent upon computer networking, remote access and user and operator awareness. SCADA administrators interviewed represented their systems to be less vulnerable due to fewer authorized users. (Ref-05) However, any cyber-attack on SCADA "…could result in devastating physical consequences to such things as critical infrastructure and services, the environment, and even human life." (Ref-16)

Seven of the 14 water providers interviewed by the Grand Jury have experienced some form of cyber-attack within the last five years, ranging from successful phishing attacks to ransomware. (Ref-05) These attacks exploited cyber vulnerabilities such as an attacker's familiarity with the network, vulnerability of connected devices, or poor access controls. (Ref-05, Ref-17) The AWWA website provides tools and a robust suite of guidance to support cybersecurity assessments,

including review of security weaknesses. (Ref-18) CISA offers a variety of exercises simulating cyber-attacks, many levels of cyber awareness training, and detailed vulnerability assessments, all of which are free to the recipient. Additionally, CISA offers resources to address vulnerabilities identified by their assessments. (Ref-19) The California State Water Resource Control Board also offers information to assist water agencies in becoming more cyber aware and cyber resilient. (Ref-20) Only three of the water providers interviewed have pursued available state or federal assistance to improve cybersecurity. (Ref-05)

The Grand Jury investigation revealed that all Ventura County public water providers interviewed have some level of cybersecurity for their IT and SCADA. Ten of 14 water providers interviewed have recently conducted cyber vulnerability assessments, however the complexity level and frequency vary among those assessments. (Ref-05) Cybersecurity experts recommend that a robust cyber security program includes firewalls, backups, controlled VPN access for mobile devices and multi-factor authentication. (Ref-21, Ref-22) All the water providers interviewed utilize remotely accessible IT and SCADA systems. Thirteen of 14 water providers interviewed employ firewalls, VPN access and/or multi-factor authentication to protect against unauthorized access. The water providers also employ various forms of data backup; some utilize the Cloud, while others utilize remote servers. (Ref-05)

Per the America's Water Infrastructure Act of 2018, every drinking water utility that serves at least 3,300 citizens was required to submit a Risk and Resilience Assessment by June 30, 2021 and update it at least every five years. (Ref-23) These assessments specifically address SCADA vulnerability. All Ventura County water providers interviewed by the Grand Jury are aware of this requirement, and 12 of 14 have completed the assessment. (Ref-05)

The Biden-Harris Administration's Water Sector Action Plan and CISA recommend raising the awareness of cyber risks and lessons learned from past incidents in the water and wastewater sector through cybersecurity training and information sharing. (Ref-08, Ref-21) Twelve of 14 Ventura County water providers interviewed by the Grand Jury have recently conducted cyber training in addition to the operator training required to achieve and maintain operational certification. All water providers interviewed are members of professional water associations such as the Association of Water Agencies Ventura County (AWAVC), the Association of California Water Agencies (ACWA) and AWWA; however, none have shared information with other local providers regarding cyber-attacks. (Ref-05)

The AWWA encourages member agencies to ensure their business recovery plans identify potentially disruptive events including cyber-attack, estimate their impact, and implement mitigation strategies. (Ref-24) Thirteen of 14 Ventura County water providers interviewed by the Grand Jury confirmed that their agencies had some form of business recovery plan, but not all addressed recovery from cyber incidents. (Ref-05) CISA directs that all cyber incidents must be reported to Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) in addition to local law enforcement. (Ref-21) All water providers interviewed agreed that cyber incidents should be reported, however only five of 14 identified FBI or DHS as report recipients. (Ref-05)

FINDINGS

F-01. The Grand Jury finds that cybersecurity of both IT and SCADA systems is essential to safe and effective delivery of water.

F-02. The Grand Jury finds inconsistent levels of cybersecurity for IT systems among the investigated water providers.

F-03. The Grand Jury finds inconsistent levels of cybersecurity for SCADA systems among the investigated water providers.

F-04. The Grand Jury finds that the level of training on cybersecurity is inconsistent among the investigated water providers.

F-05. The Grand Jury finds that the level and frequency of cybersecurity assessments are inconsistent among the investigated water providers.

F-06. The Grand Jury finds that knowledge of cyber incident reporting requirements is inadequate among the investigated water providers.

F-07. The Grand Jury finds that there is insufficient information exchange among the interviewed water providers regarding cybersecurity threats, attacks, protections and remedies.

F-08. The Grand Jury finds that there is insufficient awareness among public water providers of available government expert cybersecurity services and support for water provider systems.

F-09. The Grand Jury finds that not all the investigated water providers' business recovery plans addressed recovery from a cyber incident.

RECOMMENDATIONS

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)

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)

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)

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)

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)

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)

RESPONSES

Responses required from:

The following agencies within 90 days:

Calleguas Municipal Water District (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

Camrosa Water District (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

Casitas Municipal Water District (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

Triunfo Water District (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

United Water Conservation District (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

Ventura County Public Works Agency (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Camarillo Department of Public Works (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Fillmore Public Works Department (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Oxnard Public Works Department (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Port Hueneme Public Works Department (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Santa Paula Public Works Department (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Simi Valley Public Works Department (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Thousand Oaks Public Works Department (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

City of Ventura, Ventura Water (F-01, F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09) (R-01, R-02, R-03, R-04, R-05, R-06)

REFERENCES

Ref-01. Cybersecurity & Infrastructure Security Agency. Alert (AA21-042A): Compromise of U.S. Water Treatment Facility, February 12, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-042a Accessed May 7, 2022

Ref-02. Collier, Kevin. NBC News, June 17, 2021. 50,000 Security Disasters Waiting to Happen: The Problem of America's Water Supplies. https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206 Accessed May 7, 2022

Ref-03. Water Information Sharing and Analysis Center (Water ISAC). Insider Threat - Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District, October 21, 2021. https://www.waterisac.org/portal/updated-october-21-2021-insider-threat-–-former-employee-indicted-unauthorized-computer Accessed May 7, 2022

Ref-04. Cybersecurity & Infrastructure Security Agency, Alert (AA21-287A): Ongoing Cyber Threats to U.S. Water and Wastewater Systems, October 14, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-287a Accessed May 7, 2022

Ref-05. Interviews with Ventura County water providers

Ref-06. Germano, Judith H. Cybersecurity Risk & Responsibility in the Water Sector. American Water Works Association, 2019. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf Accessed May 7, 2022

Ref-07. Cybersecurity & Infrastructure Security Agency. Cyber Security Practices for Industrial Control Systems. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf Accessed May 7, 2022

Ref-08.   The White House. Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector, January 27, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/ Accessed May 7, 2022

Ref-09.   United States Environmental Protection Agency. EPA Announces Action Plan to Accelerate Cyber-Resilience for the Water Sector, January 27, 2022. https://www.epa.gov/newsreleases/epa-announces-action-plan-accelerate-cyber-resilience-water-sector Accessed May 7, 2022

Ref-10.   United States Environmental Protection Agency. SDWIS Federal Reports Search. Water Systems Summary for Quarter 4 2021. https://ordspub.epa.gov/ords/sfdw/sfdw/r/sdwis_fed_reports_public/21?clear=RP,RIR Accessed May 7, 2022

Ref-11.   The Metropolitan Water District of Southern California. How We Get Our Water: Infrastructure Serving Our Communities. https://www.mwdh2o.com/your-water/how-we-get-our-water/ Accessed May 7,2022

Ref-12.   Metropolitan Water District of Southern California. Metropolitan's Water Treatment Plants: Safeguard Public Health, September 2018. https://www.mwdh2o.com/media/4360/water-treatment-plants-fact-sheet-final_web.pdf Accessed May 7,2022

Ref-13.   Miller, Joanna M. Working out the Bugs: Calleguas Playing it Safe with New Treatment Plant. Los Angeles Times, September 27, 1995. https://www.latimes.com/archives/la-xpm-1995-09-27-me-50595-story.html Accessed May 7,2022

Ref-14.   Ventura County Grand Jury Final Report. Cybersecurity Strategies for Cities in Ventura County, April 17, 2020. https://vcportal.ventura.org/GDJ/docs/reports/2019-20/Cybersecurity_Final_Report_2019-2020.pdf. Accessed May 7, 2022

Ref-15.   Williamson, Graham. OT, ICS, SCADA – What's the difference? Kuppingercole Analysts, July 7, 2015. https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference Accessed May 7, 2022

Ref-16.   Maddison, John. Resolving the Challenges of IT-OT Convergence. CSO. June 21, 2018. https://www.csoonline.com/article/3283238/resolving-the-challenges-of-it-ot-convergence.html Accessed May 7, 2022

Ref-17.   Cybersecurity & Infrastructure Security Agency, Alert (AA21-209A): Top Routinely Exploited Vulnerabilities, August 20, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-209a Accessed May 7, 2022

Ref-18.   American Water Works Association. Cybersecurity & Guidance: What Water Utility Leaders & Professionals Should Know. https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance Accessed May 7, 2022

Ref-19.   Cybersecurity & Infrastructure Security Agency. CISA Services Catalog. https://www.cisa.gov/publication/cisa-services-catalog Accessed May 7, 2022

Ref-20.   California State Water Resources Control Board. https://www.waterboards.ca.gov Accessed May 7, 2022

Ref-21.   Cybersecurity & Infrastructure Security Agency. Preparing for and Mitigating Potential Cyber Threats ISA Insights, December 15, 2021. https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf Accessed May 7, 2022

Ref-22.   Ekran Systems. 15 Cybersecurity Best Practices to Prevent Cyber Attacks in 2022, April 6, 2022. https://www.ekransystem.com/en/blog/best-cyber-security-practices Accessed May 7, 2022

Ref-23.   Environmental Protection Agency. America's Water Infrastructure Act of 2018, January 3, 2018. https://www.epa.gov/ground-water-and-drinking-water/americas-water-infrastructure-act-2018-awia Accessed May 7, 2022

Ref-24.   American Water Works Association. Emergency Response and Recovery Planning for Water Systems: A Kit of Tools. https://engage.awwa.org/PersonifyEbusiness/Store/Product-Details/productId/7944 Accessed May 7, 2022

ATTACHMENTS

Att-01.   Ventura County Water Providers by Population Served

Att-02.   Map of Ventura County Water Purveyors

GLOSSARY

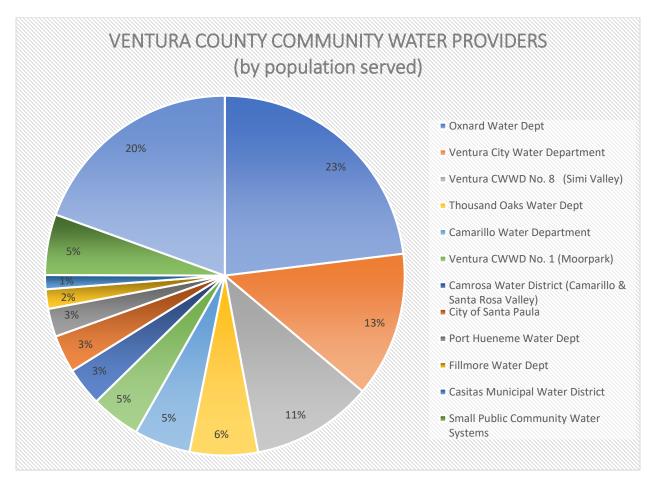| TERM	DEFINITION
ACWA	Association of California Water Agencies
AWAVC	Association of Water Agencies Ventura County
AWWA	American Water Works Association
CISA	Cybersecurity & Infrastructure Security Agency
CWS	Community Water Systems
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
IT	Information Technology
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
VPN	Virtual Private Network
Water ISAC	Water Information Sharing and Analysis Center

Attachment-01

Ventura County Waster Providers by Population Served

VENTURA COUNTY COMMUNITY WATER PROVIDERS
(by population served)

Legend:
- Oxnard Water Dept
- Ventura City Water Department
- Ventura CWWD No. 8 (Simi Valley)
- Thousand Oaks Water Dept
- Camarillo Water Department
- Ventura CWWD No. 1 (Moorpark)
- Camrosa Water District (Camarillo & Santa Rosa Valley)
- City of Santa Paula
- Port Hueneme Water Dept
- Fillmore Water Dept
- Casitas Municipal Water District
- Small Public Community Water Systems

The Grand Jury developed this pie chart and the following table with data from EPA Safe Drinking Water Information Service Federal Reports Search. (Ref-10)

COMMUNITY WATER PROVIDERS	POPULATION SERVED
Oxnard Water Department	200,232
(City of) Ventura Water	113,500
Ventura CWWD No. 8 - Simi Valley	94,738
Cal American Water Company	69,828
Thousand Oaks Water Department	53,157
Golden State Water Company - Simi Valley	43,934
Camarillo Water Department	40,481
Ventura CWWD NO. 1 - Moorpark	38,703
Camrosa Water District	30,000
City of Santa Paula	29,321
Port Hueneme Water Department	21,926
California Water Service Company - Westlake	19,477
Fillmore Water Department	15,222
Oak Park Water Service (now Triunfo)	12,200
Casitas Municipal Water District	11,042

COMMUNITY WATER PROVIDERS (CONTINUED)	POPULATION SERVED
Ojai Water System	6,712
Ventura River Water District	5,700
Channel Islands Beach CSD	5,180
Pleasant Valley Mutual Water Company	5,000
Meiners Oaks CWD	4,200
Naval Base Ventura County, Port Hueneme	3,500
Ventura CWWD No. 19 - Somis	3,275
Warring Water Service Inc.	2,100
Cal American Water Company - Las Posas Estates	2,049
Ventura CWWD No. 17 - Bell Canyon	2,049
Crestview Mutual Water Company	2,040
Vineyard Avenue Acres MWC	1,820
Cal American Water Company - Rio Plaza	1,716
Naval Base Ventura County, Point Mugu	1,700
Ventura CWWD No. 38 - Lake Sherwood	1,527
Vineyard Ave Estates MWC	1,200
Dempsey Road Mutual Water Company	990
Rio Manor Mutual Water Company	983
Nyeland Acres Mutual Water Company	915
Garden Acres Mutual Water Company	840
Limoneira Ranch #1	832
Senior Canyon Mutual Water Company	800
Yerba Buena Water Company	690
Rancho Sespe Workers Imp Association	600
Cloverdale Mutual Water Company	455
Strickland Acres	429
Saviers Road Mutual Water Company	368
Fillmore Irrigation Company	353
Sisar Mutual Water Company	340
Siete Robles Mutual Water Company	323
Casitas Mutual Water Company	238
Cypress Mutual Water Company Inc.	228
Del Norte Mutual Water Company	211
Saticoy Club (Ventura Water)	196
U.S.N., San Nicolas Island	187
Glenview Mobile Park	160
Navalair Mobile Home Park	160
Elkins Ranch	150
Middle Road Mutual Water Company	134
Solano Verde Mutual Water Company	100

COMMUNITY WATER PROVIDERS (CONTINUED)	POPULATION SERVED
Fillmore West Mobile Home Park	99
Tico Mutual Water Company	70
South Mountain Mutual Water Company	58
Community Mutual Water Company	53
Esterina Properties	50
San Cayetano Mutual Water Company	46
Krotona Institute	31
Rincon Water & Road Works	25
Waters Road Domestic Users Group	25

Attachment-02

Map of Ventura County Water Purveyors

Ventura County
Watershed Protection District
December 2009

DISCLAIMER: You may use this map for general information,
However, the information contained herein was created by the
Ventura County Watershed Protection District solely for its own use.
The VCWPD assumes no liability for damages incurred directly or
indirectly as a result of errors, omissions or discrepancies.