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)

United Water
CONSERVATION DISTRICT

August 19, 2022

Ventura County Grand Jury
800 South Victoria Avenue
Ventura, CA 93009

Subject: Response to 2020-2021 Ventura County Grand Jury Report—Cybersecurity of Water Providers in Ventura County

Dear Members of the Ventura County Grand Jury:

Following this cover letter, please find United Water Conservation District's ("District") formal responses to the findings and recommendations of the County of Ventura's Grand Jury Report *Cybersecurity of Water Providers in Ventura County.*

If you have any questions or require additional information, please do not hesitate to contact me at 805-525-4431.

Sincerely,

Mauricio E. Guardado, Jr., general manager

Findings

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

Response: Agree. (Pen. Code, § 933.05(a)(1)).

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding.

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding.

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding. Our cybersecurity staff continues to pursue professional growth and development in this area.

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding.

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding. As part of our facilities fall within FERC-regulated project boundaries, the District is required to report relevant cyber incidents to FERC. Additionally, the District has an ongoing partnership within the FBI Cyberhood Watch program out of the Bureau's Los Angeles Field Office and will make the appropriate reporting to these FBI contacts as appropriate.

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding. As specified in response to F-06 above, the District is an active participant of the FBI Cyberhood Watch program and participates in monthly calls that includes FBI personnel and cybersecurity representatives from regional water providers.

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.

Response: Agree. (Pen. Code, § 933.05(a)(1)).

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

Response: Partially disagree. (Pen. Code, § 933.05(a)(2)).

Explanation: The District does not have adequate insight into this finding. Please see the contents of our response in R-05.

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.

Response: This recommendation has been implemented. (Pen. Code, § 933.05(b)(1)).

Explanation: The District has consistently addressed both IT and SCADA with EPA, CISA, and FERC recommended best practices. As a member of both the dams and water & wastewater critical infrastructure sectors as defined by CISA, the District receives timely updates on best practices. Furthermore, the District's Santa Felicia Dam is under the regulatory purview of FERC and is required to provide updates to the agency's Security Branch on cyber security efforts. In June 2020, FERC conducted a cyber security inspection, and the District has been implementing recommendations by the Security Branch. For context, FERC leverages its in-house cyber security expertise as well as best practices by CISA. In November 2020, the District underwent a Validated Architecture Review Design Assessment by CISA. As a result of this assessment, some of the recommended best practices include the development of an IT Use Policy and implementation of SANS, NIST, etc. best practices. The District also included a cyber component as part of the Emergency Response Plan as required by the EPA.

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 form as the AWAVC.

Response: This recommendation has been implemented. (Pen. Code, § 933.05(b)(1)).

Explanation: The District regularly receives timely cyber threat intelligence reports from a variety of local, state, and federal partners as well as organizations such as MS-ISAC. Additionally, the District's IT Department actively participates in monthly FBI Cyberhood Calls to share information within a trusted environment.

In August 2021, the District arranged a cyber security briefing for the Ventura County Special District Association to discuss both current threats and best practices to mitigate those threats.

R-03 The Grandy Jury recommends that the investigated public water providers use free federal and state expert assistance to enhance cybersecurity.

Response: This recommendation has been implemented. (Pen. Code, § 933.05(b)(1)).

Explanation: The District initiated an inquiry with the Regional CISA Cyber Advisor in 2020. Since then, the District's IT and OT teams have met with CISA staff virtually and on site for various risk-based services and assessments, which are considered industry best practices.

R-04 The Grand Jury recommends that the investigated public water providers regularly conduct cyber awareness training.

Response: This recommendation has been implemented. (Pen. Code, § 933.05(b)(1)).

Explanation: The District has provided cyber security trainings to staff through multiple methods. Virtual training is generally assigned through the District's Learning Management System (LMS). On occasion, the IT Department has hosted lunch-and-learn sessions. Specific, targeted cyber security training has also been and continues to be provided to staff depending on their roles. For example, awareness training on social engineering was provided to the Operations & Maintenance staff at monthly safety meetings.

The IT Team also sends advisories providing awareness and tips to all staff utilizing examples from real phishing email attempts.

On occasion, the District also shared actional-intelligence reporting to the appropriate staff based on their functions within the organization.

R-05 The Grand Jury recommends that the investigated public water providers address recovery from cybersecurity incidents in their business recovery plans.

Response: This recommendation has been implemented. (Pen. Code, § 933.05(b)(1)).

Explanation: The District has incorporated recovery from cybersecurity incidents into the Data Recovery Plan.

R-06 The Grand Jury recommends that each investigated public water provider establish a CISA-compliant internal protocol for reporting cyber incidents.

Response: This recommendation has been implemented. (Pen. Code, § 933.05(b)(1)).

Explanation: The District follows CISA and industry standards for reporting cyber incidents.

# # #