THE WHITE HOUSE

WASHINGTON

September 30, 2023

Governor Michelle Lujan Grisham
490 Old Santa Fe Trail Room 400
Santa Fe, NM 87501

Dear Governor Grisham:

Thank you for providing the New Mexico *Water and Wastewater System Cybersecurity Action Plan*, June 2024. On behalf of the National Security Advisor, we appreciate your timely response to the March 28, 2024, letter requesting that each state prepare an action plan to mitigate cybersecurity vulnerabilities in their water and wastewater systems. State partnership with the federal government is critical in ensuring that water and wastewater systems take necessary steps to reduce risk from and enhance resilience to cyberattacks.

The National Security Council (NSC), Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA) are committed to working with states, as appropriate, to help address the cybersecurity gaps at water and wastewater systems. The NSC and EPA reviewed the New Mexico (NM) state plan in relation to the *Guidance to States on Water System Cybersecurity Action Plans* included with the March 28 letter. While states were welcome to tailor their plans to fit their current programs and capabilities, we have used the recommended goals for state cyber plans from the March 28 guidance to present our understanding of your plan. If we have misinterpreted or overlooked any aspects of your plan, we invite you to send supplemental clarifying information.

Key Take-Aways from Overall State Cyber Plan Review

1. Many states identified resources as a constraint to their cybersecurity program, including funding for additional state personnel, funding to operate state cybersecurity programs, and funding to support individual utility cybersecurity projects.

2. Although fifteen states identified existing state-level cybersecurity requirements, several states cited the need for federal requirements as an important precursor to promote the adoption of basic cyber security practices within their states.

3. Most states offer cybersecurity training, but many have not yet incorporated the important topics of risk mitigation and emergency response planning. Including these topics in cybersecurity training can improve overall resilience at water systems.

What follows is a summary of goals for state cyber plans from the March 28 guidance, a brief description of NM's review, and an appendix covering the status of water sector cybersecurity and proposed future actions in the NM state plan in relation to achieving those goals. Finally, the

summary appendix describes the alignment of the NM state plan with the guidance and areas that NM may consider addressing in further development of the plan.

Goals for State Cyber Plans in Guidance

The recommended actions for state cyber plans in the March 28 guidance were directed towards achieving the following goals for covered water and wastewater systems:

- Determine whether each covered system has recently assessed its cybersecurity practices to identify significant vulnerabilities and direct each system that has not conducted an assessment to establish a plan to do so.

- Assess whether each covered system has a risk mitigation plan to address significant cybersecurity vulnerabilities, work with each system that either lacks or has a deficient risk mitigation plan to develop one, and follow-up with each system to ensure that the risk mitigation plan is implemented.

- Ascertain whether each covered system has an emergency response or incident response plan for a cyberattack, including a schedule to exercise the plan, and follow-up with each system to assure that the plan is updated and exercised.

Summary of NM's Review and Next Steps

Overall, the NM state plan fully addresses all the water sector cybersecurity goals in the guidance, provided that potential barriers identified in the plan to implementing the elements are overcome.

We request that NM provide us with any significant updates or modifications to the plan as it is implemented.

Again, thank you for responding to my request for a state action plan to reduce the vulnerability of water and wastewater systems to cyberattacks. The NSC and EPA look forward to our continuing partnership with you in our joint mission to protect the nation's drinking water and wastewater systems from the threat of cyberattack. If you or your staff have questions or concerns regarding any aspect of this effort, please contact my team at: MBX.NSC.NSC.WaterCybersecurity@nsc.eop.gov

Anne Neuberger
Deputy Assistant to the President and Deputy National Security Advisor Cyber and Emerging Technologies

Appendix: Review of NM State Plan

Scope of the NM state plan

The plan covers public water systems (PWS) and wastewater treatment facilities (WWTF) in NM that serve a population of more than 3,300, subject to a capacity and risk-based phased implementation.

Schedule for the NM state plan

The plan begins with addressing the first component by January 31, 2025, with a final date of June 30,2026 identified to address emergency response plans.

Status of water sector cybersecurity in the NM state plan

The status of water sector cybersecurity in NM is not currently categorized. However, the actions identified in the plan will provide an update.

Actions in the NM state plan

- NM will work with PWSs and WWTFs to facilitate access to the federal and state resources necessary to ensure legal compliance and adoption of best practices.
- NM will provide more intensive guidance and support to high-risk facilities to safeguard these critical systems from cyber threats.

Alignment of the NM state plan and NSC guidance

Guidance Criteria	Present/Absence & Supporting Statements
Determine whether covered water and wastewater systems in your state have recently assessed their current cybersecurity practices to identify significant vulnerabilities using an established method (e.g., a method from EPA, CISA, or AWWA).	Present. NM will use a survey and risk assessment tool to identify and assess risks for all covered facilities, and, more specifically, to identify high-risk facilities/operations, and their associated risk factors.
Contact each covered system in your state that has not conducted an assessment for significant cybersecurity vulnerabilities to request that the water system establish a plan, schedule, and method for conducting the assessment.	Present. NM will direct any facility that has not conducted a cybersecurity risk assessment within the past twenty-four months to do so, and provide guidance and resources offered by the EPA and CISA to complete the assessment. NM will direct facilities to complete EPA's Water Cybersecurity Assessment Tool.
Determine whether each covered system in your state has a risk mitigation plan (or	Present.

equivalent) to address significant cybersecurity vulnerabilities that includes specific actions, schedule, funding (if necessary), and responsible personnel.	NM will collect and analyze survey responses and risk assessments to identify high-risk systems or facilities. The CSO will triage the assessments to prioritize support for the development and implementation of risk mitigation plans for the high-risk exposures.
Work with each covered system in your state that either lacks or has a deficient risk mitigation plan for significant cybersecurity vulnerabilities (per question 3) to establish a process and schedule for developing the plan.	Present. NM will prioritize support for high-risk operations that present the greatest impact risk resulting from a cyber incident, and that lack an adequate risk mitigation plan. The goal will be for each high-risk system to have a mitigation plan responsive to the vulnerabilities that includes specific actions, an implementation schedule, funding, and testing with assigned roles, responsibilities and deadlines. Within the high-risk cohort, support shall be prioritized based on a weighted score that accounts for both risk, as a factor of vulnerabilities, and potential impact, greatest-to-least.
Follow-up with each covered system in your state on a regular schedule to determine if the system is implementing its cybersecurity risk mitigation plan (including documenting modifications to the plan when necessary).	Present. NM will request all systems to verify continued compliance with their program specific mitigation plan, and to provide updates responsive at least annually.
Determine whether each covered system in your state has an emergency response or incident response plan to prepare for, respond to, and recover from a cyber incident, including a schedule to exercise the plan.	Present. NM will support compliance with AWIA, to include guidance concerning cybersecurity emergency response and disaster recovery in the mandated Emergency Response Plan. NM will disseminate general and specific emergency preparedness and response guidance for systems to use in the event of a cyber incident that threatens loss of life, destruction of property or economic injury. The guidance will address incident response practices, and emergency managers roles and responsibilities.

	Recommendation: NM can use EPA's Cybersecurity Incident Action Checklist as a starting point for its emergency response plan guidance.
Follow-up with each covered system in your state on a regular schedule to determine if the emergency response or cyber incident response plan is up-to-date, and that the water system is exercising the plan as scheduled.	Present. NM will support compliance with AWIA, to include guidance concerning cybersecurity emergency response and disaster recovery in the mandated Emergency Response Plan. NM will increase water systems' awareness of risks and drive voluntary cooperation with the various provisions of this plan. NM will enforce the ERP requirements for wastewater systems by incorporating requirements into the five-year GWQB Discharge Permits renewal process after January 1, 2025.