WATER AND WASTEWATER SYSTEM CYBERSECURITY ACTION PLAN FOR THE STATE OF NEW MEXICO

COOPERATING AGENCIES:

State of New Mexico Cybersecurity Office (CSO)

Established through legislation in 2023, the CSO, in coordination with a Cybersecurity Advisory Committee, is charged with protecting the information technology systems of New Mexico's executive agencies from cyber threats. The CSO also serves as a clearinghouse for cybersecurity resources and information for all New Mexico public bodies and is authorized to provide cybersecurity services to all public entities, capacity permitting. The CSO's mission and authorities allow it to support development and implementation of New Mexico's Public Water System Cybersecurity Action Plan as detailed herein.

New Mexico Department of Homeland Security and Emergency Management (DHSEM)

DHSEM works to protect the people of New Mexico through comprehensive and coordinated programs that mitigate hazards, prepare for emergencies, prevent attacks, and recover from disasters regardless of cause. Our department prepares for a wide variety of emergencies, including wildfires, flooding, health crises, impacts to critical infrastructure, and domestic attacks. When necessary, DHSEM assists localities whose capabilities are overwhelmed, and DSHEM serves as the conduit for disaster federal assistance.

New Mexico Environment Department (NMED)

The NMED Water Protection Division implements regulatory programs to protect the environment and human health. These programs include permitting, oversight and enforcement responsibilities associated with drinking water and wastewater systems. The Drinking Water Bureau (DWB) oversees regulatory compliance as well as technical, managerial, and financial assistance of 1,064 public drinking water systems throughout the state. The Construction Programs Bureau (CPB) oversees financial assistance to wastewater systems throughout the state. The Ground Water Quality Bureau (GWQB) issues groundwater discharge permits to wastewater treatment facilities (WWTF), assists communities and oversees groundwater compliance and enforcement. The Surface Water Quality Bureau (SWQB) assists the U.S. Environmental

Protection Agency (EPA) and the U.S. Army Corps of Engineers with implementing surface water permitting programs, permit compliance, and enforcement for WWTFs, and provides technical assistance to WWTFs. The Ground Water Quality Bureau role with WWTF is to control the discharge of water contaminants by issuing Discharge Permits in order to protect groundwater and those segments of surface water gaining from groundwater inflow for present and potential future use as domestic and agricultural water supply and other uses, and to protect public health.

AGENCY LEADERSHIP:

CSO: Raja Sambandam – New Mexico Chief Cybersecurity Officer

DHSEM: Ali Rye – State Director, DHSEM

NMED: John Rhoderick – Water Protection Division Director, NMED

OPERATIONAL LEADS:

CSO:

Melissa Gutierrez – IT Project Manager

DHSEM:

Jim Keefner – Intelligence Bureau Chief

NMED:

Kelsey Rader - Water Protection Division Deputy Director
Joe Martinez – Drinking Water Bureau Chief
Adele McKenzie - Drinking Water Bureau Emergency Response Coordinator
Shelly Lemon – Surface Water Quality Bureau
Justin Ball – Ground Water Quality Bureau

ISSUES AND OBJECTIVES:

Because of the state's arid climate, its historically limited water resources, the ever-expanding demands on those resources, and supply reductions resulting from climate change, water scarcity and conservation are part of the everyday consciousness of many New Mexicans. In New Mexico, every drop matters. Because access to this critical resource has influenced New Mexico's history, culture and economy, and continues to do so, every external force that could adversely impact access to water deserves attention and mitigation. Malicious actors now have the capability, and drive, to disrupt public water supplies and municipal wastewater utilities through the infiltration and manipulation of information technology (IT) systems.

These cyber threats are as potentially disruptive to a community water supply as would be a burst pipe or persistent drought. Using ransomware, a trojan or a virus, a malicious actor can shut down, damage, contaminate or divert a local drinking water or wastewater utility, and cripple a system for hours, days or permanently.

New Mexico must be especially vigilant in addressing water security concerns, particularly as those relate to cyber threats, while also navigating water scarcity. The State will continue to engage with our federal partners in the EPA, FBI and Cybersecurity and Infrastructure Security Agency (CISA) to implement federal and State requirements and best practices.

This plan establishes processes, roles and responsibilities for (1) identifying drinking water and wastewater systems that are vulnerable to high cybersecurity risks, (2) ensuring compliance with cybersecurity laws and directives, and (3) mitigating risks through compliance, oversight and up-to-date emergency response plans. As detailed below, the Cooperating Agencies will work with public water systems (PWS) and wastewater treatment facilities (WWTF) to facilitate access to the federal and state resources necessary to ensure legal compliance and adoption of best practices. The Cooperating Agencies will provide more intensive guidance and support to high-risk facilities to safeguard these critical systems from cyber threats.

SCOPE:

Covered facilities subject to this plan are PWSs and WWTFs in New Mexico that serve a population of more than 3,300, subject to a capacity and risk-based phased implementation.

The initial focus of the plan is to identify systems and facilities that present the highest risk of a debilitating cyber incident and then to assist with the mitigation of those risks. Within this high-risk category are facilities that have operational technologies (OT) exposed to the public facing internet and that present one or more of these risk factors: (1) has not completed a recent cybersecurity risk assessment, (2) does not have backup OT/IT systems, (3) has not implemented MFA, (4) has not updated or patched systems to eliminate known vulnerabilities, (5) has not implemented strong password requirements for network management devices, including firewalls, and/or (6) lacks a cybersecurity incident response and recovery plan. Mitigation for entities that present one or more of these risk factors will be prioritized based on risk score ranking and the potential impact of a debilitating cyber incident.

METHODOLOGY:

Survey and Assessment – To identify at risk facilities, the Cooperating Agencies must establish a compliance baseline. The Cooperating Agencies must identify the current cybersecurity risks, cyber hygiene and compliance practices of the covered facilities. The Cooperating Agencies 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. The risk assessment will pin-point cyber vulnerabilities that will be the focus of mitigation.

Any facility that has not conducted a cybersecurity risk assessment within the past twenty-four months will be directed to do so, and provided guidance and resources offered by the EPA and CISA to complete the assessment. Specifically, the Cooperating Agencies will direct facilities to complete the EPA's Water Cybersecurity Assessment Tool. The CSO will provide instructional guidance and directions to mitigation resources, including EPA services, to support the facilities. The risk assessment process will enable all facilities, including those with only low or medium cybersecurity risk, to achieve compliance with America's Water Infrastructure Act (AWIA) requirements.

Target Completion Date (TCD): January 31, 2025.

Mitigation – The CSO 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. The CSO 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.

Facilities that do not use operational technologies facing the public internet, or that use IT systems only for communications, information and records management may be classified as medium or low risk depending on risk assessment outcomes and potential impacts. These facilities will be referred to EPA and CISA resources for any cybersecurity compliance.

The CSO, in consultation with the New Mexico Cybersecurity Advisory Committee, will establish the scoring criteria and determine the scores that will drive outreach and assistance. The CSO, through its parent agency, the New Mexico Department of

Information Technology, recently conducted cybersecurity risk assessments for executive branch agencies in New Mexico. That process will serve as a model for management of the PWS and WWTF risk assessment process, using the EPA Water Cybersecurity Assessment Tool as the substantive foundation.

A mitigation plan will prioritize rectification of vulnerabilities that contribute to high-risk classification. Specifically, as indicated by the risk assessment: (1) creation of backup OT/IT systems, (2) implementation of MFA, (3) installation of system patches, (4) deployment of access management practices, including firewalls, (5) development of an incident response and recovery plan, including testing (6) hardening servers and workstations, (7) deploying encryption for critical and confidential data, and (8) cybersecurity training focused on human factors risks.

The CSO will offer technical support for implementation of MFA and will encourage covered facilities to leverage free penetration testing services offered by the EPA, to the extent available, to test system for vulnerabilities and strength of defenses. Facilities that cannot access free mitigation and testing through the EPA will be encouraged to receive those through the CSO.

The CSO offers these cybersecurity services:

- **Attack Surface Management (ASM)**: The process of continuously identifying, monitoring, and managing all internal and external internet-connected assets for potential attack vectors and exposures. The ultimate goal of ASM is to increase visibility and reduce risk.
- **Vulnerability Management (VM):** The process of identifying, classifying, prioritizing, remediating, and mitigating security vulnerabilities.
- **Penetration Testing (Pen Testing)**: A security test performed by security experts to attack your cyber defenses and analyze any exploitable vulnerabilities.
- **Cybersecurity Awareness Training:** End IT user education and testing with an emphasis on human factors vulnerabilities, common security risks and mistakes that users can avoid to prevent unauthorized access, reinforced through regular testing (e.g., spoof phishing attempts).

The CSO can extend these services to high risk PWS and WWTF. The CSO will seek funding that will allow it to extend these critical services at low or no cost. Using the CSO provided services will ensure monitoring by personnel that have been trained in the state IT ecosystem, utilizing highly effective cybersecurity tools. This allows rapid identification, classification and response to localized risks and non-risks.

TCD – December 31, 2025 (contingent upon funding)

Emergency Response Plans – The AIWA requires all community water systems[1] serving populations of more than 3,300 to conduct and certify completion of an assessment of the risks to, and resilience of their systems, including an emergency response plan. The Cooperating Agencies will support compliance with AIWA, to include guidance concerning cybersecurity emergency response and disaster recovery in the mandated Emergency Response Plan. The goal of this planning will be to enable resumption of normal operations as soon as possible in the event of a disabling cyber incident. Although there is no corollary state or federal requirement for WWTFs, the Cooperating Agencies will extend this support to high-risk WWTFs as a best practice compliance.

TCD – June 30, 2026

Guidance – In consultation with the CSO, DHSEM will disseminate general and New Mexico 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. DHSEM will also work with the county emergency managers to identify any resources that may be needed in order to assist with recovery efforts. CSO shall provide general guidance for IT system back-up and recovery, and shall, capacity permitting, offer implementation support services or connections to support services.

TCD – June 30, 2025

Compliance Monitoring and Enforcement – Neither the CSO nor DHSEM has regulatory jurisdiction over PWSs or WWTFs. Any mandatory directive required to implement this plan must be based upon, and implemented under, NMED's general authority to regulate water system operators, including enforcing the ERP requirements applicable to certain systems. To the extent that existing enforceable requirements are not sufficient to mandate compliance with cybersecurity directives, NMED will rely on support from the CSO and DHSEM to increase water systems' awareness of risks and drive voluntary cooperation with the various provisions of this plan. For covered facilities, enforceable requirements for GWQB Discharge Permits will be incorporated into the five-year permit renewal process for existing Discharge Permits and incorporated into new Discharge Permits developed after January 1, 2025. Compliance may also be limited by lack of adequate funding for State agency activities, as well as lack of funding for water and wastewater system mitigation and planning activities.

At least annually, the CSO, through NMED, will request all systems to verify continued compliance with their program specific mitigation plan, and to provide updates responsive

[1] New Mexico definitions and categorization of public water systems mirror federal law.

to any intervening changes in their specific IT systems. For annual reviews, the CSO will lead efforts to provide IT support, DHSEM will lead disaster recovery support, and NMED will serve a facilitative role.

TCD – Ongoing

Respectfully Submitted,

DocuSigned by:
437214FBE82C453...

Raja Sambandam
NM State Chief Information Security Officer

DocuSigned by:
Ali Rye
6A6DCF42DCC0487...

Ali Rye, State Director
NM Department of Homeland Security and Emergency Management

DocuSigned by:
John Rhoderick
AAE252B561DC4DE...

John Rhoderick, Water Protection Division Director
NM Environment Department