

**PUBLIC SERVICE COMMISSION
OF WEST VIRGINIA
CHARLESTON**

At a session of the PUBLIC SERVICE COMMISSION OF WEST VIRGINIA
in the City of Charleston on the 16th day of May 2024.

CASE NO. 24-0460-PWD-W-GI

CASE NO. 24-0461-PSD-S-GI

**GENERAL INVESTIGATION INTO CYBERSECURITY
OF WATER AND SEWER UTILITIES**

COMMISSION ORDER

The Commission opens a general investigation to examine water and sewer system cybersecurity.

DISCUSSION

The Public Service Commission was created by the Legislature for the purpose of exercising regulatory authority over public utilities to serve the interests of the public. Its function is to require such entities to perform in a manner designed to safeguard the interests of the public and the utilities.¹ Furthermore, the Commission may investigate all practices of public utilities in the State.²

The Commission has jurisdiction over water and sewer utilities in the State. Further, water and sewer utilities are required to “establish and maintain adequate and suitable facilities, safety appliances or other suitable devices, and shall perform such service in respect thereto as shall be reasonable, safe and sufficient for the security and convenience of the public.”³

Cyberattacks against water and sewer utilities are increasing throughout the United States.⁴ Cyberattacks threaten the distribution of clean and safe drinking water to the public. In addition, cyberattacks can create significant costs to the public and the affected utilities. Vulnerability to cyberattacks threatens water and sewer service at all levels.

¹ Boggs v. Public Serv. Comm'n, 154 W. Va. 146, 174 S.E.2d 331(1970).

² W. Va. Code § 24-2-2(a).

³ W. Va. Code § 24-3-1.

⁴ Alert (AA21-287A), Ongoing Cyber Threats to U.S. Water and Wastewater Systems, <https://www.cisa.gov/uscert/ncas/alerts/aa21-287a>.

Water and sewer utilities are key segments of our infrastructure. Thus, improving cybersecurity for water and sewer utilities is a high priority for the State. Therefore, the Commission will open this general investigation as a means to assess the vulnerability of water and sewer utilities under Commission jurisdiction to cyberattacks.

To initiate this process, the Commission will require all water and sewer utilities to obtain a cyber threat vulnerability assessment. While the Commission does not have specific requirements related to cyber threat vulnerability assessments, state law requires all water and sewer utilities to “maintain adequate and suitable facilities, safety appliances or other suitable devices, and shall perform such service in respect thereto as shall be reasonable, safe and sufficient for the security and convenience of the public.”⁵

Moreover, a water or sewer system shall “inspect its plant and facilities in such manner and with such frequency as is necessary to ensure a reasonably complete knowledge as to conditions and adequacy at all times. Such inspections must comply with the legally applicable requirements of the Minimum Federal Safety Standards (Federal Occupational Safety and Health Administration) and the Bureau for Public Health and the Department of Environmental Protection.”⁶

Pursuant to the National Primary Drinking Water Regulations,⁷ states are required to conduct periodic sanitary surveys of public water utilities.⁸ The Federal Environmental Protection Agency (EPA) interprets the regulations regarding sanitary surveys to include an evaluation of the adequacy of the cybersecurity of any operational technology used in the production and distribution of safe drinking water.⁹ The West Virginia Bureau for Public Health and Department of Health, are the state agencies responsible for conducting sanitary surveys.¹⁰

Thus, to initiate this process, the Commission will require all water and sewer utilities to obtain a cybersecurity vulnerability assessment. To assist water and sewer utilities in this endeavor, the EPA¹¹ and the Department of Homeland

⁵ W. Va. Code § 24-3-1.

⁶ Rule 7.1.5 of the Commission’s Rules for the Government of Sewer Utilities (Sewer Rules), 150 C.S.R. 5; Rule 7.1.2 of the Commission’s Rules for the Government of Water Utilities (Water Rules), 150 C.S.R. 7.

⁷ See 40 C.F.R. parts 141 and 142.

⁸ See, e.g., 40 C.F.R. part 142.16(b)(3).

⁹ See “Evaluating Cybersecurity During Public Water System Sanitary Surveys,” https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508_c.pdf.

¹⁰ See, e.g., Rule 6.1, Public Water Systems, 64 C.S.R. 3.

¹¹ See “Cybersecurity Assessments,” <https://www.epa.gov/waterresilience/cybersecurity-assessments>. To contact the EPA regarding its Water Sector Cybersecurity Evaluation Program,

Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)¹², provide cybersecurity assessment programs at no cost. In addition, the EPA provides a tool that produces an assessment report and risk mitigation plan for the entity. This tool is called the EPA Water Cybersecurity Assessment Tool (WCAT).¹³ Therefore, each water utility and sewer utility subject to the jurisdiction of the Commission must, within sixty (60) days of the entry of this Order, certify to the Commission in a filing in this general investigation that it has contacted either the EPA or CISA to have a cybersecurity vulnerability assessment performed. Once the EPA or CISA has performed the cybersecurity vulnerability assessment, a water or sewer utility must certify¹⁴ to the Commission that an assessment was completed, provide the date(s) of completion, and identify the entity that performed the assessment.¹⁵

In lieu of an EPA or CISA assessment, a water or sewer system may have a cybersecurity vulnerability assessment performed by a different entity at its own cost. Any cybersecurity vulnerability assessment performed by an entity or individual outside of the EPA or CISA's program identified above must conform, at a minimum, with the EPA's Cybersecurity Checklist for Public Water System Sanitary Surveys (Checklist).¹⁶ A water and sewer utility that chooses to have an assessment performed at its own cost must, within sixty (60) days of the entry of this Order, certify to the Commission that it has scheduled a cyberattack vulnerability assessment, and identify the individual or entity that will perform the assessment. Once the cybersecurity vulnerability assessment is performed, a water or sewer utility must certify to the Commission that the assessment was completed, provide the date(s) of completion, and identify the entity that performed the assessment.

see <https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program>.

¹² A free cybersecurity assessment can be administered by a CISA cybersecurity advisor. To contact a regional cybersecurity advisor, see <https://www.cisa.gov/about/regions>. For more information, see <https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf>.

¹³ https://www.epa.gov/system/files/documents/2023-03/EPA%20Water%20Cybersecurity%20Assessment%20Tool%201.0_0.xlsx. More information may be found at https://www.epa.gov/system/files/documents/2023-10/epa-cybersecurity-fact-sheet_508.pdf.

¹⁴ The certification must substantially comply with the form attached to this Order as Attachment B.

¹⁵ Given the sensitive nature of the assessments, the Commission will not collect the results of the assessments or any other documents related thereto.

¹⁶ The Checklist can be found at Section 5 and Appendix A of "Evaluating Cybersecurity During Public Water System Sanitary Surveys," https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf.

The Commission further recognizes that a larger water or sewer utility may have policies and procedures in place to assess and address cyberthreats. If such is the case, the water or sewer utility, within sixty (60) days of the entry of this Order, should certify that it has policies and procedures in place to conduct periodic cyberattack vulnerability assessments, the date of the last assessment, and identify the individual or entity that performed the assessment.

Once an assessment is complete, a water or sewer utility will be required to develop a plan to address cyber threats. In addition, the water or sewer utility will be required to designate an individual employee responsible for compliance with that plan and to attend cybersecurity training for water and sewer utilities. These issues will be addressed in a later Commission Order in this general investigation.

FINDINGS OF FACT

1. Cyberattacks against water and sewer utilities are increasing throughout the United States.

2. The Federal Environmental Protection Agency (EPA) interprets the regulations regarding sanitary surveys to include an evaluation of the adequacy of the cybersecurity of any operational technology used in the production and distribution of safe drinking water.¹⁷

CONCLUSIONS OF LAW

1. The Commission has jurisdiction over water and sewer utilities in the State.

2. All water and sewer utilities are required to “maintain adequate and suitable facilities, safety appliances or other suitable devices, and shall perform such service in respect thereto as shall be reasonable, safe and sufficient for the security and convenience of the public.”¹⁸

3. Because of threats of cyberattacks, it is reasonable for the Commission to open a general investigation and require all water and sewer utilities to have cybersecurity vulnerability assessments performed as discussed in this Order.

¹⁷ See “Evaluating Cybersecurity During Public Water System Sanitary Surveys,” https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508_c.pdf.

¹⁸ W. Va. Code § 24-3-1.

4. Notice of this general investigation should be provided to all water and sewer utilities.

ORDER

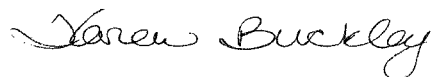
IT IS THEREFORE ORDERED that the Commission opens a general investigation in the cybersecurity of water and sewer utilities.

IT IS FURTHER ORDERED that within sixty (60) days of the entry of this Order, each water and sewer utility shall certify that it has scheduled a cyberattack vulnerability assessment, or that it has policies and procedures in place to assess and address cybersecurity threats, as discussed in this Order. Certification of the assessment completion shall be made using Attachment B attached hereto.

IT IS FURTHER ORDERED that the Executive Secretary publish a copy of Attachment A once in newspapers of general circulation in each of the following cities: Beckley, Bluefield, Charleston, Clarksburg, Elkins, Fairmont, Huntington, Keyser, Lewisburg, Logan, Martinsburg, Morgantown, Moundsville, Parkersburg, Point Pleasant, Weirton, and Wheeling. The Executive Secretary shall thereafter file proof of publication of each notice in this proceeding.

IT IS FURTHER ORDERED that the Executive Secretary serve a copy of this Order on all water and sewer utilities providing service in West Virginia, the Office of the Governor, West Virginia Water Development Authority, West Virginia Department of Environmental Protection, West Virginia Department of Health and Human Resources Bureau for Public Health, Department of Homeland Security, West Virginia Office of Technology, West Virginia Emergency Management Division, by electronic service, or by United States First Class Mail, and on Staff by hand delivery.

A True Copy, Teste,



Karen Buckley, Executive Secretary

JAF/lcw
240460c

**PUBLIC SERVICE COMMISSION
OF WEST VIRGINIA
CHARLESTON**

CASE NO. 24-0460-PWD-W-GI

CASE NO. 24-0461-PSD-S-GI

GENERAL INVESTIGATION INTO
CYBERSECURITY OF WATER AND
SEWER UTILITIES

Cybersecurity Water and Sewer Utilities

On May 16, 2024, the Public Service Commission of West Virginia (Commission) opened a general investigation into the cybersecurity of water and sewer utilities. Water and sewer utilities must provide responsive information as specified in the May 16, 2024 Order to the Executive Secretary of the Commission, Karen Buckley, at P.O. Box 812, Charleston, WV 25323, by Monday, July 15, 2024. Interested parties may review the order opening the general investigation online at <http://www.psc.state.wv.us/>

PUBLIC SERVICE COMMISSION OF WEST VIRGINIA

**PUBLIC SERVICE COMMISSION
OF WEST VIRGINIA
CHARLESTON**

CASE No. 24-0460-PWD-W-GI

CASE No. 24-0461-PSD-S-GI

**GENERAL INVESTIGATION INTO CYBERSECURITY
OF WATER AND SEWER UTILITIES**

CYBERSECURITY ASSESSMENT CERTIFICATION

Pursuant to the Commission Order entered on May 16, 2024, in Case Nos. 24-0460-PWD-W-GI and 24-0461-PSD-S-GI, _____ (Utility Name) provides the following cybersecurity assessment certification.

Utility Name:

ADDRESS:

PHONE NUMBER:

Date of Cybersecurity Assessment:

Person or Company Completing Assessment:

Type of Assessment (self or third party):

I, _____ (name of certifying person) hereby certify that the public utility system named above has conducted or reviewed and updated an annual cybersecurity assessment.

Signature of Owner or Operator: _____ Date: _____

COMPLETED AND SUBMITTED TO:

**Office of the Executive Secretary
Public Service Commission of West Virginia
201 Brooks Street
PO Box 812
Charleston, WV 25323**