NEW YORK STATE OF OPPORTUNITY. | Department of Health

ANDREW M. CUOMO
Governor

HOWARD A. ZUCKER, M.D., J.D.
Commissioner

SALLY DRESLIN, M.S., R.N.
Executive Deputy Commissioner

New York State Community Water Systems
Serving 3,301 people or more

April 25, 2017

Water Supply Vulnerability Assessment – Cybersecurity

Dear Community Water System Administrator:

Water systems provide a critical service to the people of New York State. The Vulnerability Assessments required of community water systems are intended to identify and reduce risks from intentional acts and unintentional events. Regular updates ensure that newly discovered vulnerabilities are addressed as they arise.

Our records indicate that your community water system is subject to the Vulnerability Assessment (VA) and Emergency Response Plan (ERP) requirements of Public Health Law (PHL) Section 1125: Water Supply Emergency Plans. This Section of the PHL was recently modified to require an assessment of cybersecurity in the required VAs. Community water systems are **mandated to begin this assessment by June 1, 2017**, and to **submit the cybersecurity VA to the New York State (NYS) Department of Health (DOH) by January 1, 2018.**

DOH in consultation with the NYS Division of Homeland Security and Emergency Services (DHSES) is providing this guidance to assist you in accomplishing this important task.

<u>Cybersecurity Vulnerability Assessment Options</u>

DOH has identified four options that will result in a strong cybersecurity assessment: either an independent third-party assessment or the use of any one of three assessment tools.

Independent Professional Assessments

- Third-party assessments completed by professional consultants with information security expertise may be used to meet the cybersecurity assessment requirements. To demonstrate this expertise, third-party contractors must, at a minimum, possess cybersecurity certification from at least one of these three entities:
    - ISACA
    - (ISC)2
    - SANS

Cybersecurity Assessment Tools

As an alternative to an independent, third-party assessment, one of the following three tools may be used to satisfy the cybersecurity vulnerability assessment requirements. These may require assistance from independent Information Technology (IT) contractors or consultants. As with a third-party assessment, the utilization of a comprehensive security vulnerability scanner is highly recommended.

For Organizations with Medium to Large Network Presences:

- AWWA Cybersecurity Guide & Tool (http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx); or
- Cyber Security Evaluation Tool (CSET) (https://ics-cert.us-cert.gov/Assessments; scroll towards bottom of web page)

For Organizations with Small to Medium Network Presences:

- The Water System Cybersecurity Checklist developed by DOH in consultation with NYS DHSES and NYS Office of Information Technology Services, Enterprise Information Security Office. This checklist will soon be posted on the NYS DOH Drinking Water website at https://www.health.ny.gov/environmental/emergency/water/drinking/preparing_emergency_response_plans.htm.

Your assessment must assess the vulnerability of each aspect of the IT system used by your water system to conduct both operations and business functions. The results from any of the above methods of assessment must be reported to DOH in a manner, or summarized in a manner, consistent with our standard VA format. Specifically, the assessment should list identified vulnerabilities and provide a prioritized plan with actions and dates for addressing the vulnerabilities.

Cybersecurity Guidance Documents

The following may also be useful guidance documents as you undertake this task:

- USEPA Cyber Security 101 for Water Utilities (http://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P100KL4T.TXT)
- MS-ISAC Center for Internet Security (https://msisac.cisecurity.org/resources/)
- 10 Basic Cybersecurity Measures (https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf)
- AWWA Standard G430-14

Cyber Attack Updates to Emergency Response Plans

Once you have completed your cybersecurity VA, please review your ERP. Your ERP must include an emergency response plan for a cyber attack. This response plan must include actions to be taken and people to be contacted. Contact information for essential personnel and entities is required. You may wish to include a completed copy of the US EPA Cyber Incident Response Guide, a copy of which is enclosed and will also be posted on the DOH drinking water website noted above. The ERP revisions should be submitted along with the cybersecurity VA.

Document Submittals

As with all VA/ERP documents, initial submission of your cybersecurity VA must be through your local health department (LHD). Your LHD may request revisions before they forward your documents on to DOH for approval. You may submit your cybersecurity VA as an appendix to your current VA. Additionally, you may incorporate the cybersecurity VA into your 5-year VA/ERP resubmission providing it is complete by January 1, 2018, the cybersecurity submission deadline.

The DOH values your ongoing efforts to provide clean, safe water to the residents of New York State under all conditions and appreciates your efforts to address this latest threat. If you have any questions about cybersecurity vulnerability assessments, emergency response plans or vulnerability assessments, please contact your local health department representative.

Sincerely,

Roger C. Sokol, Ph.D.
Director
Division of Environmental Health Protection

Enclosure (1):
EPA Cyber Incident Response Guide

cc: Michael Cerretto, Director NYS Office of Counter Terrorism
Deborah Snyder, Deputy CISO
Cecil Elmore, Manager, GRC