STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
NEW HAMPSHIRE CYBERSECURITY INTEGRATION CENTER
27 Hazen Drive | Concord, NH | 03301
Fax: (603) 271-1516 | TDD: (800) 753-2964
https://www.doit.nh.gov/cybersecurity

Ken Weeks, *Chief Information Security Officer*

Date: 2/9/2026

NH House Science, Technology and Energy
Committee
1 Granite Place, Room 229
Concord, NH 03301

Subject: **TESTIMONY IN SUPPORT OF HB 1728, REQUIRING SUFFICIENT CYBERSECURITY ROTECTIONS FOR CRITICAL INFRASTRUCTURE AND TECHNOLOGY PROJECTS**

Enclosures:
(1) Cyber Protections for SCADA Operators Training
(2) Drinking Water Cybersecurity in a Box
(3) Wastewater Cybersecurity in a Box

1. Malicious actors, both nation-state sponsored and cyber criminals are actively targeting Critical Infrastructure sectors across the United States. Several recent examples include:

- In October 2024, American Water, the largest regulated water utility in the US, detected a cyberattack that forced the company to disconnect the MyWater customer portal and pause billing systems as a precautionary measure. Operations were restored within a few days, and regulators were notified.
- The Municipal Water Authority of Aliquippa in Pittsburgh had to shut down its OT systems after a cyberattack from the Iran-backed group “Cyber Av3ngers” on one of its booster stations. The attack shut down equipment that monitors water pressure at the station, forcing the water company to switch to manual monitoring.
- The Municipal Water Division of Oldsmar, Florida, had to defend against a poisoning attack. The actor accessed a utility control network and raised levels of sodium hydroxide to over 100 times their normal concentrations. Sodium hydroxide is dangerous in large quantities but is safely used in everyday water treatment. An operator who noticed the hack in real time – by seeing his mouse cursor move by itself – stopped the chemicals from reaching the water supply.

2. The risk of attacks to New Hampshire and Regional Drinking Water and Wastewater systems is significantly reduced if basic cyber hygiene measures are put in place, such as those outlined in the “standard of care” in HB 1728, currently under consideration.

3. These measures are not expensive to implement and, in many cases, grant-funded programs, leveraging the State and Local Cybersecurity Grant Program (SLCGP), State Homeland Security

Grants, and funding provided by the New Hampshire Department of Environmental Services are available, at no initial cost to the Water/Wastewater System Operator to implement the Standard of Care in HB 1728 and train Water/Wastewater System Operators on Cybersecurity for their respective systems.

4. Details on these grant-funded programs administered and executed by The Atom Group and The Overwatch Foundation can be found on their respective websites:

The New Hampshire Municipal Cyber Defense Program (MCDP)

The Overwatch Foundation Cybersecurity in a Box Programs

5. Additional information on these programs can also be found in the enclosures.

Respectfully submitted,

K.L. Weeks III

K.L. Weeks III
Kenneth L. Weeks III
Chief Information Security Officer

Cybersecurity Training for SCADA Operators

Purpose:

This training session is designed to provide SCADA operators with the essential cybersecurity knowledge and skills needed to protect critical infrastructure from cyber threats. Participants will learn about the latest security measures, best practices, and practical solutions to ensure the integrity and safety of SCADA systems.

Audience:

- SCADA Engineers
- Industrial Control System (ICS) Professionals
- IT and OT Security Personnel
- Plant Managers
- System Integrators
- Security Analysts

Outline of the Training:

1. Introduction to SCADA Systems and Cybersecurity
- Overview of SCADA systems and their critical role in infrastructure
- Importance of cybersecurity in SCADA environments
- Current threat landscape and common attack vectors

2. Remote Access Security for SCADA Engineers
- Securing remote access and connections to SCADA systems
- Implementing robust authentication and authorization mechanisms
- Case studies on successful remote security practices

3. Cybersecurity Testing for SCADA Systems
- Techniques for vulnerability assessment and penetration testing in SCADA environments
- Utilizing tools and frameworks specific to SCADA systems
- Identifying and addressing common security flaws

4. The Importance of Software and Firmware Updates
- Managing software and firmware updates in SCADA systems
- Ensuring compatibility and minimizing downtime during updates
- Real-world examples of the impact of timely updates

5. Setting Up SCADA Controls for Cybersecurity
- Fundamental cybersecurity controls for SCADA systems
- Understanding firewalls, intrusion detection systems, and encryption

6. Incident Response and Recovery in SCADA Systems
- Developing and implementing incident response plans
- Recovery strategies to restore normal operations
- Case studies on effective incident response and recovery

7. Q&A Session

NH Municipal Cyber Defense Program

The New Hampshire Municipal Cyber Defense Program (MCDP), managed by The ATOM Group, is a key initiative for enhancing New Hampshire's Cybersecurity Defense Services. Funded by the NH Department of Information Technology and the State and Local Cybersecurity Grant Program, it aims to protect public trust in technology by providing comprehensive Cybersecurity training.

The MCDP is critical to New Hampshire as it enhances cybersecurity readiness across municipal and public sector entities. This program stands out because it is customized based on the municipality's type, job description, and organization's existing cybersecurity readiness.

For more information, please contact:

Emily McGovern
Cyber Operations Specialist
NH Municipal Cyber Defense Program (MCDP)

Email:
emily@theatomgroup.com

Phone:
603.501.0003 x107

Website:
theatomgroup.com/mcdp

Primex
NH Public Risk Management Exchange

State of New Hampshire DoIT Department of Information Technology

Community Water Cybersecurity "In a Box"

Turnkey protection for Critical Infrastructure

What is our goal?

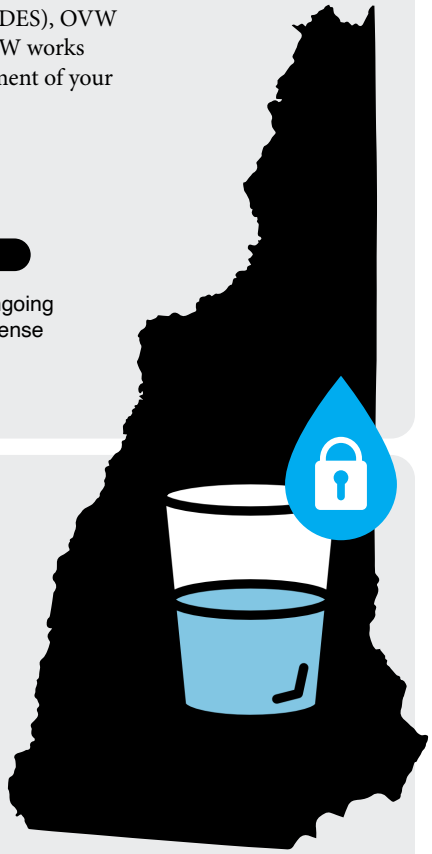
Keep our communities safe by helping prevent cyber emergencies through this grant program. This also helps prevent months of disruption and thousands of hours rebuilding a community compromised by a cyber attack.

How does it work?

Through a successful partnership with the State of New Hampshire Department of Environmental Services (DES), OVW is committed to upgrading equipment for eligible municipality drinking water systems at no cost to you. OVW works with you and your SCADA Integrator, to ensure a smooth and minimally disruptive deployment and installment of your new hardware and software.

APPLY → **ASSESS** → **DEPLOY** → **TRAIN**

- **APPLY**: Fill out form at www.overwatch.org/apply
- **ASSESS**: Work with OVW to provide organizational information to prepare for the deploy.
- **DEPLOY**: Support logistics on the deployment day.
- **TRAIN**: Participate in ongoing OVW cyberdefense trainings.



Our solution offers 4 components:

- 3 years of support
- Community-owned software and hardware
- Secure SCADA systems
- Remote access tablets

What will we need from you?

- ☐ Gain necessary approval for your community to work with OVW and execute necessary contracts within 2 weeks of program acceptance
- ☐ Facilitate IT provider and/or SCADA integrator estimates for approved grant work.
- ☐ Participate in any recommended cybersecurity and incident response training throughout the 3-year support period
- ☐ Be prepared to bring technical support onboard to manage new technology *(e.g.,* firewall, new email accounts, tablets*)*

» What we need most from you is an open mind and a collaborative attitude!

For more information, visit: www.overwatch.org/learn-more
To apply for this grant program, visit: www.overwatch.org/apply

The Overwatch Foundation (OVW), founded in 2022, is a 501(c)(3) not-for-profit foundation that delivers grant-based services in cybersecurity, critical systems modernization, network and physical defense, training, and workforce development to state and local government organizations in New Hampshire and across the nation.

Community Water Cybersecurity "In a Box"

Turnkey protection for Critical Infrastructure

What is our goal?

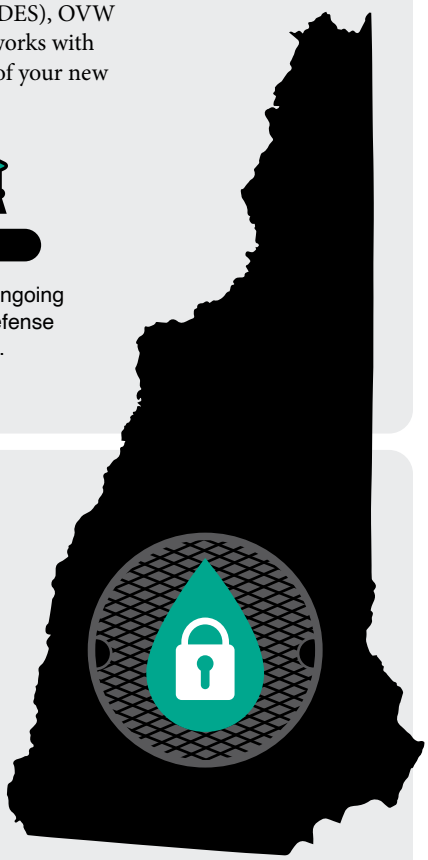
Keep our communities safe by helping prevent cyber emergencies through this grant program. This also helps prevent months of disruption and thousands of hours rebuilding a community compromised by a cyber attack.

How does it work?

Through a successful partnership with the State of New Hampshire Department of Environmental Services (DES), OVW is committed to upgrading equipment for eligible municipality wastewater systems at no cost to you. OVW works with you and your SCADA Integrator, to ensure a smooth and minimally disruptive deployment and installment of your new hardware and software.

APPLY → **ASSESS** → **DEPLOY** → **TRAIN**

- **APPLY**: Fill out form at www.overwatch.org/apply
- **ASSESS**: Work with OVW to provide organizational information to prepare for the deploy.
- **DEPLOY**: Support logistics on the deployment day.
- **TRAIN**: Participate in ongoing OVW cyberdefense trainings.



Our solution offers 4 components:

- 3 years of support
- Community-owned software and hardware
- Secure SCADA systems
- Remote access tablets

What will we need from you?

- ☐ Gain necessary approval for your community to work with OVW and execute necessary contracts within 2 weeks of program acceptance
- ☐ Facilitate IT provider and/or SCADA integrator estimates for approved grant work.
- ☐ Participate in any recommended cybersecurity and incident response training throughout the 3-year support period
- ☐ Be prepared to bring technical support onboard to manage new technology *(e.g.,* firewall, new email accounts, tablets*)*

›› What we need most from you is an open mind and a collaborative attitude!

For more information, visit: www.overwatch.org/learn-more
To apply for this grant program, visit: www.overwatch.org/apply

The Overwatch Foundation (OVW), founded in 2022, is a 501(c)(3) not-for-profit foundation that delivers grant-based services in cybersecurity, critical systems modernization, network and physical defense, training, and workforce development to state and local government organizations in New Hampshire and across the nation.

NH Cyber Defense Program — Powered by ATOM

New Hampshire Department of Environmental Services