Important Reminder from the Operator Certification Board on Cybersecurity Preparedness

The Operator Certification Board strongly encourages water systems throughout the Commonwealth to take all reasonable actions to improve Cybersecurity preparedness. As a starting point, has your water system implemented all the important action items below?

- ☐ **Identified all mission critical assets that are considered hackable?**
- ☐ **Designated one or more internal individuals to address our cybersecurity needs?**
- ☐ **Identified all external support resources? (e.g., CISA, legal resources, insurance, IT experts)**
- ☐ **Considered / researched cyber insurance?**
- ☐ **Trained staff to "Think before you click" to thwart phishing attempts?**
- ☐ **Conducted a recent cybersecurity assessment to identify vulnerabilities in our system?**
- ☐ **Created a detailed action plan / SOP to address all cybersecurity vulnerabilities?**
- ☐ **Incorporated on-going cybersecurity efforts into our long-term planning?**
- ☐ **Changed default passwords?**
- ☐ **Consider a password manager application?**
- ☐ **Implemented phishing-resistant multifactor authentication (MFA) for log-ins?**
- ☐ **Implemented separate user and privileged accounts?**
- ☐ **Created, maintained, and exercised Incident Response Plans?**