MassDEP Drinking Water Program (DWP) considers cybersecurity information to be **sensitive and exempt from public disclosure** under Massachusetts public records law. Specifically, cybersecurity records are protected under **M.G.L. c. 4, § 7(26)**[1], which allows agencies to withhold information that could compromise security or expose vulnerabilities if released. Because of this, cybersecurity assessment details, system configurations, and related materials are treated with heightened confidentiality and are **not maintained, stored, or shared** beyond what is strictly necessary for regulatory review and technical assistance. This approach helps ensure that information regarding critical infrastructure remains outside the scope of public records requests and reduces the risk of misuse.

How MassDEP DWP Protects Cybersecurity-Related Data
MassDEP DWP takes the security and confidentiality of cybersecurity information seriously. Key practices include:

1. **No Record Retention of Cyber Related Documents/Reports**
    - MassDEP DWP does not retain copies of any cybersecurity-related documents from Public Water Systems (PWS).
2. **Sanitary Survey & Cyber Review**
    - During sanitary surveys[2], cybersecurity assessment reports are reviewed **in person or via secure remote methods** (screen sharing) without retaining sensitive data. Based on the review, a **Cybersecurity Corrective Action Plan (CSCAP)** is issued. CSCAPs contain only high-level, non-sensitive information:
        - Attendees at the meeting
        - Type of cyber assessment completed
        - Report date
        - A table of resources
        - A PWS statement committing to address findings
    - To maintain a constructive tone, CSCAPs refer to **"findings"** rather than deficiencies or gaps.
3. **Cyber Grant Program (Link)**
    - Applications are submitted via a secure, limited-access tool.
    - Notifications/Documents about grant approval and progress do not contain sensitive data and use general terms such as **"OT improvements grant."**
4. **Controlled Storage of Cyber Documents**

---

[1] ***Protect sensitive information:*** *Relevant Massachusetts Public Records Law*
*The Massachusetts Public Records Law - MGL c. 4, § 7(26) https://www.sec.state.ma.us/divisions/public-records/download/guide.pdf. Exemption (n) applies to: records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, **emergency preparedness**, threat or **vulnerability assessments**, or any other **records relating to the security** or safety of persons or buildings, structures, facilities, utilities, transportation, **cyber security** or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (c) of section 10 of chapter 66, **is likely to jeopardize public safety or cyber security.***

[2] *MassDEP/DWP considers cybersecurity as part of the routine operations and maintenance of a PWS to ensure the continuous delivery of safe drinking water. Cybersecurity must be addressed in the PWS Emergency Response Plan (ERP) as it can be an act of vandalism or sabotage that has the potential to impact the quality or quantity of water available to the system [310 CMR 22.04(13)(a)9)].*

- Cyber-related documents are stored only on SharePoint with **access restricted to a limited staff group.**

5. **Communication with Public Water Systems**
    - MassDEP DWP uses structured and centralized communication practices to protect cybersecurity-related information:
        - MassDEP Drinking Water Program Director email for general program outreach.
        - MassDEP DWP uses Constant Contact for large-scale emails to PWS.
        - MassDEP DWP Cyber program staff contact PWS using their official work email before any phone calls

By following these practices, MassDEP DWP ensures that cybersecurity-related information remains protected while still supporting PWS in improving cybersecurity and compliance.