PART 1 - SECURITY CULTURE WEBINAR TAKEAWAYS

CYBERSECURITY THREATS

- Most water systems are currently exposed to significant risk of a cybersecurity incident.
- There are many actions that water systems can take to reduce this risk.
- The most important actions are to understand your risk, to train all water system employees and prepare your team to deal with a potential incident.

INSIDER THREATS

Practical Actions to Mitigating Insider Threats:

- Perform a thorough background investigation for potential employees.
- Train all new employees (and trusted partners) in security awareness, including insider threats, before granting access to buildings or systems. This should include janitorial and maintenance staff for security situations they may encounter, such as social engineering, active shooter, and sensitive documents left out in the open.
- Encourage the reporting of and investigate suspicious behavior.
- Consider offering an Employee Assistance Program to help staff deal with stress before it results in a negative action against your utility.

PHYSICAL SECURITY

It is important to protect your computer and network assets from unauthorized physical access. You can do this by:

- Keeping doors and panels locked
  - This may require improving ventilation for people and equipment
- Limiting authorized access
- Training staff and building up a physical security culture with:
  - “If You See Something, Say Something”® campaign
  - “Tailgating” training
- Considering a physical penetration test