PATCHING

- IT and OT systems should not be treated equal.
- Bad guys DO exploit old vulnerabilities.
- Known Exploited Vulnerabilities Catalog & ICS-CERT Advisories help with prioritization.

BACKUPS

- Good backups are essential.
- Store offline and off-site.
- Test your backups to make sure you can restore from them.
- Create and follow a backup policy and procedure.
- Keep backup (spare) parts, especially for your SCADA system.

INCIDENT RESPONSE

- Water systems need to be prepared to deal with incidents of all types, including cybersecurity.
- A failure to prepare can result in a significant impact to the organization or the services it provides.
- Effective response planning covers activities that are undertaken to mitigate the likelihood of an incident, and the consequences if it occurs.
- Response planning must identify all stakeholders and a plan to communicate with them.
- Recovery objectives define backup strategies.
- All incidents must be reported to CISA within 72 hours, and ransom payments within 24 hours.
- Near miss incidents should be reviewed to ensure that any failures of procedures or other controls are effective in future.