

COMMONWEALTH OF KENTUCKY
BEFORE THE PUBLIC SERVICE COMMISSION

IN THE MATTER OF:

| | | |
|---|---|-------------------|
| ELECTRONIC APPLICATION OF ROWAN WATER, |) | CASE NO. |
| INC. FOR APPROVAL OF WATER TRAINING |) | 2025-00133 |

APPLICATION

Come now Rowan Water, Inc., its individual directors, and its general manager (collectively, “Rowan Water”), and Honaker Law Office, PLLC (“Joint Applicants”) to apply for an Order from the Kentucky Public Service Commission (“Commission”) accrediting and approving a proposed water utility training program for continuing education credit pursuant to KRS 74.020 (6) and (7) and 807 KAR 5:070. **We request an Order by June 2, 2025.**

In support of its application, Joint Applicants respectfully state as follows:

1. The full name and office and mailing address of Rowan Water, Inc. is Rowan Water, Inc., 1765 Christy Creek, Morehead, Kentucky 40351. Its electronic mail address is rowanwater@windstream.net.

2. Pursuant to 807 KAR 5:001, Section 4(8), copies of all orders, pleadings, and other communications related to this proceeding should be directed to:

L. Allyson Honaker, allyson@hloky.com
Heather S. Temple, heather@hloky.com
Meredith L. Cave, meredith@hloky.com
HONAKER LAW OFFICE, PLLC
1795 Alysheba Way, Suite 1203
Lexington, Kentucky 40509
(859) 368-8803

3. Rowan Water, Inc. is a water association organized pursuant to KRS Chapter 273.

4. Rowan Water Inc.'s territory includes Rowan, Carter, Elliot, Morgan, and Fleming Counties in Kentucky.

5. Rowan Water, Inc., is a non-profit corporation that was organized under the laws of the Commonwealth of Kentucky on May 21, 1968 and is currently in good standing.

6. Honaker Law Office, PLLC is a Kentucky Limited Liability Company that was organized under the laws of the Commonwealth of Kentucky on June 23, 2022 and is currently in good standing. It provides legal services to local, regional, and national clients.

7. Honaker Law Office, PLLC's mailing address is: 1795 Alysheba Way, Suite 1203, Lexington, Kentucky 40509. Its email for purposes of this Application is allyson@hloky.com.

8. Joint Applicants propose to sponsor and conduct a water management training program on June 12, 2025 at Rowan Water's office in Morehead, Kentucky. The program is entitled **Rowan Water Summer Training 2025**. A copy of the proposed agenda comprised of six hours of training is attached to this Application as **Exhibit 1**. Joint Applicants propose an agenda of five hours of training for the day, including a sixth program on cyber security to be presented at the Rowan Water's August Board Meeting, which is scheduled for the second Thursday of the month.

9. The proposed program has been developed to follow the Commission's recommendations in Case No. 2019-00041¹ and the Commission decisions since that investigative report that prioritize training for the Board of Directors' duty to maintain the financial, managerial, and technical integrity of the utility and which have encouraged discussions with neighboring utilities to coordinate buying materials in bulk, and discussing shared management, equipment,

¹ See Case No. 2019-00041, ("Case No. 2019-00041 Investigation") *Electronic Investigation into Excessive Water Loss by Kentucky's Jurisdictional Water Utilities* (Ky. PSC Nov. 22, 2019), Appendix L, Confronting the Problems Plaguing Kentucky's Water Utilities: An Investigative Report by the Kentucky Public Service Commission November 2019, pp 23-26.

and resources. The training has been designed to support the Commission training regularly provided and will provide the additional hours required for Rowan Water's Directors to be in compliance with Commission Orders² and regulations: As reflected in **Exhibit 1**, the proposed training program will include presentation on the following topics:

a. **Asset Management & Financing**, including a discussion of the current state of assets, managing maintenance, and long-term funding strategy.

b. **What to Expect During a PSC Inspection**, providing an overview of the Kentucky Public Service Commission periodic inspections including an overview of the inspection process, common issues that may be identified during an inspection, and ways to improve inspection outcomes.³

c. **Regulatory Updates**, including a review of Kentucky utility statutes and regulations, and an update of Kentucky court cases, Commission decisions and legislation. Additionally, the presentation will include a discussion of Commission decisions and changes in relevant legislation for water utilities.

d. **Capital Planning Resources**, discussion with a representative from Kentucky Infrastructure Authority (KIA) regarding an update on current funds available, including the federally assisted revolving funds, the infrastructure revolving fund, and the Kentucky Water and wastewater Assistance for Troubled and Economically Restrained Systems fund. The presentation will include the application process, timelines, and federal and state requirements for loans and grants.

² Case No. 2022-00252, *Electronic Application of Rowan Water Inc. for an Alternative Rate Adjustment and Investigation into Rowan Water Inc. and its Individual Directors, Larry Johnson, Randall Cox, Mike Collins, Enoch Blair and its Manager, Jerry Patrick for Allegedly Failing to Comply with KRS 278.300 and a Commission Order* (Ky PSC Oct. 17, 2023) ordering Rowan Water's Directors to obtain 12 additional hours to the regularly required annual 12 hours of training.

³ An outline of the presentation is included as part of Exhibit 3. A copy of the full presentation will be amended prior to the training.

e. **Reducing Water Loss Step by Step**, presentation by an engineer regarding the steps to control, prevent, and reduce water loss.

f. **Cyber Security**, a detailed review of policies to encourage effective management of water utilities through defining roles, understanding duties, and responsibilities and making policy to promote healthy oversight.

10. The proposed training program consists of six hours total (five hours on June 12, 2025 and one hour at the Rowan Water August board meeting, which is scheduled for the second Thursday of the month) of instruction and should be accredited and approved as water management training satisfying the requirements set forth in KRS 74.020(7) to establish a water district commissioner's eligibility for a maximum annual salary of \$6,000. **Joint Applicants are not requesting the proposed training program be accredited as a program of instruction for newly appointed commissioners.**

11. A biographical statement containing the name and relevant qualifications and credentials for the presenters is attached at **Exhibit 2** of the Application.

12. The written materials to be provided to each attendee are attached at **Exhibit 3**. Certain presentations are in outline form and will be amended prior to the training. If any other presentations are amended prior to the training, Joint Applicants will include a copy of any revisions to the presentations with their sworn statement and report regarding the instruction.

13. The Joint Applicants will retain a record of all water utility directors and management staff that attend the proposed training program.

14. Within 30 days of the proposed training program's completion, the Joint Applicants will file with the Commission a sworn statement:

a. Attesting that the accredited instruction was performed;

b. Describing any changes in the presenters or the proposed program curriculum that occurred after certification; and

c. Containing the name of each attending water commissioner or director, their water district, and the number of hours that they attended.

15. The Joint Applicants will admit representatives of the Commission or the Office of Attorney General to the proposed training program at no charge to permit such representatives to assess the quality of the instruction, monitor the compliance with Commission decisions, regulations, or other requirements, should the Commission deem it necessary.

WHEREFORE, the Joint Applicants request that the Public Service Commission approve and accredit the proposed training program entitled, “**Rowan Water Summer Training 2025**” for six hours of water utility management training.

Dated this 30th day of April, 2025.

Respectfully submitted,



L. Allyson Honaker
Heather S. Temple
Meredith L. Cave
HONAKER LAW OFFICE, PLLC
1795 Alysheba Way, Suite 1203
Lexington, Kentucky 40509
allyson@hloky.com
heather@hloky.com
meredith@hloky.com
(859) 368-8803
Counsel for Rowan Water, Inc.

CERTIFICATE OF SERVICE

This is to certify that foregoing was submitted electronically to the Commission on April 30, 2025 and that there are no parties that have been excused from electronic filing. Pursuant to prior Commission orders, no paper copies of this filing will be submitted.

A handwritten signature in blue ink, reading "Meredith Case". The signature is written in a cursive style with a large initial "M".

Counsel for Rowan Water, Inc.

Exhibit 1
Proposed Agenda

Rowan Water Summer Training 2025

Presented by Rowan Water, Inc. and Honaker Law Office, PLLC

1765 Christy Creek, Morehead, Kentucky 40351

June 12, 2025

| | |
|----------------------|--|
| 9:00-9:30am | Registration and Welcome |
| 9:30-10:30am | Asset Management & Financing (1 hour) Robert Miller, StraightLine Kentucky, LLC |
| 10:30-11:30am | What to Expect During a PSC Inspection (1 hour) Jason Pennell |
| 11:30-12:30am | Lunch |
| 12:30-1:30pm | Regulatory Updates (1 hour) L. Allyson Honaker, Honaker Law Office, PLLC |
| 1:30-2:30pm | Capital Planning Resources (1 hour) Russell Neal, Kentucky Infrastructure Authority |
| 2:30-2:45pm | Break |
| 2:45-3:45pm | Reducing Water Loss Step by Step (1 hour) Matthew R. Curtis, P.E., Bluegrass Engineering |

August 14, 2025

| | |
|----------------------|--|
| 10:00-11:00am | Cyber Security (1 hour) Colin Glover |
|----------------------|--|

Exhibit 2

Speaker Qualifications and Credentials

ROBERT MILLER



StraightLine Kentucky - Consultant

Robert Miller is a senior utility executive with thirty-eight years of experience in the drinking water, wastewater, and stormwater industry, including: executive management, strategic planning, policy development, customer service, information technology, and program management. He is an advocate for sustainability of water infrastructure and affordability for low-income customers. His education includes a Bachelors and Masters degree in business management and finance.

JASON PENNELL



Kentucky Rural Water Association -Compliance Specialist

Jason Pennell joined the Kentucky Rural Water Association staff in August, 2017, as a project specialist. Jason's primary duties are focused on the Energy Program but he also assists on other training and technical assistance programs. Jason's experience in the water and wastewater business began in Whitesburg (Veolia Water) in 2005. There he worked as a meter reader, water treatment plant operator, laboratory manager, operations manager and from 2012-2014 he served as the Chief Operator. From (2014-2017), Jason was a Utility and Regulatory Investigator for the Kentucky Public Service Commission. He holds Kentucky certifications/licenses as follows: Class IIIA Water Treatment Operator, Class II Water Distribution Operator, Class II Wastewater Treatment Operator, Class II Collection System Operator, and is certified in Pipeline and Manhole Assessment by NASSCO.

HONAKER LAW OFFICE, PLLC

1795 Alysheba Way, Ste. 6202 Lexington KY 40509

allyson@hloky.com, brittany@hloky.com, heather@hloky.com (859) 358-8803 (o)

L. ALLYSON HONAKER



University of Kentucky College of Law, J.D. – 1999

Admitted to Kentucky Bar - 1999

Clerk, Judge Gary D. Payne – Fayette Circuit Court 1999-2000

Assistant County Attorney – Fayette County Attorney's Office 2000-2006

Associate Attorney, Gambrel and Wilder, Richmond, Ky 2006-2008

Staff Attorney – Kentucky Public Service Commission 2009 – 2013.

Of Counsel and Partner Goss Samford, PLLC 2013 – 2022

Owner – Honaker Law Office, PLLC August 2022 – present.

Allyson has practiced a variety of law over her nearly 24-year legal career. She was a prosecutor for Fayette County and continues to train police officers annually regarding legal issues and procedures. For the past fifteen years, she has focused her practice on utility and energy law. Most of the cases she has handled have been in front of the Kentucky Public Service Commission regarding utility law. She was Staff Attorney at the Kentucky Public Service Commission for approximately four years where she worked on cases involving natural gas, electric and water. As the attorney that handled the accident and the investigation cases dealing with the Division of Inspections, she worked closely with the engineers and inspectors regarding routine inspections as well as the incident investigations. After leaving the PSC, she joined Goss Samford, PLLC of counsel and was later named partner. She worked utility rate cases for large and small gas, electric and water utilities, as well as advocating for utilities on regulatory matters involving a wide variety of energy law issues with Goss Samford for nearly 10 years before it dissolved. After the dissolution, she opened Honaker Law Office PLLC and continues to practice utility and energy law. Allyson is a member of the Kentucky Bar Association and the Fayette County Bar Association. She is general counsel for the Kentucky Gas Association, and regulatory counsel for several electric cooperatives.

HEATHER S. TEMPLE



University of Kentucky College of Law, J.D. – 2003, Kentucky Law Journal

Heather joined Honaker Law Office in January 2024. Heather was a former Staff Attorney for the Kentucky Public Service Commission where she was the lead attorney on cases involving investor-owned utilities, primarily focusing on electric utilities. Heather has experience on rate adjustments, certificates of public use and convenience, integrated resource plans, fuel adjustment clauses, and utility securitized bond transactions. Heather also served as a Staff Attorney for the Kentucky State Board on Electric Generation and Transmission Siting. In that role she served as counsel for the siting of utility scale solar projects and assisted in drafting new regulations.

Prior to practicing utility and energy law, Heather was a criminal defense attorney with expertise in all aspects of criminal and civil motion practice and trials.

Heather resides in Elizabethtown, Kentucky with her husband and daughter.

MEREDITH L. CAVE



University of Kentucky College of Law, J.D. – 2019

Meredith Cave joined Honaker Law Office in February 2025. A graduate of the University of Kentucky College of Law (J.D., 2019), Meredith brings a wealth of experience from her background in commercial civil litigation. She previously focused on malpractice defense, as well as commercial and residential real estate disputes, including quiet title actions, foreclosures, boundary disputes, and eminent domain matters. Recently recognized as a Rising Star by Kentucky Super Lawyers in 2025, Meredith has transitioned into energy and utility law, continuing to build on her expertise in complex legal matters.

RUSSELL NEAL

Kentucky Infrastructure Authority – Staff Assistant to the Executive Director

Russell Neal received his Bachelor of Science degree in Biology, with a minor in Chemistry, from Kentucky State University. He went on to obtain his Master of Aquatic Science degree, also from Kentucky State University. He served in the Kentucky Division of Water for nearly six years in the Drinking Water Technical Assistance Program and later served as supervisor of Municipal Planning for eight years, leading environmental and State Revolving Fund programs. He began serving at the Kentucky Infrastructure Authority (KIA) in July 2024 as a Staff Assistant to the Executive Director to help advance the objectives of KIA through educating and connecting communities with funding options to improve their water and sewer infrastructure.

MATTHEW CURTIS



Bluegrass Engineering, PLLC

Matthew Curtis has over twenty-one years of professional experience as a consultant in the public utility (water, gas, stormwater, and wastewater) sector. He has been responsible for the development of various projects from the conceptual planning, engineering design reports, and overseeing project completion through the construction phase for all aspects of the projects. Mr. Curtis has design experience and supervised various designers and engineers in the development of plans and specifications for wastewater treatment plants and water storage facilities.

Mr. Curtis is the Managing Member of Bluegrass Engineering, PLLC and oversees the day-to-day operation of the company. He also serves as a Project Manager with Bluegrass Engineering, PLLC where his responsibilities include completing contract documents, reviewing schedule and cost of ongoing projects, technical overview of projects, checking completed work under his supervision, and conducting research and investigation for compiling written reports. In addition, he maintains contact with clients during study, design, and construction, and is responsible for follow up after project completion.

COLIN GLOVER



U.S. Department of Homeland Security – Cyber Security State Coordinator

Colin Glover currently serves as a Cybersecurity State Coordinator (CSC) for the state of Kentucky. Mr. Glover supports homeland security efforts and contributes to the development of the national risk picture by identifying, assessing and monitoring risks to critical infrastructure assets.

As a CSC, Mr. Glover serves as the liaison between Federal services and State, Local, Territorial, and Tribal Governments, Critical Infrastructure, and the Private Sector. He serves as the focal point for communications to promote Cyber Preparedness, Incident Response, Risk Mitigation, and Situational Awareness. Colin provides direct coordination, outreach and support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Territorial and Tribal governments.

Prior to joining DHS, Mr. Glover held positions within the private sector assisting companies achieve their cybersecurity goals and in the DoD where he served as a Counterintelligence Special Agent for the Defense Counterintelligence and Security Agency. Amongst other duties, he worked with Cleared Contractors to secure their networks against advanced threats.

Additionally, he served in the United States Marine Corps with multiple combat tours in Iraq.

Mr. Glover has a Master of Engineering and Mechanical and Aerospace Engineering from the University of Virginia. He holds multiple cybersecurity certifications to include Certified Information systems Security Professional (CISSP), Certified Information Security Auditor (CISA), and Certified Ethical Hacker (CEH).

Exhibit 3
Presentations and Materials

Questions that Water Utility Boards Should Ask About Their Utility Finances

Bob Miller
Kentucky Rural Water
Association

Johnnie Baum, CPA
Lebanon Water Works
Company

I'm in the 4th quarter of my career. Some might even say that at this point I'm in overtime. But I'm grateful to be asked to talk about what I've learned along the way.

Back when I was in the 3rd quarter of my career, I focused on helping broken utilities. I went to New Orleans to help after Hurricane Katrina. After eight years there, I went to Jackson Mississippi to help after their catastrophic failed implementation of an automated meter reading and billing system left their finances devastated.

Along the way, I've learned several things. First, water utilities are businesses.

Questions to Ask at Monthly Meeting with Management

2

Second, nearly all of their costs are fixed while nearly all of the revenues are variable. Maybe 80 percent or more of your costs don't vary by water sales volume, while maybe 80 percent or more of your revenues do vary by sales volume.

And third, it's a high transaction volume, low transaction value business. Thousands of transactions each month, most under \$50 each. Anything that disrupts the transactions in your revenue cycle can ruin your finances in a hurry. **When we talk about the revenue cycle, we're talking about meter reading, billing, and collecting.**

What we'll be discussing today are the questions you should be asking in order to keep your eye on the ball: **questions at the monthly board meeting** and **questions at the annual meeting with the auditors**. We'll also be presenting **an example of how the materials you receive each month might look.**

What Expectations Should a Board Have for Financial Information?

- ✓ Timely enough to be relevant,
- ✓ accurate enough to be relied upon,
- ✓ interpreted enough to understand what has happened, and
- ✓ accompanied by recommendations for action.

3

In other words:

What are the numbers?

Are they accurate?

What do they mean?

What are we going to do about it?



When are revenues recognized through?

When is payroll recognized through?

When is accounts payable recognized through?

These should be as close to month-end as possible.

Were there any accruals made to cover the period between the cutoff time for revenues and expenses and month end?



Is the Information Accurate Enough to Be Relied Upon?

1. Were the full set of financial statements prepared?
Statement of Net Position (Balance Sheet)
Statement of Revenues, Expenses, and Changes in Net Position (Income Statement)
Statement of Cash Flows
2. Where there any significant transactions that are not reflected on the financial statements?
3. Where there any errors detected since the financial statements were prepared?
4. Have there been any significant subsequent transactions?



Are there comparisons with Prior Year and Budget?

Are the variances computed in dollar amount and percentage?

Are results presented as Current Month and Year to Date?

Are there graphics that show results over time?

Is **special cause variation** differentiated from **normal variation**?

Does management offer meaningful and reasonable explanations?

Are management's explanations consistent over time?



Does Management Provide Recommendations for Necessary Actions?

Are we travelling “between the navigational buoys”?

Is it “fair weather ahead” or are there “storm clouds on the horizon?”

Is a change in direction needed?

New source of supply?

New water line extension?

New supplier?

Change in customer policies?

Rate increase?

Merger or acquisition?

Sometimes “Steady As It Goes” is all that is needed.

Financial results should be considered in terms of financial objectives.

8

1. **Are we reading all of our meters?**
2. **Are we billing all of our accounts according to our tariff?**
3. **Are we collecting what we are billing?**
4. **How much money do we have access to at our bank?**
5. **How much money did we take in? How much money did we spend?**



1. Are We Reading All of Our Meters?

It all starts with the meter reading. If you don't get the meter reading, everything can go downhill from there.

The key metric to watch is the percentage of meters read.

This can be broken down into meters read automatically versus manually.

The key is to track the number of accounts where no reading was available which requires the bill to be estimated.

It's important to set targets for this:

For automated meters, the read rate should be above 98%.

For manual read meters, the read rate should be above 95%.



What percentage of accounts billed based upon reading versus what percentage of accounts with estimated bills ?

What is the number of accounts with multiple estimated bills in a row?

What is the number of months for account with longest number of estimates?

What is the total quantity of water billed?

What is the dollar value of water billed?

How much water did our Top Ten Customers use?



3. Are We Collecting What We Are Billing?

11

Dollar amount of collections with comparison to amount billed

Percentage of amount collected versus amount billed

Aged accounts receivable: 0-30, 31-60, 61-90, and more than 90 days past due

Number of accounts turned off for non-payment

Top ten accounts with delinquent balances

Top ten accounts with longest delinquent balances



4. How Much Money Do We Have Unrestricted Access to In the Bank?

12

Where do we have our money? Bank names and balances.

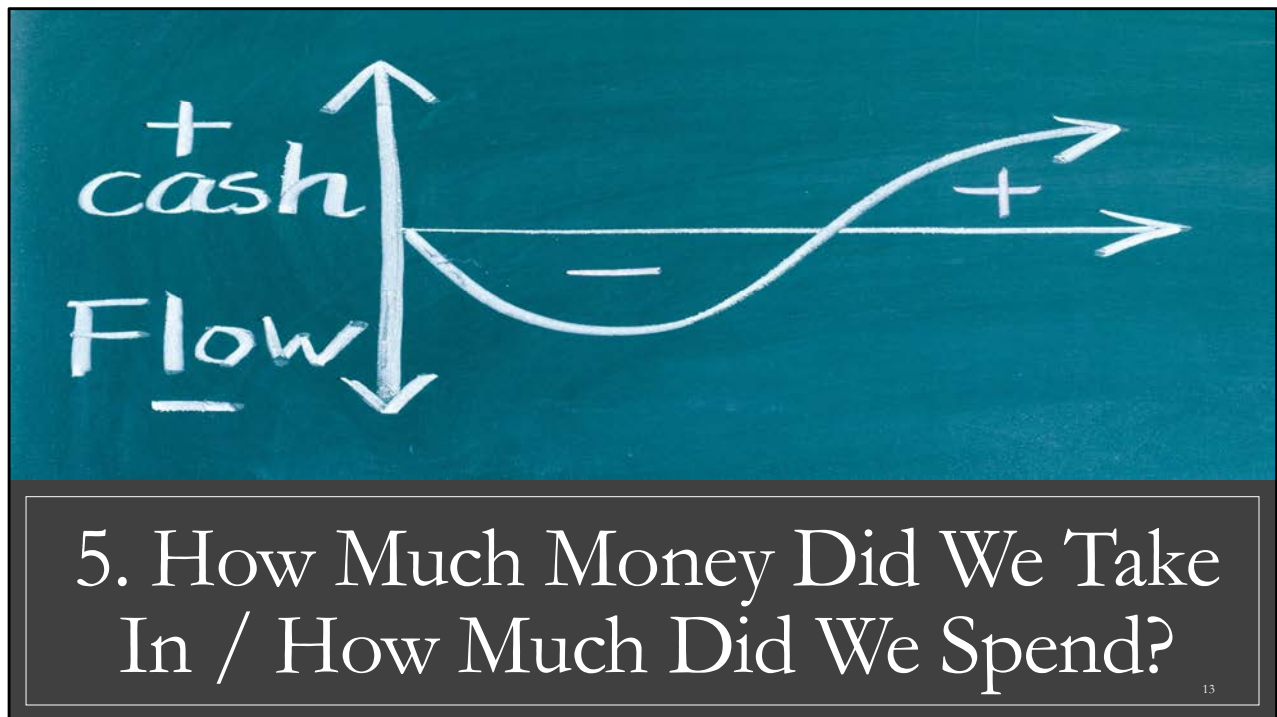
How many days could we operate and pay bills without additional cash coming in?

(Operation and maintenance expenses plus debt service) divided by 365 to compute One Day of Expenses

Total unrestricted cash balances divided by One Day of Expenses to compute Days of Cash: target minimum of 60 days with preferably at least 90 days.

What is our projected debt service coverage ratio?

(Net Income plus Depreciation) divided by annual debt service payment: target at least 1.2 times, preferably 1.5 times or more.



Is our net cash flow for the month positive or negative?

What bills did we pay last month?

Is there a clear description for each payment?

Are we paying our bills on time?

What percentage of invoices are paid before the due date?

Are we “sitting on” any invoices? Even when unprocessed and unpaid, these invoices represent expenses and liabilities.

Practical Examples of Financial Information Presentation

14

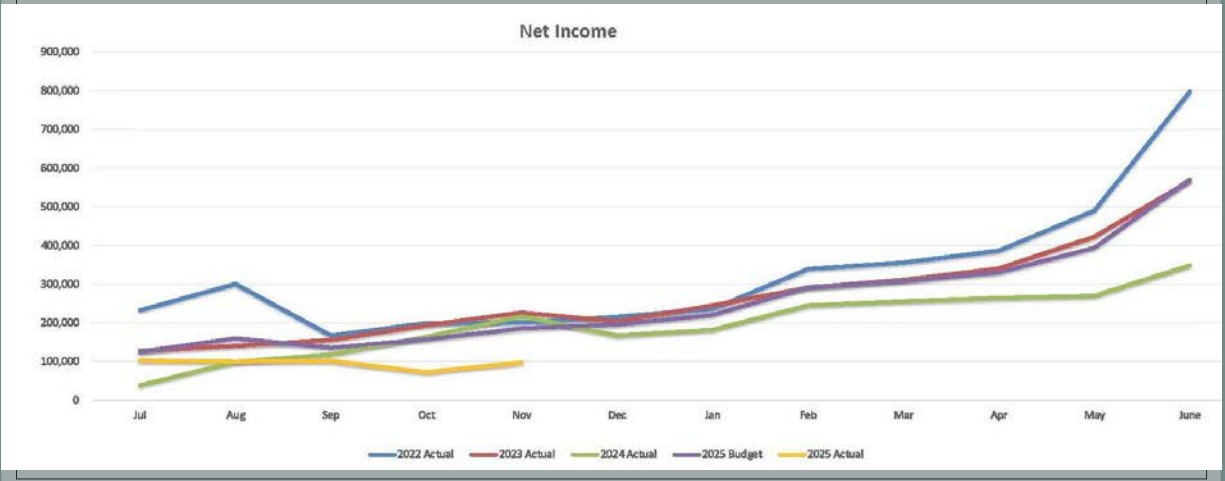
Johnnie Baum is a CPA and the CFO for Lebanon Water Works Company and Springfield Water and Sewer Commission. He's going to describe how he presents financial information to his board each month. He's also going to go through the questions you should consider asking your auditor each year.

Key Performance Indicators

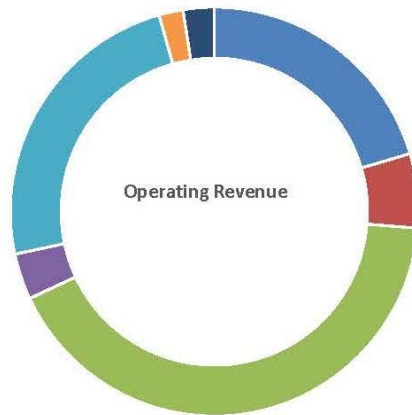
Key Performance Indicators

| | 11/30/2024 | 11/30/2023 | | |
|------------------------------|---------------|---------------|---|--------------|
| Net Op Rev YTD | \$ 97,926 | \$ 216,995 | ↓ | \$ (119,069) |
| Net Op Rev MTD | \$ 25,512 | \$ 52,970 | ↓ | \$ (27,458) |
| Net Profit Margin | 10.50% | 12.47% | ↓ | -1.97% |
| Capital Assets | \$ 40,799,649 | \$ 39,828,457 | ↑ | \$ 971,192 |
| % Capital Depreciated | 43.8% | 43.2% | ↓ | 0.62% |
| Debt Ratio | 44.2% | 45.3% | ↑ | -1.09% |
| Debt Service Coverage | 160% | 164% | ↓ | -4.00% |
| Cash EOP | \$ 3,233,649 | \$ 2,939,681 | ↑ | \$ 293,968 |
| Days Cash | 108 | 98 | ↑ | \$ 10 |
| Depreciation Funded variance | (73,545) | (30,823) | ↓ | \$ (42,722) |
| Deprecation Funded % | 69.9% | 86.2% | ↓ | -16.28% |

Net Operating Revenue

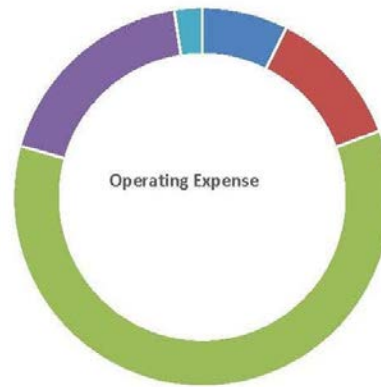


OPERATING REVENUE



- Residential/Small Business Sales
- Commercial Sales
- MCWD Sales
- Public Sales
- Industrial Sales
- GIS
- Penalties/Other

OPERATING EXPENSES

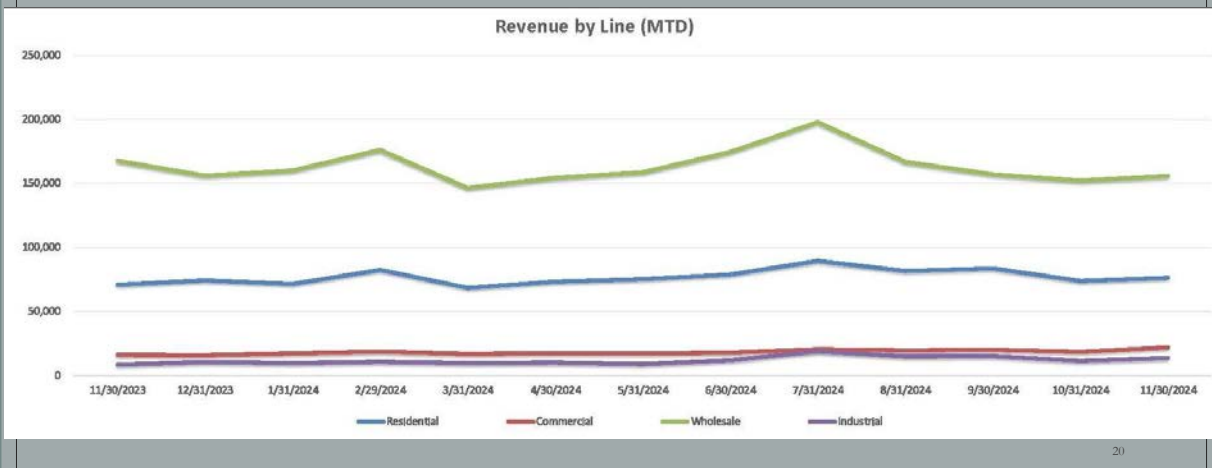


» Power & Chemicals » Purchased Water » Other Operating expense » Depreciation and amortization » GASB pension actuarial adjustment

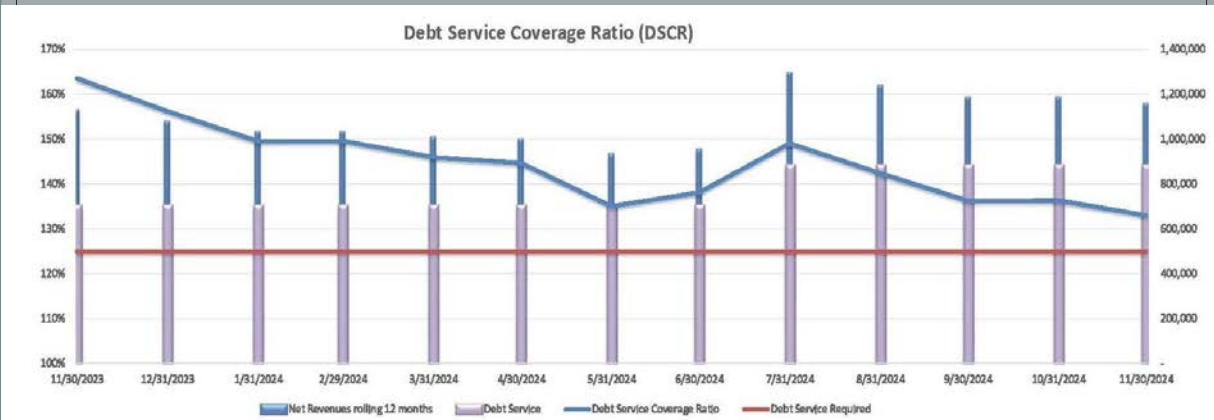
Profitability Ratios



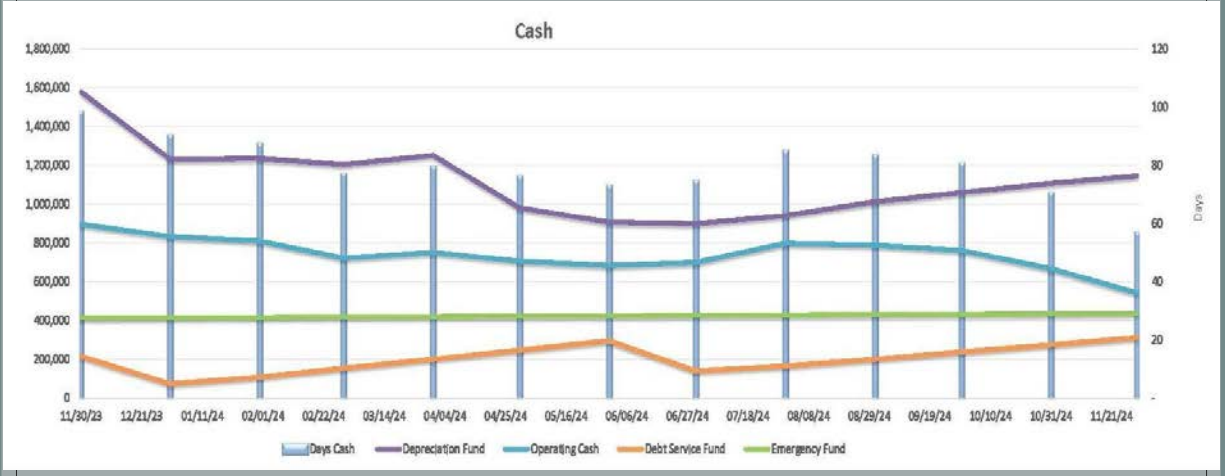
Revenue by Customer Class



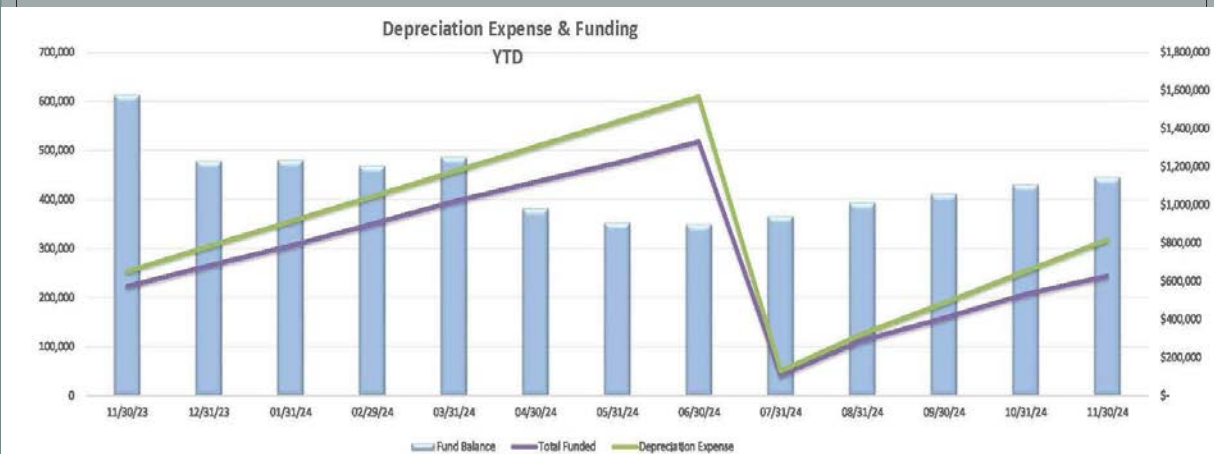
Debt Service Coverage Ratio



Cash Amounts and Days



Depreciation Expense and Funding



Accounts Receivable Balance



Questions to Ask at Annual Meeting with Auditors

25

The Board should meet with the auditor without management and staff present. The meeting can remain “open” unless there are specific reasons to go into closed session that meet the statutory requirements.

The discussions should be candid so that the board can have a clear understanding of the reliability of the financial statements.

The auditor should be treated as a professional that is neither the friend or the foe of management.

Focus on Internal Controls

A process designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- ✓ effectiveness and efficiency of operations
- ✓ reliability of financial reporting
- ✓ compliance with applicable laws and regulations.

26



1. Can You Explain the Audit Process?

What was specifically included in the audit scope?

What was specifically excluded from the audit scope?

Who worked on the audit?

How long has each person been assigned to this account?

Who prepared the Management Discussion and Analysis?

Was the audit completed within the number of hours budgeted for project?

What threshold did you consider for materiality?

Does the auditor perform audits for any other similar entities?



Were the changes in accounting policy intentional or inadvertent?

How do any changes in accounting policies affect the presentation of the financial statements?

Were there any significant changes in accounting or billing software?

Did the software changes have any significant effect on the financial statements?



Were management and staff ready for the audit when you arrived?

Were management and staff cooperative?

Were management and staff available for questions when needed?

Were management and staff sufficiently knowledgeable?

Were requested records produced in a timely fashion?

Were records prepared in an orderly fashion?

The Difference Between Concern And Worry



4. Did You Identify Any Areas of Concern?

30

Were the checking accounts balanced each month?

Did you find any evidence of fraud?

Did you find any overly complex transactions?

Where there any surprises?

Did you find any occasions where management overrode the internal controls?

Does the auditor believe that the Board is sufficiently monitoring the financial condition of the utility?



5. What Weaknesses Did You Identify in Our Reporting and Controls?

31

Were there any weaknesses in internal control identified?

How did the auditor identify the weaknesses?

How serious were the weaknesses?

How long have the weaknesses existed?

Did the weaknesses affect the auditors opinion provided?

Did management have a response to the weaknesses identified?

Does management have a reasonable plan to address them?



6. Were There Any Adjustments Made to the Financial Statements?

32

The adjustments should be reviewed one-by-one.

Why the adjustments had not already been made by management?

Does the size of the adjustments impact the Board's understanding of the utility's financial condition during the year?

Does the auditor believe that similar adjustments will be needed in the future?

Is it realistic to expect that a utility would not have any adjustments?



7. What Regulations Did You Review For Compliance?

33

How do you monitor changes in regulations affecting our utility?

Are you aware of any noncompliance with those regulations?

What is the significance of noncompliance?

What new regulations have upcoming due dates?

Do you think that we are prepared to meet those new regs?

How do you recommend that we maintain awareness of new regulation?

Do you have recommendations for improving this board's ability to monitor compliance?



Will we need any short term borrowings in order to continue operations?

Will we need to pursue an increase in rates this year?

Do we maintain enough cash reserves to meet emergency needs?

Are our bank accounts sufficiently secure?

Do we have adequate insurance coverage?

Are there any new insurance coverages that we should consider?

CHANGE



loading...

9. Are There Any Changes in Practice That We Should Adopt?

35

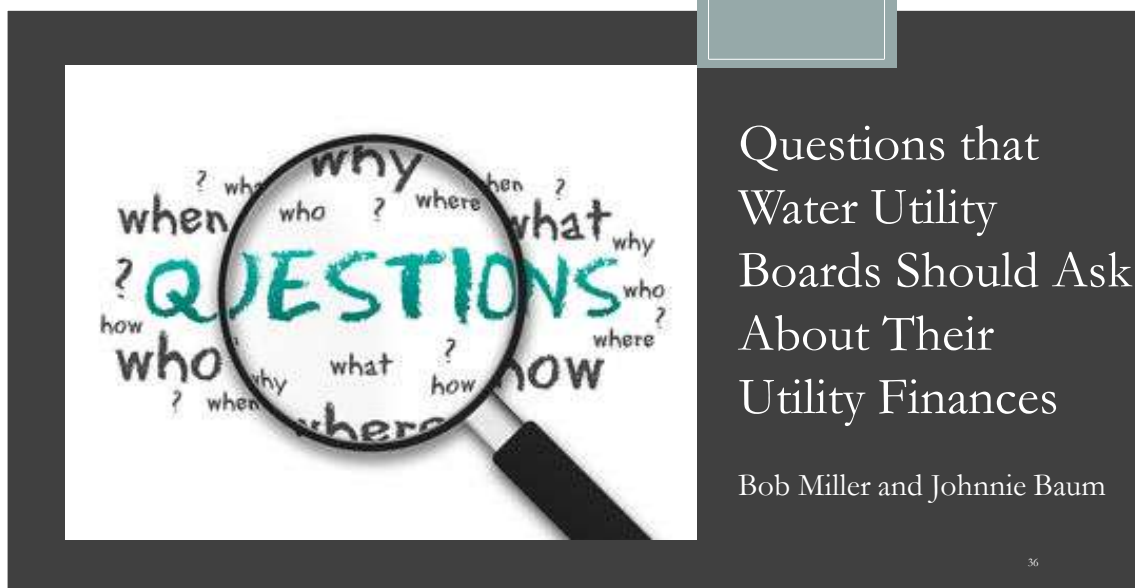
Are there any other clients of yours that you would recommend that we consider their practices?

Is there any training that our staff needs?

Is our staff sufficiently cross-trained to continue operations if a key employee departs?

Is our staff sufficiently compensated to prevent the loss of key employees?

Are our billing and accounting software systems sufficient for the coming year?



Asking these questions on a monthly and an annual basis will help you get the information that you need so that the decisions that you make can keep your utility financially healthy.

We're ready to take your questions now.

What to Expect During a PSC Inspeccion

Jason Pennell
Kentucky Rural Water Association



Today's Topics

- Division of Inspections
- Inspection Process
- Areas of Concern
- Water Loss

PSC Mission Statement

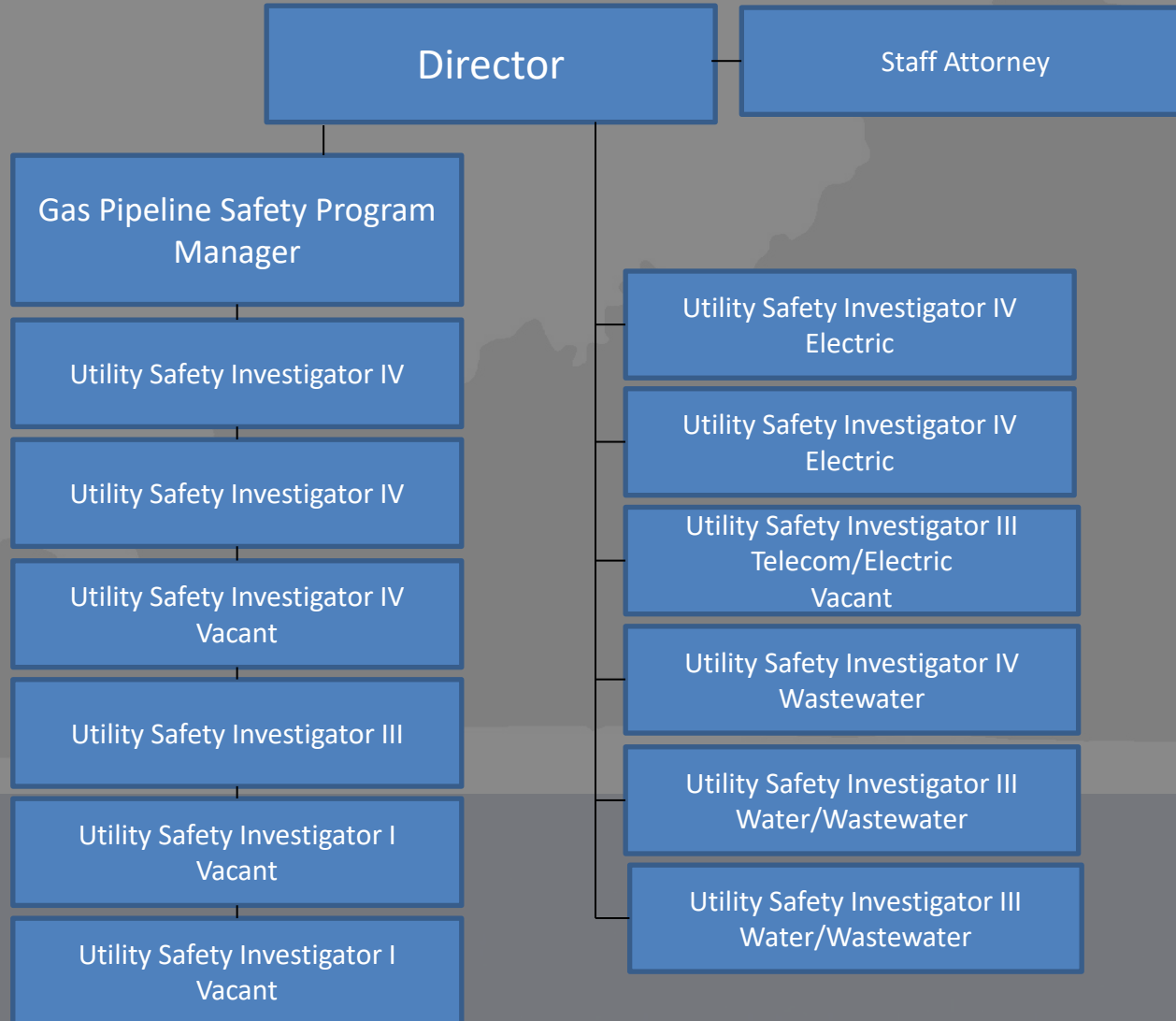
- To foster the provision of safe and reliable service at a reasonable price to the customers of jurisdictional utilities while providing for the financial stability of those utilities by setting fair and just rates, and supporting their operational competence by overseeing regulated activities.

Water and Wastewater Utilities Under PSC Jurisdiction

- Investor-owned utilities
- Water districts
- Water associations
- Municipal water utilities BUT only the wholesale rates for water sold to a utility under full PSC jurisdiction
- Wastewater utilities – No municipalities*

* KRS 278.010(3) excludes “a city” from the definition of a “Utility”

Division Of Inspections



Regulated Water Utilities

- In 2023, the PSC received annual reports from 116 of 138 drinking water utilities throughout the state serving residential, commercial and industrial customers:
 - 5 Investor-Owned – AMB \$ 65.97
 - 17 of 20 Water Associations – AMB \$ 43.85
 - 94 of 112 Water Districts – AMB \$ 51.57
 - 731,206 Customers
- \$ 471,384,883 Total Revenues
- 632,349,509,000 gallons sold

* Source - 2023 annual reports submitted to the Kentucky Public Service Commission



Regulated Wastewater Utilities

- In 2023, the PSC received annual reports from 32 of 53 wastewater utilities throughout the state serving residential, commercial and industrial customers
- 36,644 Customers
- Total Revenues \$ 26,062,601
 - Residential AMB - \$ 44.87
 - Commercial AMB - \$ 97.32
 - Industrial AMB - \$ 3,214.60

Improving The Inspection Process

- Three investigators for the water and wastewater sectors
- IRS database
- Standard Operating Procedures
- Inspection cycle
- As of January 2019, now scheduled annually
- **Risk Assessment (Water Utilities)**
- Now collaborating with the Division of Water
 - Drinking Water and Wastewater Advisory Councils
 - Data sharing – Boil Water Advisories

Risk Assessment

- Seven Metrics
 - Number of deficiencies last inspection
 - Unresolved deficiencies
 - Excessive water loss %
 - Management/employee turnover
 - Inspector's subjective knowledge
 - Construction activity
 - Elapsed time since last inspection
- Higher point value will warrant more attention

Inspection Process

- Contact utility to set inspection date(s)
- Utility is provided a document list and inspection checklist
- Internal records review
 - Case history
 - Annual Reports/Water Produced/Purchased/Loss
 - Previous Inspections
- Go through inspections checklist, reviewing utility documentation at office
 - Line break logs
 - Fire Dept. usage
 - Pressure charts
 - Facility self-inspections (plant, tanks, manholes, etc.)

Inspection Process cont.

- Field Review
 - Plant
 - Tanks
 - Pump/lift stations
 - Construction projects
 - Safety/Security
- Exit Interview
- Inspection provided to utility approximately 30 days later

Inspection Process cont.

- Full internal review of inspections by executive staff and the commissioners
- Frequent internal discussion on cited deficiencies
- Utility given 30 days to respond to deficiencies
- Failure to respond or to correct deficiencies will result in initiation of formal action
 - Informal Conference
 - Show Cause Hearing

Areas of Concern

- **Water loss***

- Water Districts – 34.54% or 103 billion gallons
- Water Associations – 22.16% or 31 billion gallons
- Investor-Owned – 18.12% or 3 billion gallons

- Abandonment of Utilities

- Infrastructure

- Written documentation of facility inspection procedures and other required records

*Source - 2023 annual report statistics compiled by the Kentucky Public Service Commission



Water Loss

- Excessive water loss will be a primary focus of PSC interactions with water utilities
 - PSC's position is that excessive water loss poses a threat to the utility's financial and operational stability & viability
 - Point of emphasis at PSC training seminars
 - Water loss exceeding 15% will be cited as a deficiency by water system inspectors
 - Rate cases, purchased water adjustments, CPCNs and water financing cases will all include language on water loss in excess of 15%
 - A utility's inability or continued inaction to reduce water loss will lead to greater PSC attention

Water Loss

- Annual Reports are being reviewed to identify utilities with water loss in excess of 15% (61 systems reported > 15%)
- Deficient utilities will:
 - Be cited with 5:066, Section 7 – Standards of Construction
 - Receive letter copying water commissioners and where applicable, the County Judge Executive/Magistrates

Water Loss

“**Water loss**” means the sum of all water purchased and produced by the utility less the volume of water:

(a) Sold;

(b) Provided to customers without charge as authorized by the utility’s tariff; and

(c) Used by the utility to conduct the daily operation and maintenance of its treatment, transmission, and distribution systems.

807 KAR 5:095

Section 9. A utility that permits a fire department to withdraw water from its water distribution system for fire protection and training purposes at no charge or at reduced rates shall:

- (1) Require a fire department to submit quarterly reports demonstrating its water usage for the quarter; and
- (2) State in its tariff the penalty to be assessed for failure to submit the reports required by subsection (1) of this section.

Commission Orders

- The Commission is placing greater emphasis on monitoring utilities that consistently exceed the fifteen (15) percent water loss threshold and strongly encourages *Subject Utility* to pursue reasonable actions to reduce its water loss. Failure by *Subject utility* to make significant progress towards reducing water loss may cause the Commission to pursue additional action with the utility.

Suggestions

- Ensure accurate reporting
- Review and document water loss reduction efforts
- PSC will consider utility requests for surcharges to assist in financing water loss reduction efforts

Contact Information

Jason Pennell
j.pennell@krwa.org
270-843-2291

HONAKER
LAW
OFFICE

ROWAN WATER SUMMER TRAINING

HONAKER LAW OFFICE, PLLC

L. ALLYSON HONAKER

► June 12, 2025

Regulatory Update of COMMISSION ORDERS & RELEVANT LEGISLATION

HONAKER
LAW
OFFICE

Introduction & Disclaimer

HONAKER
LAW
OFFICE



- ▶ On the waterfront – bills relating to water fluoridation programs (HB16 & SB180), eminent domain (SB171 & HB353), sanitation districts (HB 85), Public Service Commission (SB8), and PFAs (HB102), among others did not pass this session.

Legislative Update

Legislative Updates

However, Senate Bill 89, initially vetoed and later overridden, has now been delivered to the Secretary of State to become law. SB 89 revises the definition of Waters of the Commonwealth to more closely align with federal Waters of the US definitions. In its final form, the bill reflects input from KRWA and industry stakeholders, working collaboratively with legislators to more effectively address some key water quality concerns.

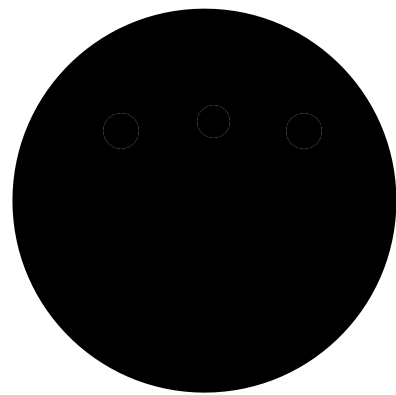
HONAKER
LAW
OFFICE



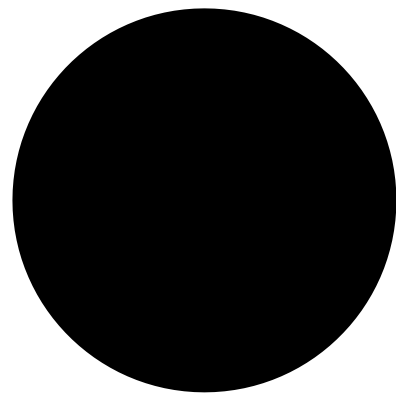
COMMISSION UPDATE TOPICS:

- * Show your work
- * Play nice with others
- * Know your surcharges
- * Noteworthy investigations
- * Advantageous agreements

Show Your Work



PSC saw several applications for water storage tank replacement that lacked repair or inspection records.



PSC CaseNo. 2024-00348:The Water District was asked to describe preventative maintenance, parts replacement, and repairs to their water storage tank including dates and expenditures. The response identified the tank's needs but failed to provide record of any preventative actions. PSC admonished the Water District to perform required maintenance on assets in the future.

HONAKER
LAW
OFFICE

Play Nice with Others: Case No. 2025-00022

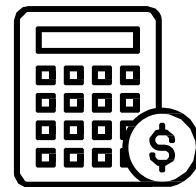
Issue: City issued public comment on Water District's Application for CPCN to construct water system improvements



Response: Water District responded calling out City's inability to provide the highest quality and most reliable water noting issues with water loss, disinfection byproducts, inability to cope with flash freezes, and poor communication skills.



PSC's Order: held that, based on City's comment, an investigation was necessary to determine the reasonable necessity and appropriateness of the request and continued the application.



HONAKER
LAW
OFFICE

SURCHARGES

Stay inside the
surcharge time
period!

* 2025-0403: The commission denied a request to approve the use of water loss surcharge funds for meters installed in 2019 because the installation occurred prior to the water loss surcharge being granted.

Noteworthy investigations:

* In 2024-00325, the Commission advised that it is placing a greater emphasis on monitoring utilities that consistently exceed the 15 percent unaccounted-for water loss. The Commission advised the water district to study its system to identify sources of unaccounted-for water loss.



Advantageous Agreements

IN 2024-00202, THE WATER DISTRICT ENTERED INTO 2 AGREEMENTS:

1. **ASSISTANCE AGREEMENT** WITH THE WATER PLANT BOARD TO ASSIST WITH METER INSTALLATION, METER READING, METER TESTING, PROJECT PROFILES, GRANT AND LOAN APPLICATIONS, DEVELOPING A CAPITAL IMPROVEMENT PLAN, AND OTHER SERVICES. IN EXCHANGE, THE WATER DISTRICT AGREED TO PAY THE PLANT BOARD'S COST OF LABOR, EQUIPMENT, MATERIALS, ETC.
2. **MUTUAL AID AGREEMENT** WHEREBY THE WATER PLANT BOARD AGREED TO PROVIDE EMERGENCY WATERLINE REPAIR SERVICES

THESE AGREEMENTS ALLOWED THE WATER DISTRICT TO DEVELOP A CAPITAL SPENDING PLAN, ACCOMPLISH METER REPLACEMENT, AND OBTAIN FUNDING TO FINISH AC WATERLINE REPLACEMENT WHILE ALLOWING THE DISTRICT AND THE BOARD TO MORE KNOWINGLY CONSIDER A JOINT OPERATIONS AGREEMENT IN THE FUTURE.

HONAKER
LAW
OFFICE

QUESTIONS

- ▶ L. Allyson Honaker
- ▶ ALLYSON@HLOKY.COM
- ▶ (859)396-3172



HONAKER
LAW
OFFICE

Capital Planning Resources:
WRIS Portal, State Revolving Fund, Clean Water Act Grants
Presented by: Russell Neal, Kentucky Infrastructure Authority

- I. Introduction
 - a. Background on KIA
- II. Current Available Funds
 - a. Federally assisted revolving fund
 - b. Infrastructure revolving fund
 - c. Kentucky Water and wastewater Assistance for Troubled and Economically Restrained Systems fund
- III. Loan and Grant Overview
 - a. Application process
 - b. Timeliness
 - c. Federal requirements
 - d. State requirements
- IV. Conclusion and Q&A

Reducing Water Loss Step by Step Approach

Allen County Water District



Juan Martinez, ACWD



Matt Curtis, Bluegrass Engineering

February 21, 2024

**Kentucky Rural Water Association
Management Conference**

Bluegrass Engineering, PLLC

- Utility Consulting Firm established in 2017
- Located in Georgetown, KY
- Work for 35+ utilities across the Commonwealth of Kentucky



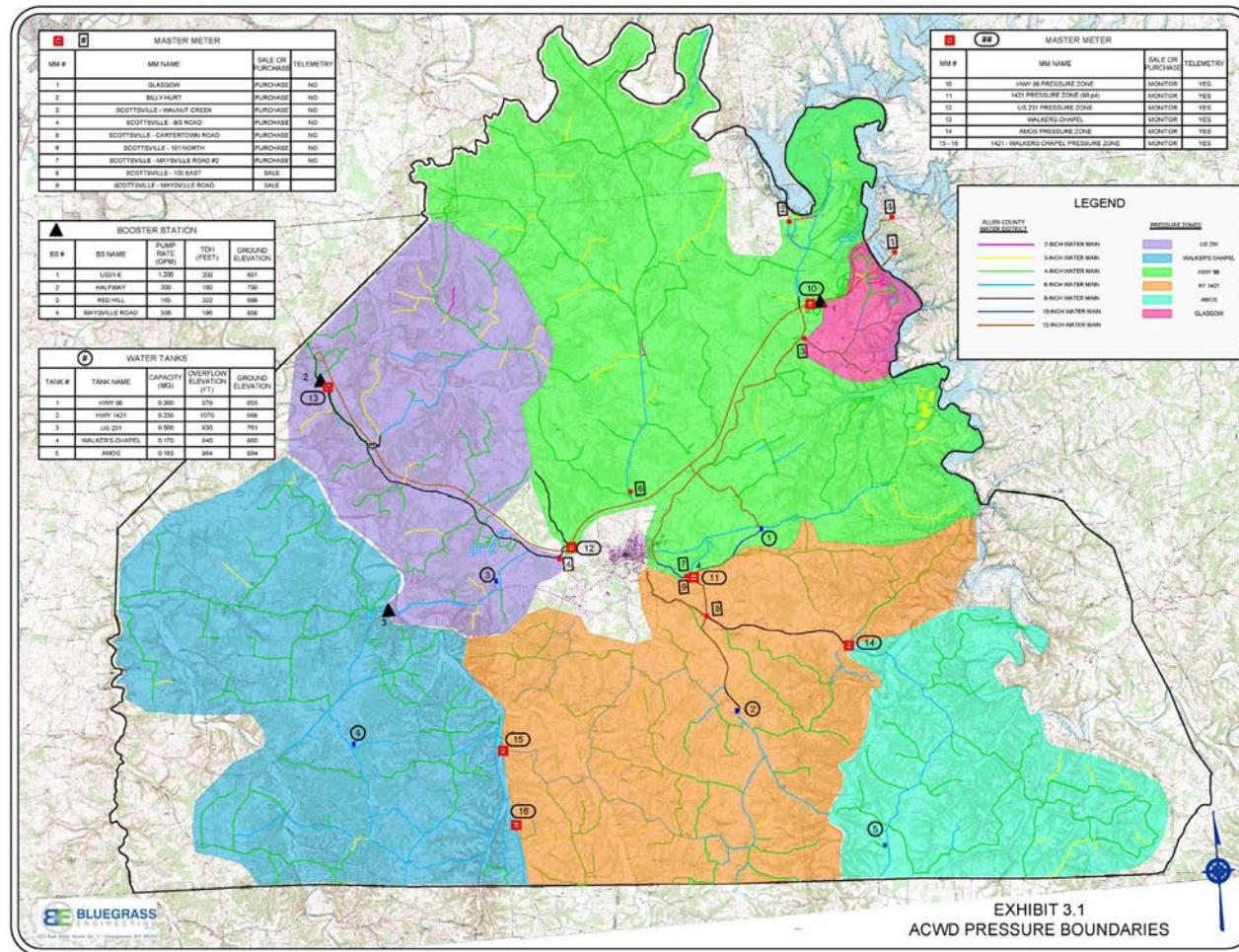
Allen County Water District

- Water District (KRS Chapter 74) formed in 1974
- Purchases water from Glasgow Water Company & City of Scottsville
- ~6,500 total customers
- Historic Water Loss from 20% - 40%
- Operate Six Pressure Zones – Pressures from 35 – 200 psi



Allen County Water District

- System Makeup



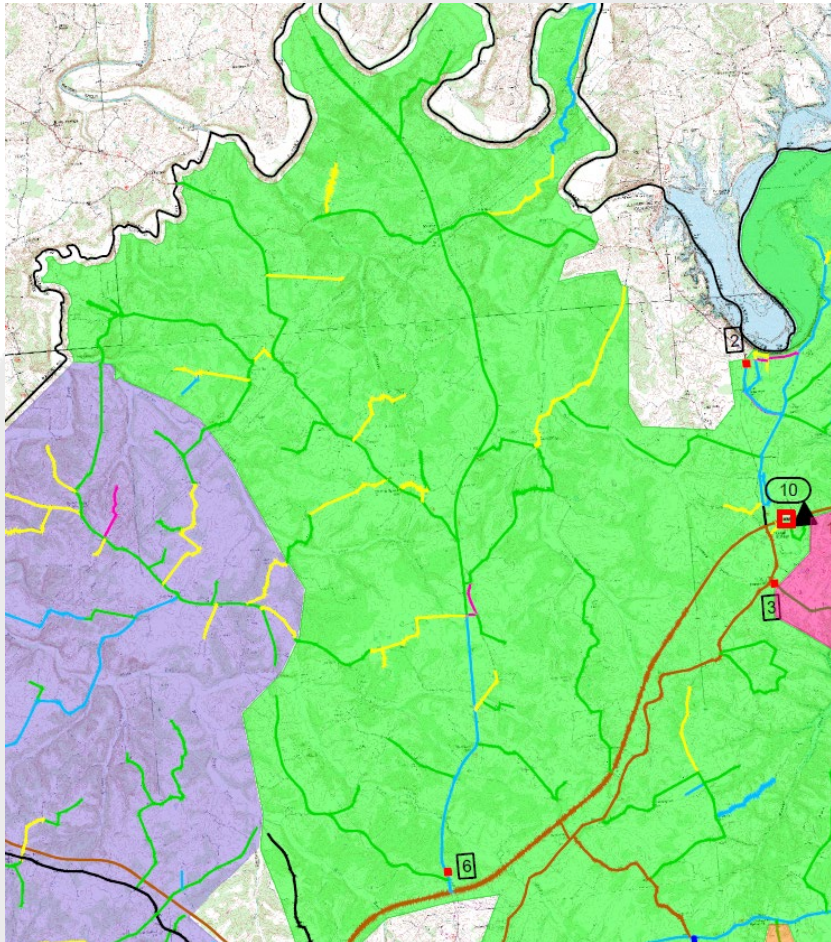
| Decade of Installation | Pipe (Linear Feet) | Percentage of Total Pipe |
|------------------------|--------------------|--------------------------|
| 1970 | 1,323,515 | 52% |
| 1980 | 518,761 | 20% |
| 1990 | 226,008 | 9% |
| 2000 | 416,289 | 16% |
| 2010 | 68,632 | 3% |

| Diameter of Pipe | Pipe (Linear Feet) | Percentage of Total Pipe Diameter |
|------------------|--------------------|-----------------------------------|
| 2-inch or less | 33,749 | 1.3% |
| 3-inch | 239,783 | 9.5% |
| 4-inch | 1,473,814 | 58.1% |
| 6-inch | 514,047 | 20.3% |
| 8-inch | 94,047 | 3.7% |
| 10-inch | 17,831 | 0.7% |
| 12-inch | 161,675 | 6.4% |



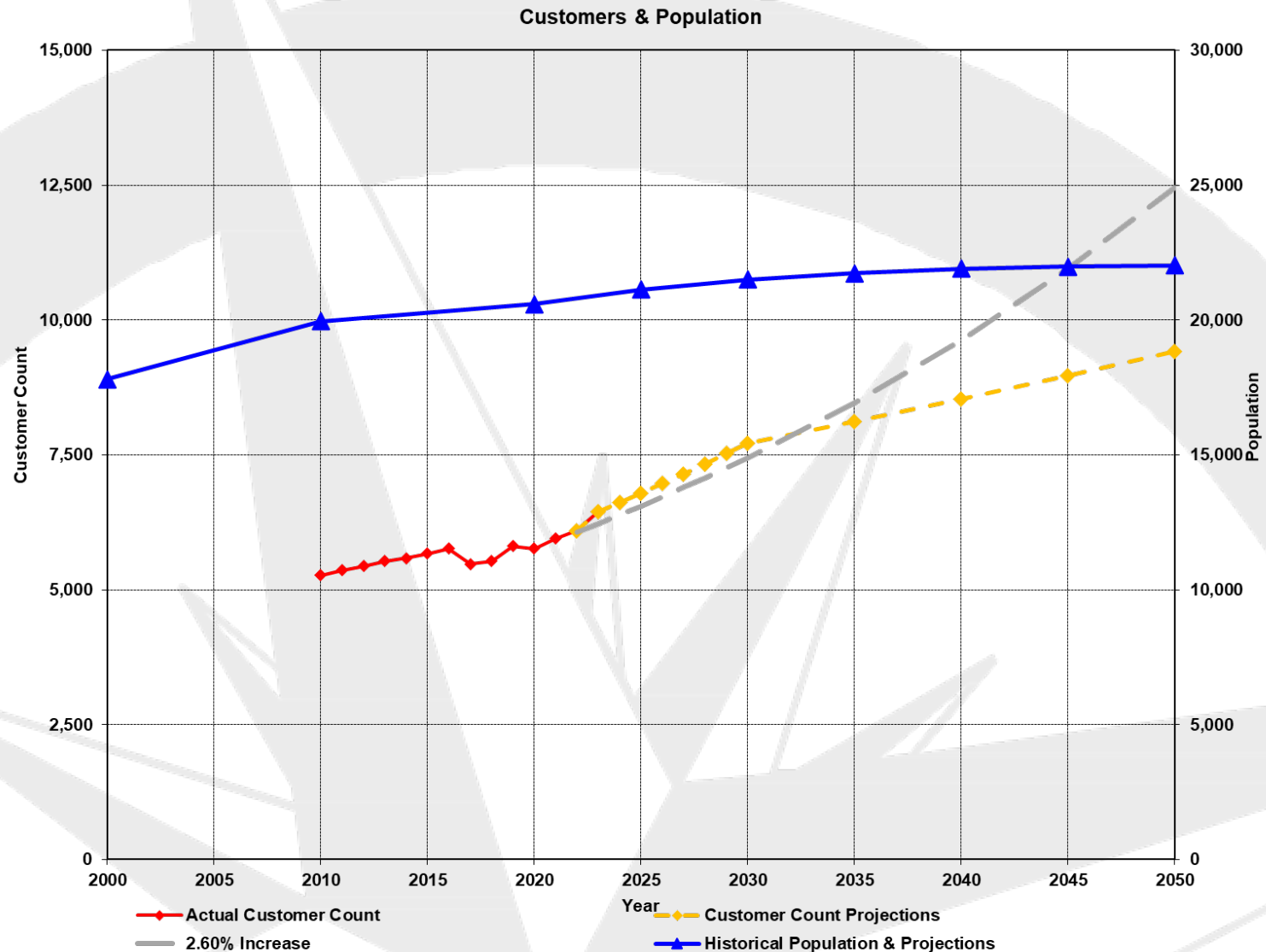
Allen County Water District

- Growth, Growth



- Historically heavy with agricultural customers
- Shifting End Users
- More customer density
- Customer Expectations
- Seasonal Customers

Allen County Water District



Allen County Water District

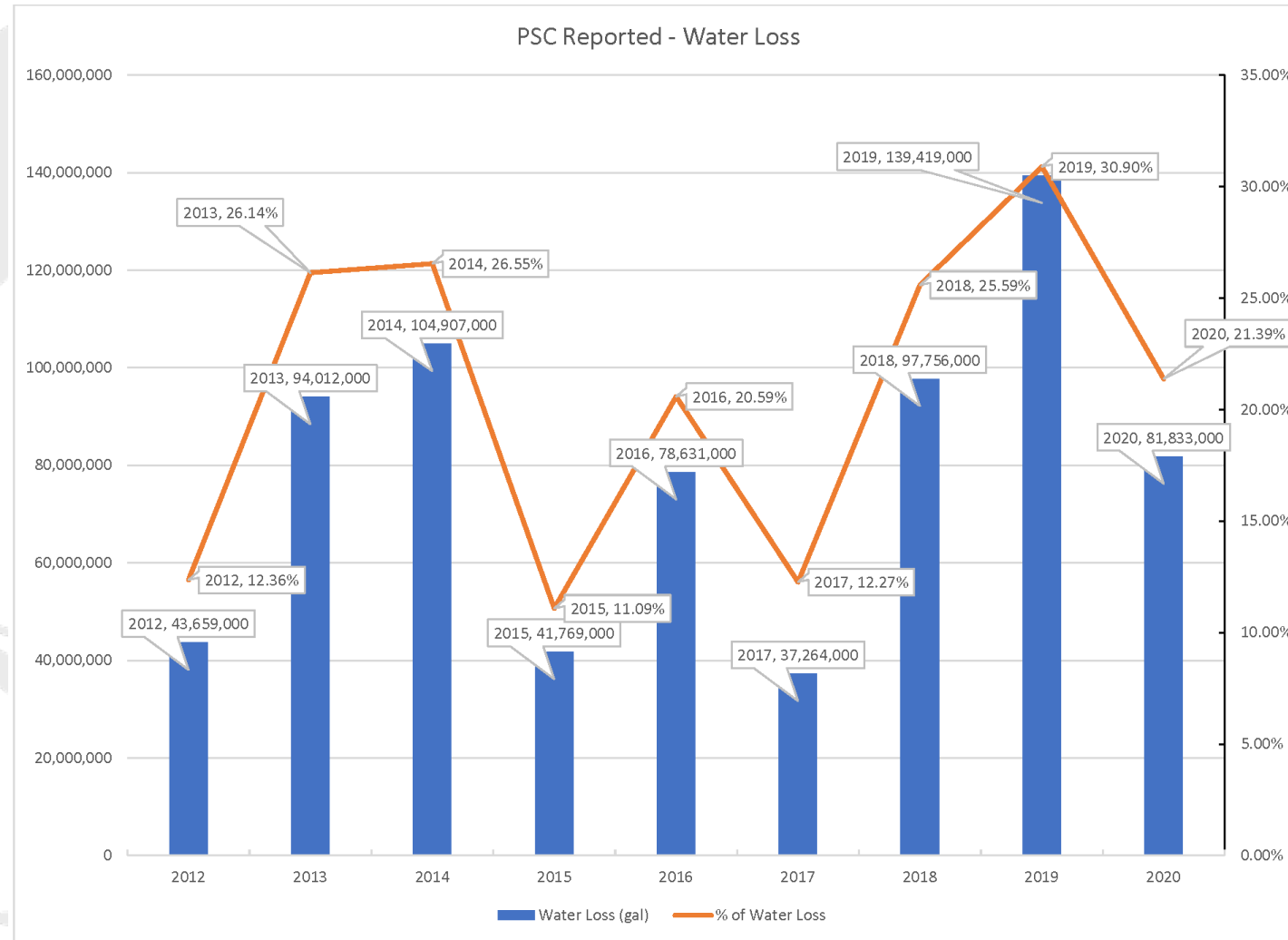
- ACWD Goals



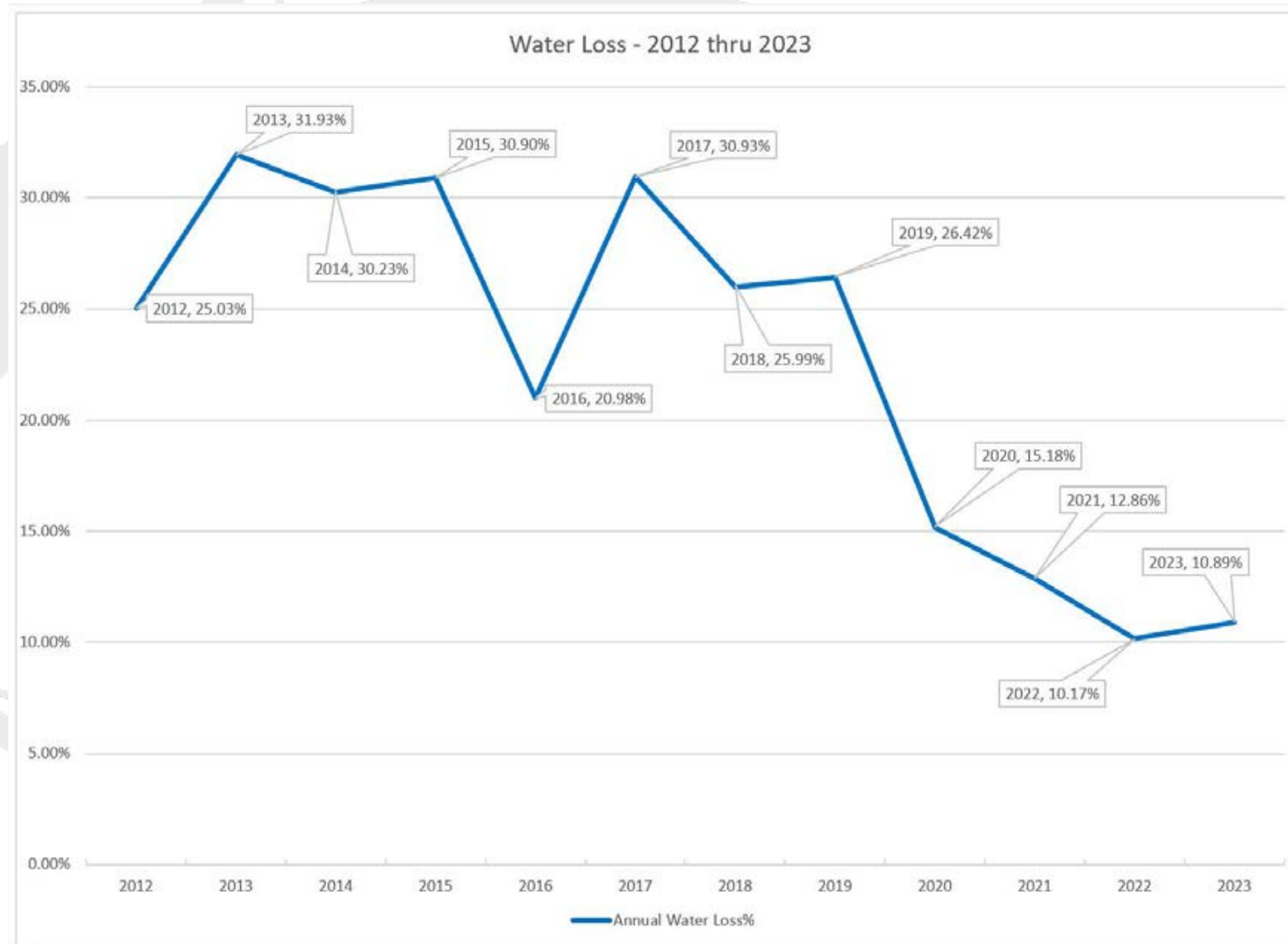
- Reduce Non-Revenue Water
- Maintain less than 15% Water Loss on a 12-month average
 - Would reduce lost revenue by \$81,000 annually
- Develop & Implement Water Loss Control Program
- Be Proactive in Finding & Removing Water Loss Sources

Allen County Water District

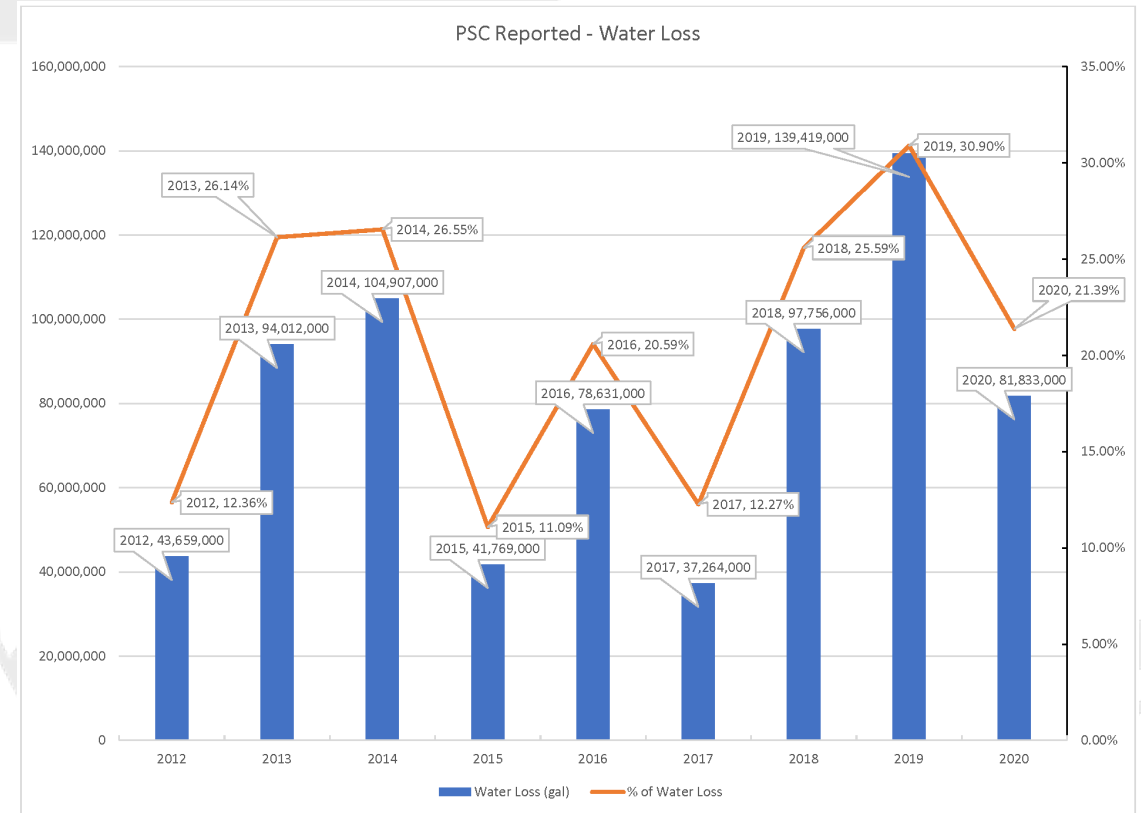
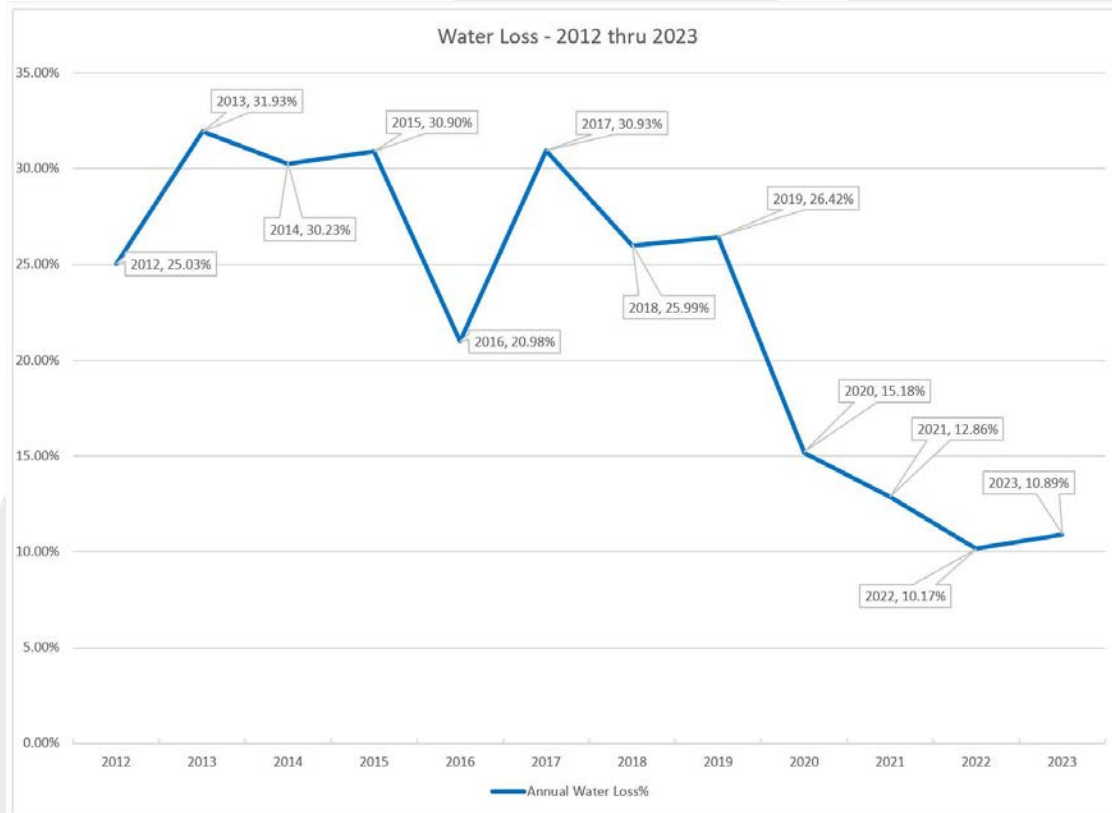
- ACWD Historic Water Loss



Allen County Water District



Allen County Water District



Allen County Water District



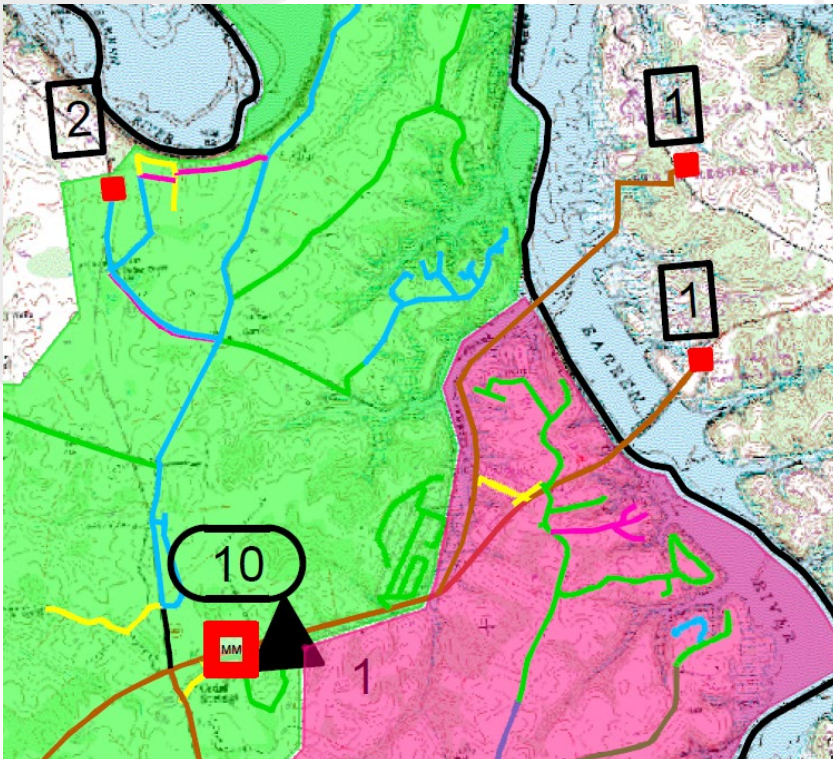
Allen County Water District

- ACWD Steps to Water Loss Reduction
 - Review of Existing Data
 - Establish Baseline
 - Improve Data Accuracy
 - Use the Data
 - Be Proactive



Allen County Water District

- Review of MORs
 - ACWD purchases water from GWC & Scottsville
 - Discrepancies between GWC & ACWD MORs
 - Discrepancies in Water Loss %



Allen County Water District

- Review of System Operations
 - Established Pressure Zone account classifications
 - Review Usage Biannually
 - Established Pressure Zone Metering Locations
 - Read Master Meters Daily
 - Established Spreadsheets for Data Entry
 - Building Historic Baseline



Allen County Water District

- Review of Data
 - Correlating Meter Readings
 - Read at different times of the month
 - GWC reads on 1st of the month
 - Scottsville reads on 20th of the month
 - ACWD reads on the 18th of the month
 - Water Loss on a 12-month rolling average



Allen County Water District

- Water Loss Control Program
 - Formalized SOPs
 - Data Collection
 - Data Monitoring
 - Trigger Limits



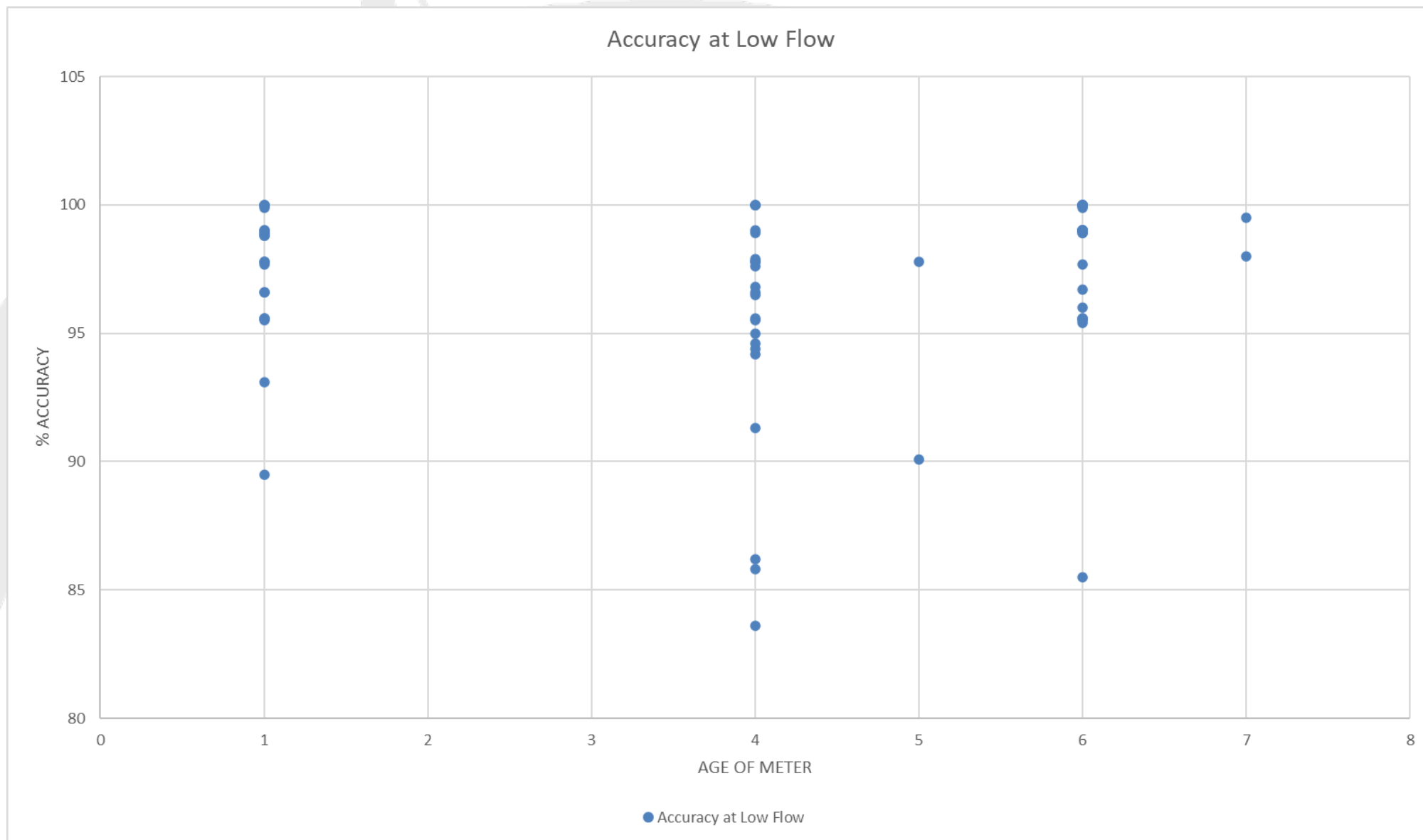
Allen County Water District

- Water Meter Accuracy Verification
 - No reads increased
 - Randomly pulled meters for testing

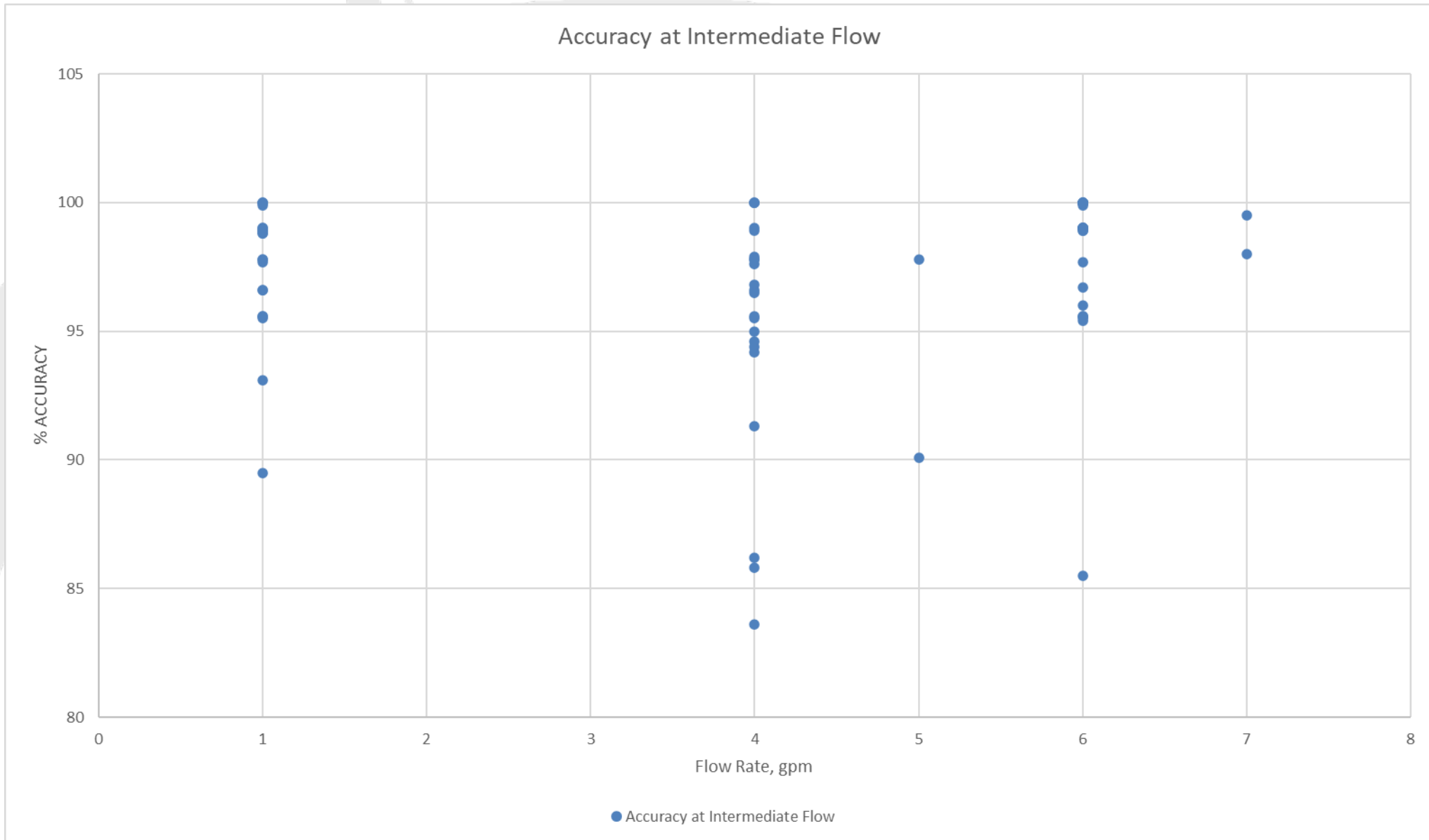
| Meter Year | Total Number of Meters | Margin of Error (%) | | |
|------------|------------------------|---------------------|--------|--------|
| | | 10 +/- | 15 +/- | 20 +/- |
| 2022 | 537 | 82 | 40 | 23 |
| 2025 | 617 | 83 | 40 | 23 |
| 2028 | | | | |
| Totals | | | | |

| Meter Age | # of Meters Tested | Low Flow (1/4 gpm) Slow/Accurate/Fast | Intermediate Flow (2 gpm) Slow/Accurate/Fast | Maximum Flow (15 gpm) Slow/Accurate/Fast |
|-----------|--------------------|--|---|---|
| 1-Year | 20 | 50%/50%/0% | 30%/70%/0% | 0%/70%/30% |
| 4-Year | 24 | 79%/21%/0% | 25%/71%/4% | 4%/79%/17% |
| 6-Year | 26 | 39%/61%/0% | 4%/88%/8% | 4%/77%/19% |

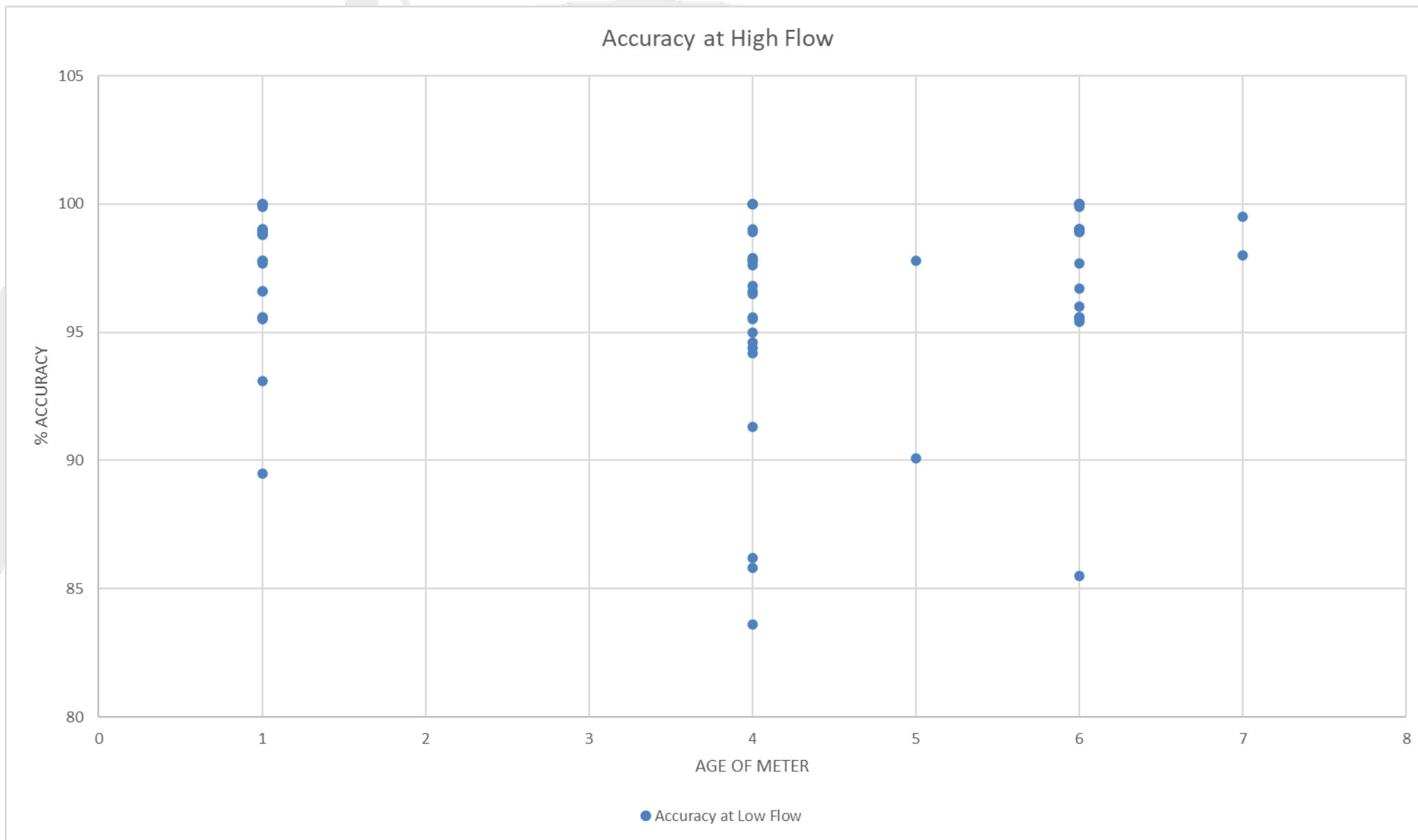
Allen County Water District



Allen County Water District



Allen County Water District



Allen County Water District

- Water Meter Selection
 - Capture low flow at the meter
 - Radio Read System
 - Losing 25 work days to manual
 - Monitoring of water usage



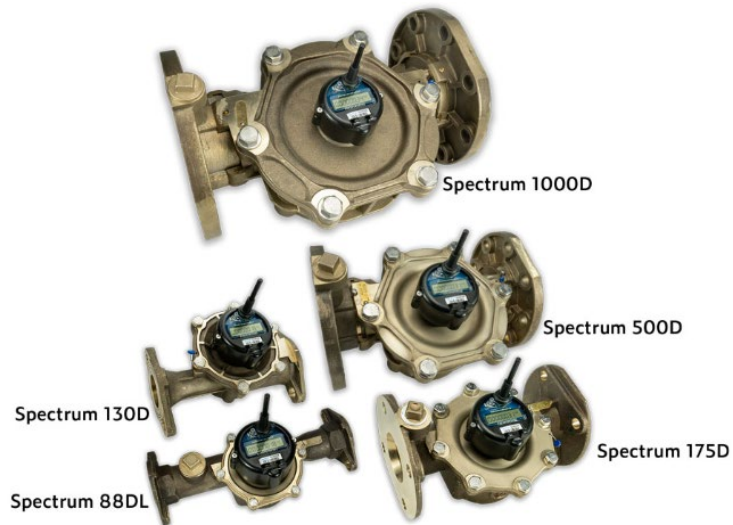
Allen County Water District

- Residential Water Meters
 - Neptune, Sensus, Badger, Diehl, Kamstrup
 - Had to capture low flow
 - Monitoring of water usage for customer relations






Allen County Water District

- Zone Master Meters
 - Utilized several different manufacturers
 - Mag Meters at Booster Stations & Isolation MM
 - e-Flowmeter (insertion flow meter) at Control Valves
 - Smart Meter Technology



Allen County Water District

| | | | | | | | |
|--|--------|--|------------------------|--|------------------------------------|---|---|
| Your Account Information | | Account Number: | Consumer Name: Hwy 252 | Address: VN ID: 4100105 | Water Budget: Wasteful | Utility Defined Type: Commercial | |
| LCD Read @02/20/2024 02:00 AM 07796755 | G x10 | Water Consumption - 02/19 to 02/20 60980 G | | So far this month 1625150 G | Daily Average 85534.21 G | The following conditions have been detected (hover on the icon for more info)   | Meter innov8-VNremote LTE Sensus 4" |
| Billing Read 779675 | Gx 100 | Read Date 02/20/2024 | | Projected Water Budget Status Wasteful | | |  |

Consumption History

Last updated Tue Feb 20 2024 15:26:07  

Time Interval 1 WEEK 

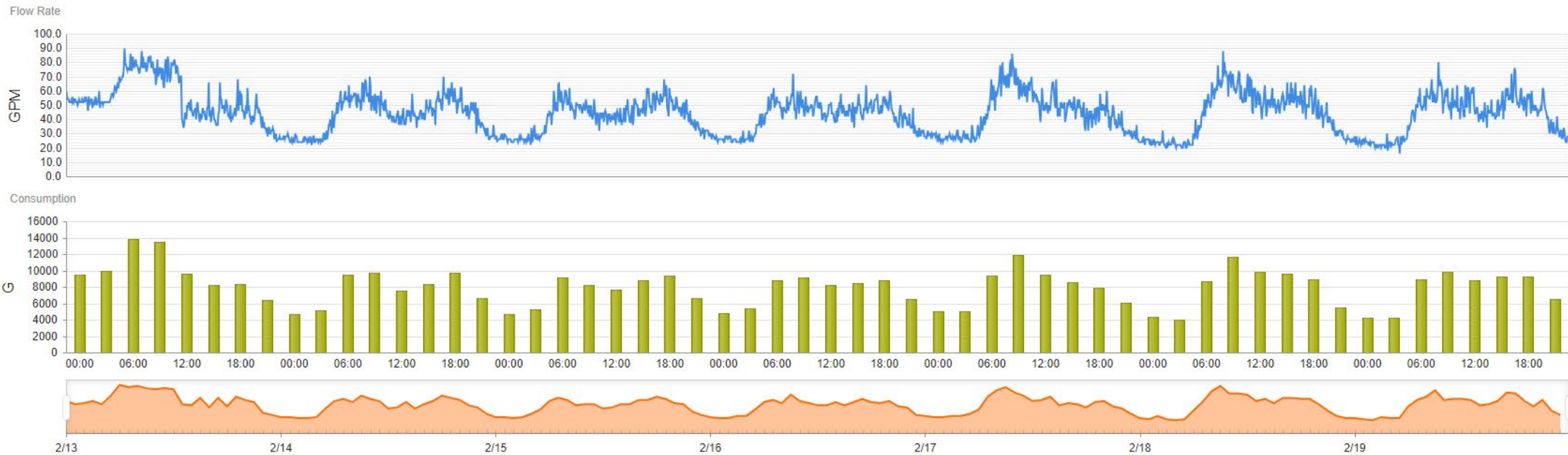
Date interval From Date 2/13/2024  To Date 2/19/2024 

Total Consumption: 447060.00 G

Export

 PDF

Displaying 13 Feb - 19 Feb  Week 



Allen County Water District

Interval

Monthly

Select Date Interval

From Date

1/21/2024

To Date

2/19/2024

Export to CSV

Go

Flowrate Statistics

Maximum Flowrate:

188 GPM at 02:55 AM on 1/23/2024

Average Flowrate:

63.023 GPM

Minimum Flowrate:

16 GPM at 05:05 AM on 2/19/2024

Consumption Statistics

Peak Hour:

5970

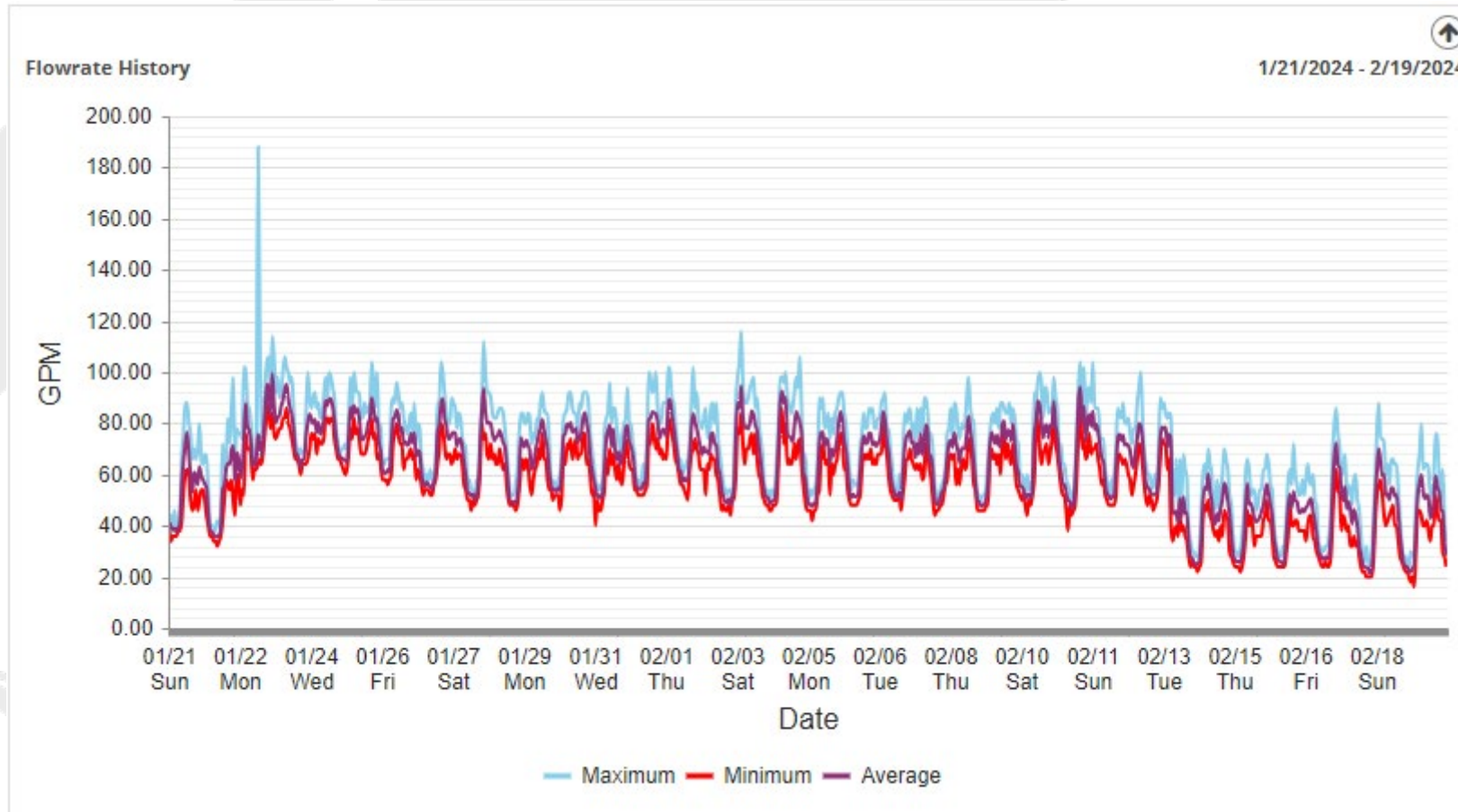
Peak Day:

118660 on 1/23/2024

Total Consumption:

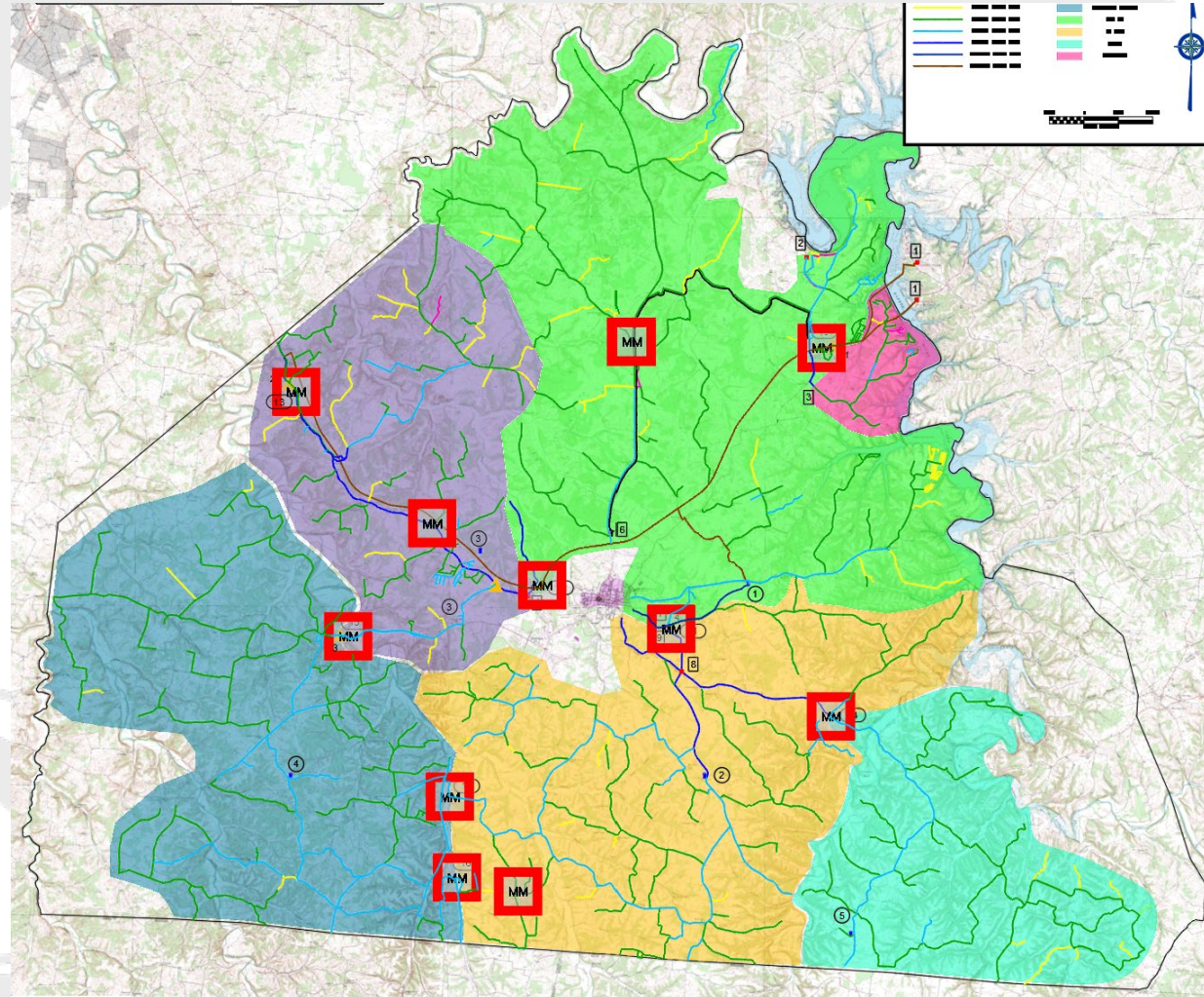
2722580

Allen County Water District



Allen County Water District

- Zone Master Meter Locations



Establishing a Baseline

- What is our water loss?
 - Real or Apparent Water Losses
- What are potential sources of real water loss?
- How can we isolate pressure zones via meters, usage & water loss?



Establishing a Baseline

- Real Water Losses
 - Water on the Ground from water mains
 - Service Connections
 - Tank Overflows
- Apparent Water Losses
 - Data Entry Errors
 - Failing Meters
 - Inaccurate Meters
 - Unauthorized Consumption
- How can we isolate pressure zones via meters, usage & water loss?



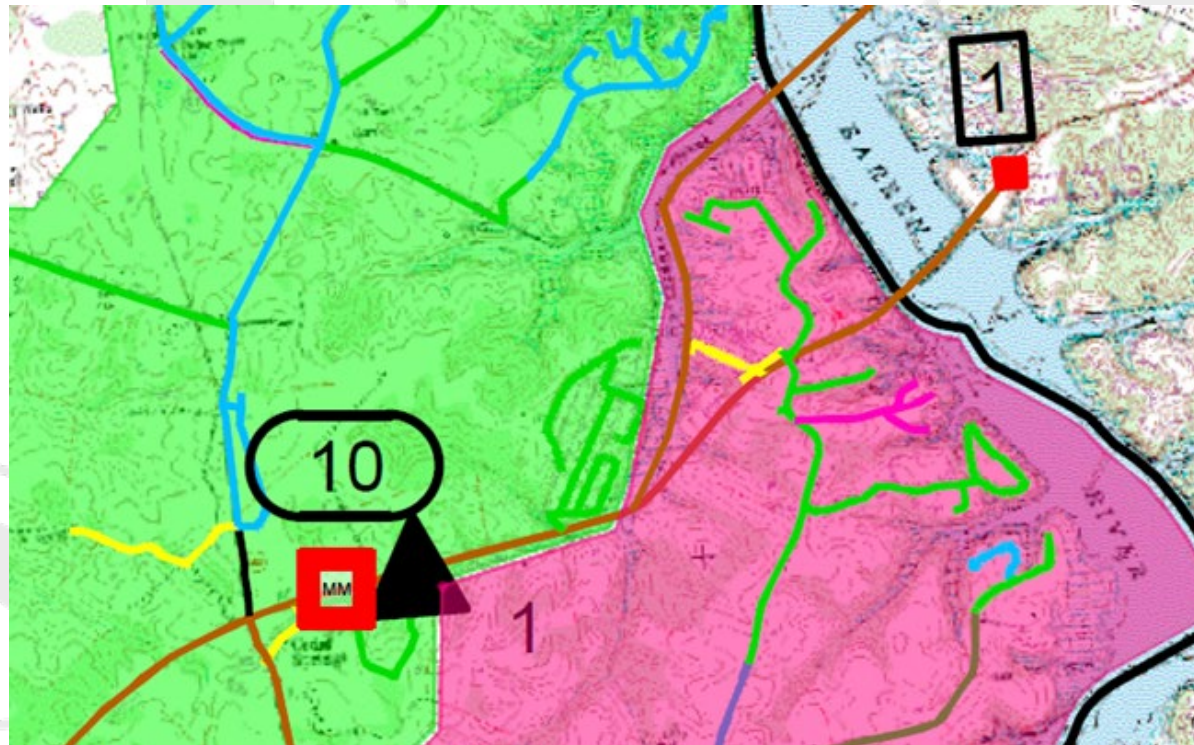
Real Water Loss

- Identifying Leaks
 - Step Down Valve Isolation
 - Daily Master Meter Readings
 - Tank Levels
 - Verifying SCADA set points
 - Pressure & Flow Monitoring



Real Water Loss

- US 31-E Emergency Water Main Repair
- Gate Valve Replacement at 31-E BPS
- Old Bowling Green Road Water Main



Apparent Water Loss

- Data Entry Errors
 - Radio Read Meters
 - Master Meter Readings
 - Downloaded Data vs hand written
- Failing/Inaccurate Meters
 - The meter is your cash register
 - Get what you pay for
 - Low Flow is water loss
- Unauthorized Consumption
 - Jumpers
 - Fire Hydrant



Improve Data Accuracy

- Smart Meter Technology
 - Radio Read Meters
 - Cellular Meters
 - SCADA
 - Fixed Net
- Monitoring High Users Meters
- Keep your Data



Use the Data

- Data Acquisition
 - Data for Data sake is a waste of time
 - Use data to determine status
 - Adjust Metrics over time
- Monitor Metrics Daily
 - Hot Spots
 - Usage Changes
- 12-Month Running Averages
 - Discrepancies in Meter Reading Schedules
 - Main line breaks happen
 - Seasonal Usages
 - More Accurate Assessment



Be Proactive

- Follow the Data Trends Not Raw Data
- Establish Responsibility for Water Loss
 - Water Loss Team
 - Attainable Water Loss %
 - Low Flow is water loss
- Success of ACWD was empowering the staff
 - Took ownership of water loss



Questions



Matthew Curtis, PE
mcurtis@bluegrassengineering.net
502.370.6551





CISA

**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

Critical Infrastructure Protection

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.



FEDERAL NETWORK
PROTECTION



PROACTIVE CYBER
PROTECTION



INFRASTRUCTURE
RESILIENCE &
FIELD OPERATIONS



EMERGENCY
COMMUNICATIONS

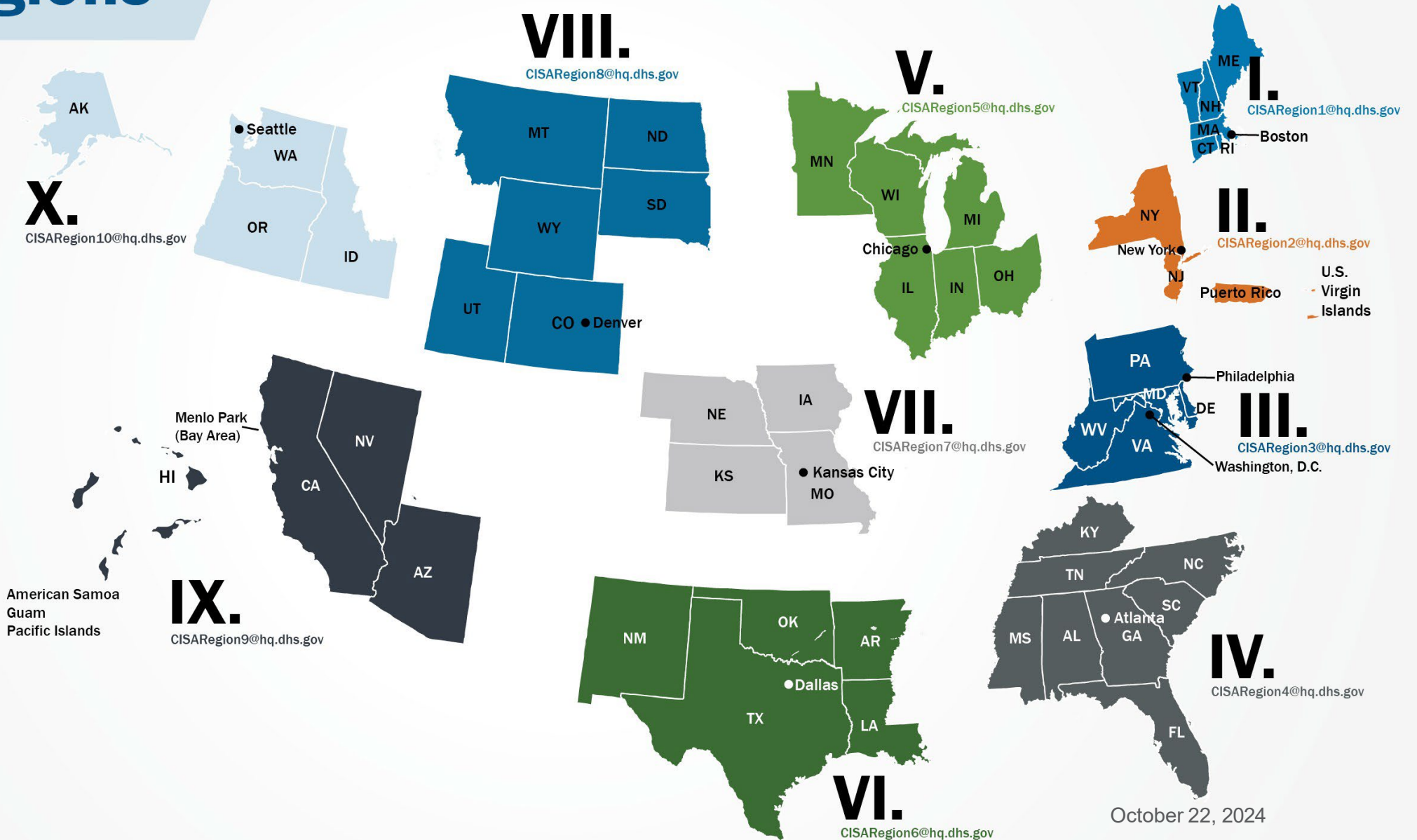


16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

| | |
|---|---|
|  CHEMICAL DHS (CISA) |  FINANCIAL Treasury |
|  COMMERCIAL FACILITIES DHS (CISA) |  FOOD & AGRICULTURE USDA & HHS |
|  COMMUNICATIONS DHS (CISA) |  GOVERNMENT FACILITIES GSA & DHS (FPS) |
|  CRITICAL MANUFACTURING DHS (CISA) |  HEALTHCARE & PUBLIC HEALTH HHS |
|  DAMS DHS (CISA) |  INFORMATION TECHNOLOGY DHS (CISA) |
|  DEFENSE INDUSTRIAL BASE DOD |  NUCLEAR REACTORS, MATERIALS AND WASTE DHS (CISA) |
|  EMERGENCY SERVICES DHS (CISA) |  TRANSPORTATIONS SYSTEMS (TSA & USCG) |
|  ENERGY DOE |  WATER EPA |

CISA Regions

- I** Boston, MA
- II** New York, NY
- III** Philadelphia, PA
- IV** Atlanta, GA
- V** Chicago, IL
- VI** Irving, TX
- VII** Kansas City, MO
- VIII** Lakewood, CO
- IX** Oakland, CA
- X** Seattle, WA
- CS** Pensacola, FL



October 22, 2024

Protective Security Advisors

- Protective Security Advisors have five mission areas that directly support the protection of critical infrastructure:
 - Plan, coordinate, and conduct security surveys and assessments
 - Plan and conduct outreach activities
 - Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events
 - World Games, 60th Anniversary of “Bloody Sunday”, Mardi Gras, Rock the South, NASCAR 500
 - Respond to incidents, provide a vital link for information sharing in steady state and incident response
 - Coordinate and support improvised explosive device awareness and risk mitigation training



CISA Priorities- Target Rich/ Cyber Poor

Healthcare - K-12 Schools - **Water/Wastewater**



Water-Wastewater Sector Toolkit

- [Water and Wastewater Cybersecurity | CISA](#)
 - Specific Alerts and Advisories for Water/Wastewater Sector
 - EPA Resources
 - **Incident Response Guide**
 - Funding Resources
 - CISA Live Events on Water/Wastewater



CYBER THREATS

Cyber Threats of Today

Business Email Compromise

- 2 Billion in Loss
- Credential Stealing
- Phishing/ PopUps/ Poison Domains/ Onsite Exchange Vulnerabilities
- Steals Data
- Finance Diversions
- SupplyChain/External Dependencies Exploitation

Ransomware

- 700K per Victim
- Ransomware-As-A-Service Brokers – Gootloader
- Phishing-As-A-Service – Greatness (M365 exploitations)
- Lockbit, Blackcat, Blacksuit, AlphV, Conti, Darkside
- Russian and North Korea State Actors
- Steals and Encrypts Data
- Double Extortion
- Destructive Malware Trends- Russia
 - Hermeticwiper and Wispergate



Denial of Service

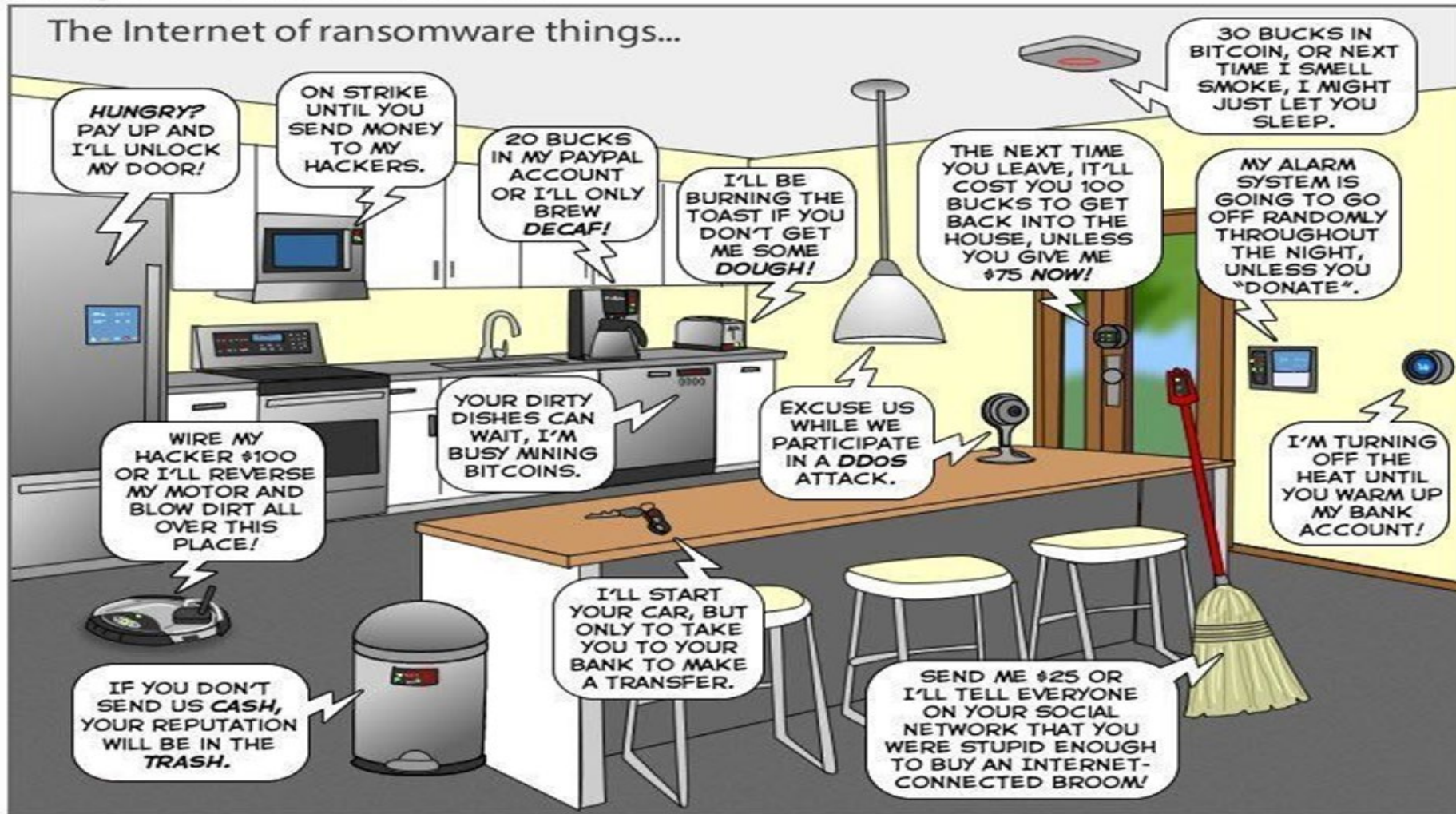
- Russian-affiliated KILLNet Group
 - Feb 2023 Coordinated DDoS of Healthcare
- Dark Storm and Anonymous Sudan
 - Russian-Affiliated
 - Aug 2023 and March 2024 Threats to CI

Common Defensive Measures

- Multifactor Authentication (MFA)
- Backups- Off Network
- Vulnerability Management – Patching
- Configuration Management - RDP, SMB, etc
- Log Management and Review

Ransomware: Infects...Encrypts...Extorts

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon.com/joyoftech

joyoftech.com

#Stop Ransomware - Resources



STOP RANSOMWARE

#STOPRANSOMWARE:
BLACKSUIT
(ROYAL) RANSOMWARE

STOP RANSOMWARE

UPDATED

Ransomware

#STOPRANSOMWARE
GUIDE

**HAVE YOU
BEEN HIT BY
RANSOMWARE?**

[LEARN MORE](#)

Protection and Response Services Public Safety Preparation

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.



Events of interest

- **Ransomware**

- Social engineering- phishing and malware
 - Gootloader- asset management important
- Ransomware notifications via phone calls and voicemails
- Encrypted a network via an IP Camera

- **Hactivists**

- Cyber Av3ngers targeting Unitronics PLCs and default passwords
- Pro-Russian targeting HMIs via VNC protocol over default port 5900

- **Volt Typhoon**

- People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.



ICS/OT Threat – CyberAv3ngers

- IRGC-Affiliated Cyber Actor
- Exploited PLCs in Multiple U.S. Critical Infrastructure Sectors (Nov-Dec 2023)
 - Water/Wastewater, Health, Food, Energy, Manufacturing
 - **Water/Wastewater primary target with 60 percent of activity**
- Targeted Israeli-made Unitronics Vision Series PLCs/ Human-Machine-Interfaces (HMI)
 - However, likely pivot to other vendors
- Most exploitations took advantage of “**Default**” **passwords (1111)** and direct
 - **exposure to the internet.**
- Group used destructive wiper malware in past



Pro-Russian Hacktivist Targeting

- Defending OT Operations Against Ongoing Pro-Russian Threats
- Joint Advisory Published May 2024
- Pro-Russian hacktivist groups ongoing activity against US and Europe
- Targeting Operational Technology (OT)/ ICS in Critical Infrastructure
- Primary Targets: Water/Wastewater, Dams, Energy, Food and Agriculture
- **Exploitations of internet-exposed ICS through their software components, such as human machine interfaces (HMIs), virtual network computing (VNC) remote access software, and PLCs.**
- Leveraging default passwords; weak passwords; lack of multi-factor



Pro-Russian Hacktivist Targeting cont..

- **Physical disruptions** from attacker remotely manipulating HMIs.
- Caused water pumps and blower equipment to exceed their normal operating parameters.
- Maxed out set points, altered other settings (Ladder Diagram Logic), turned off alarm mechanisms, and changed administrative passwords to lock out the WWS operators.
- Some victims experienced minor tank overflow events; however, most victims **reverted to manual controls** in the immediate aftermath and quickly restored operations.



Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Published 13 Dec 24

Threat actors can exploit exposed HMIs at WWS Sector utilities to view the contents of the HMI, make unauthorized changes, and potentially disrupt the facility's water and/or wastewater treatment process.

In the absence of cybersecurity controls, unauthorized users can exploit exposed HMIs in Water and Wastewater Systems to:

- **View the contents of the HMI (including the graphical user interface, distribution system maps, event logs, and security settings) and**
- **Make unauthorized changes and potentially disrupt the facility's water and/or wastewater treatment process.**

[Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems | CISA](#)



Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

In 2024, pro-Russia hackers manipulated HMIs at Water and Wastewater Systems, causing water pumps and blower equipment to exceed their normal operating parameters. In each case, the hackers maxed out set points, altered other settings, turned off alarm mechanisms, and changed administrative passwords to lock out the water utility operators. These instances resulted in operational impacts at water systems and forced victims to revert to manual operations.

Defending OT Operations Against Ongoing Pro-Russia Hacker Activity



Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Mitigations

- Conduct an inventory of all internet-exposed devices.
- If possible, disconnect HMIs and all other accessible and unprotected systems from the public-facing internet.
- If it is not possible to disconnect the device, secure it by creating a username and strong password to prevent a threat actor from easily viewing and accessing the devices. Change factory default passwords.
- Implement a strong password and multifactor authentication (MFA) for all access to the HMI and OT network.
- Implement network segmentation by enabling a demilitarized zone (DMZ) or a bastion host at the OT network boundary.
- Implement geo-fencing across the entire network and enforce network segmentation based on specific locations.

Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity



Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

Mitigations

- Keep all systems and software up to date with patches and necessary security updates.
- Establish an allowlist that permits only authorized IP addresses to access the devices.
- Log remote logins to HMIs; be aware of failed attempts and unusual times.
- Implement your vendor's recommendations for best securing your product.
- Sign up for CISA's free cybersecurity vulnerability scanning service to identify software vulnerabilities and confirm that patching is up to date and done correctly.

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity



Volt Typhoon

- Chinese state-sponsored threat actor using stealth techniques and targeted malicious activity aimed at critical infrastructure organizations in the United States
- Observed behavior suggests that the threat actor goal to maintain access without being detected for as long as possible
- Volt Typhoon pursues capabilities to **disrupt critical infrastructure during future crises**
- Affected Sectors Include:
 - Communications
 - Manufacturing
 - Utility
 - Construction
 - Maritime
 - Government
 - Education
 - Transportation
 - Information technology



[CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance | CISA](#)

[Volt Typhoon: Hiding in Plain Sight - Critical Start](#)

[Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog](#)

Living Off the Land (LOTL)

- Sophisticated cyberattack technique that leverages legitimate tools **already present within a victim's system** to execute and sustain an attack
 - Bypasses traditional signature-based defenses (Behavioral Vs. Signature Analysis is key)
 - Windows Management Instrumentation
 - **PowerShell**
 - **Scheduled Tasks Actions**
 - **C2- Home User Networks**
 - FTP, SMB, and SSH
 - Log Deletion (Event 1102)

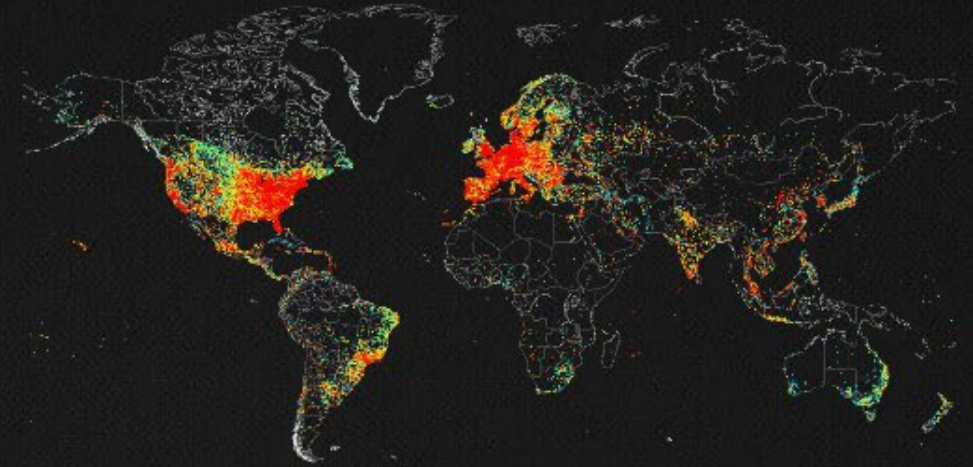




Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.


SIGN UP NOW



Shodan (www.shodan.io) is a web-based search platform for Internet connected devices. This tool can be used not only to identify Internet connected computers and Internet of Things/Industrial Internet of Things (IoT/IIoT), but also Internet connected Industrial Control Systems (ICS) and platforms.



RDP Search-KY


 SHODAN

Explore

Downloads

Pricing [↗](#)

state:ky port:3389



TOTAL RESULTS

512

TOP ORGANIZATIONS

| | |
|---------------------------------------|-----|
| Charter Communications Inc | 170 |
| AT&T Enterprises, LLC | 47 |
| CINCINNATI BELL | 25 |
| Private Customer - AT&T Internet S... | 16 |
| AT&T Services, Inc. | 14 |

[More...](#)

TOP OPERATING SYSTEMS


| | |
|---------------------------------------|-----|
| Windows (build 10.0.19041) | 169 |
| Windows 11 (build 10.0.26100) | 70 |
| Windows 11 (version 22H2) (build 1... | 49 |
| Windows (build 10.0.14393) | 41 |
| Windows Server 2022 (build 10.0.20... | 41 |

[More...](#)

[View Report](#) [Download Results](#) [Historical Trend](#) [Browse Images](#) [View on Map](#) [A](#)

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you ha](#)



 United States, Elizabethtown


self-signed

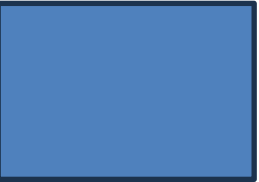
SSL Certificate


Issued By:
|- Common Name:
Server2019.monroepva.local

Issued To:
|- Common Name:
Server2019.monroepva.local

Supported SSL Versions:
TLSv1, TLSv1.1,
TLSv1.2

Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\
Remote Desktop Protocol NTLM Info:
OS: Windows 10 (version 1809)/Windows Server 2019 (version 1
OS Build: 10.0.17763
NetBIOS 
NetBIOS Comput...



 United States, Bowling Green

self-signed

SSL Certificate

Issued By:
|- Common Name:
Igor-PC

Issued To:
|- Common Name:
Igor-PC

Supported SSL Versions:
TI Sv1 TI Sv1 1

Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\
Remote Desktop Protocol NTLM Info:
OS: Windows 10 (version 2004)/Windows Server (version 2004)
OS Build: 10.0.19041
Target Name: IGOR-PC
NetBIOS Domain Name: IGOR-PC
NetBIOS Computer Name: ...



RDP Search

state:ky port:3389

os



// TOTAL: 512



| | | |
|--|-----|-------------|
| Windows (build 10.0.19041) | 169 | <div></div> |
| Windows 11 (build 10.0.26100) | 70 | <div></div> |
| Windows 11 (version 22H2) (build 10.0.22000) | 49 | <div></div> |
| Windows (build 10.0.14393) | 41 | <div></div> |
| Windows Server 2022 (build 10.0.20348) | 41 | <div></div> |
| Windows (build 10.0.17763) | 38 | <div></div> |
| Windows Server 2012 R2 | 17 | <div></div> |
| Windows (build 6.3.9600) | 11 | <div></div> |
| Windows (build 6.1.7601) | 7 | <div></div> |
| Windows 11 (version 21H2) (build 10.0.22000) | 4 | <div></div> |
| Windows (build 6.2.9200) | 2 | <div></div> |
| Windows Server 2008 R2 Standard | 2 | <div></div> |
| Windows Server 2008 Standard | 2 | <div></div> |
| Windows (build 10.0.18362) | 1 | <div></div> |
| Windows 11 (build 10.0.25110) | 1 | <div></div> |
| Windows 7 Professional | 1 | <div></div> |
| Windows Server 2008 R2 Enterprise | 1 | <div></div> |



ICS Screenshot Search - Worldwide

TOTAL RESULTS

437

TOP COUNTRIES



| | |
|---------------|-----|
| United States | 101 |
| Germany | 54 |
| Italy | 27 |
| Poland | 24 |
| China | 21 |

[More...](#)

TOP PORTS

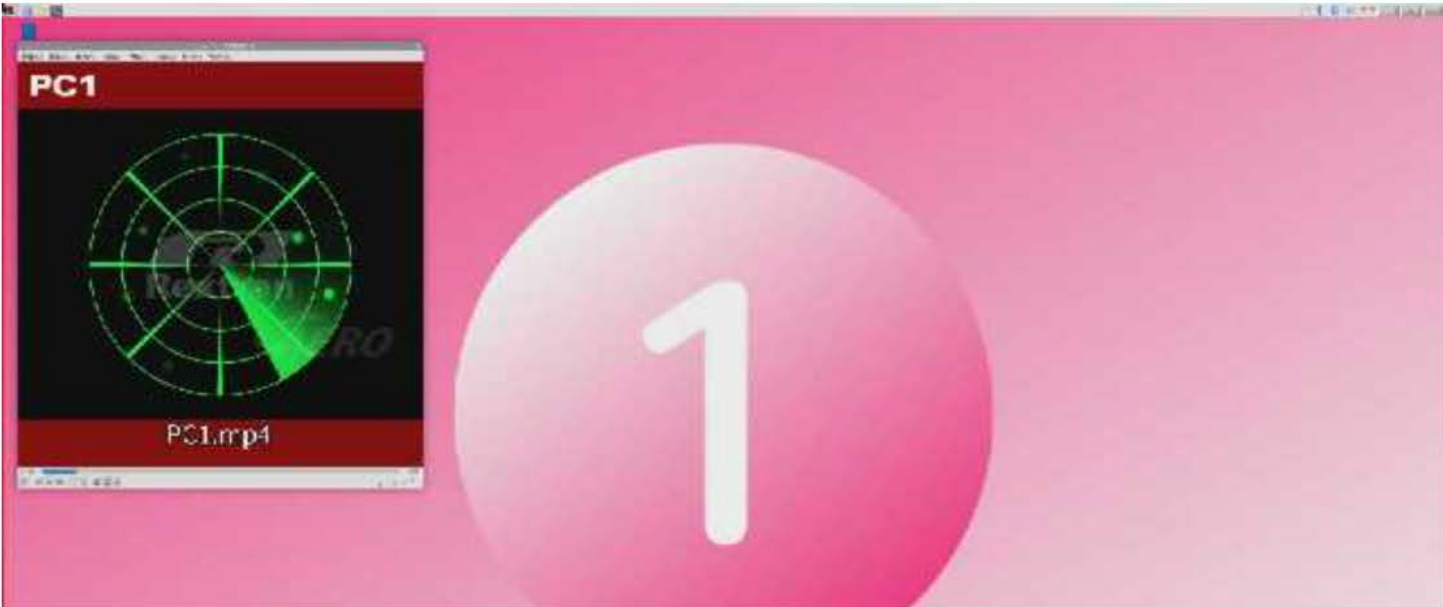
| | |
|------|-----|
| 5900 | 145 |
| 80 | 58 |
| 3389 | 42 |
| 5901 | 15 |
| 6590 | 15 |

[More...](#)

[View Report](#) [Download Results](#) [Historical Trend](#) [Browse Images](#) [View on Map](#) [Advanced Search](#)

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

2025-03-06T19:57:48.042761



PLC Search: KY

 SHODAN

Explore

Downloads

Pricing [↗](#)

state:ky "allen bradley"



TOTAL RESULTS

48

TOP PORTS

| | |
|-------|----|
| 44818 | 46 |
| 161 | 1 |






TOP ORGANIZATIONS

| | |
|--|----|
| Wireless Data Service Provider Corporat... | 26 |
| AT&T Mobility LLC | 10 |
| Charter Communications Inc | 3 |
| NORTH CENTRAL TELEPHONE COOPER... | 3 |
| Limestone Cable Vision, Inc. | 1 |

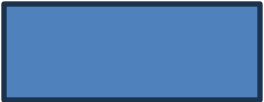
[More...](#)


TOP PRODUCTS

| | |
|---|----|
| Rockwell Automation/Allen-Bradley | 31 |
| Schweizerische Bankgesellschaft Zuerich | 1 |

 View Report  Download Results  Historical Trend  View on Map  Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)




Mayfield Electric & Water
Systems
 United States, Mayfield

ics

Product name: 1766-L32BWAA B/15.04
Vendor ID: Rockwell Automation/**Allen-Bradley**
Serial number: 0x4064ffba
Device type: Programmable Logic Controller
Device IP: 192.168.10.199




South Central Rural
Telecommunications
Cooperative Inc.
 United States, Horse
Cave

ics

Product name: 1766-L32AWAA B/13.00
Vendor ID: Rockwell Automation/**Allen-Bradley**
Serial number: 0x4062325e
Device type: Programmable Logic Controller
Device IP: 192.168.100.50



 United States, Murray

Product name: 1766-L32AWA C/21.02
Vendor ID: Rockwell Automation/**Allen-Bradley**
Serial number: 0x60e4d95f
Device type: Programmable Logic Controller
Device IP: 10.5.10.31



Specific SCADA Search: KY

TOTAL RESULTS

11

TOP ORGANIZATIONS



View Report



Download Results



Historical Trend



View on Map




Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)


Document Moved



HTTP/1.1 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: scadaweb.net/system.php
Server: Microsoft-IIS/10.0
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frames-Options: DENY
X-Content-...


Document Moved



HTTP/1.1 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: scadaweb.net/system.php
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frames-Op...

Document Moved




HTTP/1.1 302 Redirect
Content-Type: text/html; charset=UTF-8
Location: scadaweb.net/system.php
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-XSS-Protection: 1; mode=block



Open Vulnerabilities

// LAST SEEN: 2025-03-06

 General Information

Hostnames

Domains

SPECTRUM.COM

Country

United States

City

Louisville

Organization


Charter Communications Inc

ISP

Charter Communications Inc

ASN


AS10796

 Vulnerabilities

Port 22

CVSS


Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

 Critical (2)

CVE-2023-38408

9.8

The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system (Code in /usr/lib is not

 Open Ports

22

8080

// 22 / TCP -1169060451 | 2025-03-05T03:10:02.484054

OpenSSH 7.3

SSH-2.0-OpenSSH_7.3

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQCoUG08gCEJ3USWDXpaa/jjEJwX/ayY3ShTvX7HgCodGAz4n1nz+pdanKNfaDwKwmNDAnruHuyc7paJMCaHHGznxT25NwqJzWentm6+UZH0cdbamjaKn84I/40EH+vCk4TVb8lIHKexNoY0LM1P7FialPkbh9Ekx1KMdWP+r3o0pdQz+q2LIc9sYIBYyYag6f6wFZcncnH76+HF1IVum0lLsn7G4++8swhVYkc4HwV05ay4uInAyGLY3iukbjQ5YXdlsyrX7Zw1Jia5GZupukwTAs733HEYUHSZ+8A1dRAYuKRtU69niwrX1oKrNej1PtEIay0M7gDVcNpNJH5q+Fz

Fingerprint: 58:3e:96:30:e7:1d:a9:66:ba:f4:1d:d1:2a:19:1e:75

Kex Algorithms:

curve25519-sha256@libssh.org

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group16-sha512

diffie-hellman-group18-sha512

diffie-hellman-group14-sha256

diffie-hellman-group14-sha1

Server Host Key Algorithms:

ssh-rsa

rsa-sha2-512

rsa-sha2-256

...

34

Stuff Off Search

| Shodan | Censys | Thingful |
|--|---|---|
| <p>Shodan is a web-based search platform for internet connected devices.</p> <p>Key features:</p> <ul style="list-style-type: none">• Identify Internet connected devices, Internet of Things/IIoT), and industrial control systems (ICS).• Potential exploits.• Default passwords.• Integrations with vulnerability tools, logging aggregators and ticketing systems allow Shodan to be seamlessly integrated into an enterprise. <p>https://www.shodan.io</p> | <p>Censys is a web-based risk management tool that helps identify publicly accessible assets —even if they can't be scanned by a vulnerability management tool.</p> <p>Key features:</p> <ul style="list-style-type: none">• Home network risk identifier (HNRI), allowing employers to anonymously monitor staff's home network infrastructure for vulnerabilities that may pose a risk to the company.• Exposed routers.• Default credentials.• Popular vectors for ransomware. <p>https://www.censys.io</p> | <p>Thingful is a search engine for the Internet of Things (IoT).</p> <p>Key features:</p> <ul style="list-style-type: none">• Searchable index of public and private connected objects and sensors around the world.• Monitors IoT networks and infrastructures including energy, radiation, weather, and air quality devices.• Reports seismographs, iBeacons, vehicles, ships, aircraft and animal trackers. The tool assists with response by enabling end users to create watchlists and publications on public/private IoT resources. <p>https://www.thingful.net/</p> |



Operational Technology (OT) Vulnerabilities

- Building Automation Systems (BAS) BACNet Field Panels (BFP)
 - HVAC Systems Control- elevators, lighting, emergency services, sensors, access control, etc.
- Utility PLCs (programmable logic controllers) and Human Machine Interface (HMI)
- Camera Systems
- Specialty Equipment (Vender Maintained)
- Diagnostic Systems - CT, Ultrasound, MRI, Imaging etc.
 - Picture Archiving Communication System (PACS) network
 - Digital Imaging and Communications in Medicine (DICOM) format
- Medical Devices – Infusion pumps, patient monitors



CISA ICS No-Cost Virtual Training

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

<https://www.cisa.gov/ics-training-available-through-cisa>



Steps to take to be a bit more secure





[Teach Employees to Avoid Phishing](#)



[Require Strong Passwords](#)



[Require Multifactor Authentication](#)



[Update Business Software](#)



[Secure Our World | CISA](#)

Phishing

- Phishing - online messages designed to look like they're from a trusted source and/or hijack legitimate accounts intended to lure target to: click a link, open an attachment, or take an action.

- **Common Red Flags:**

- Urgent/ Emotionally Charged
- Requests to Send or Change Personal/ Finance Info
- Unexpected/ Suspicious Attachments (uncommon naming/ file types)
- Untrusted/Suspicious Links (URL mismatches)
- Email Addresses Do Not Match Sender
- Official Emails Originating from Outside Company
- Too Good To Be True



- **Mitigation:**

- Resist and Report
 - Spam – Organization
 - Blocks Current Sender
- Delete
 - Avoid Unsubscribe Link
 - Could Be Malicious

Password Defense

1

Make them long

At least 16 characters—longer is stronger!

2

Make them random

Two ways to do this are:

Use a random string of letters (capitals and lower case), numbers and symbols (the strongest!):

cXmnZK65rf*&DaaD

Create a memorable passphrase of 5–7 unrelated words:

HorsPerpleHatRunBayconShoos



Get creative with spelling to make it even stronger.



3

Make them unique

Use a different password for each account:

k8dfh8c@Pfv0gB2

LmvF%swVR56s2mW

e246gs%mFs#3tv6

Tip!

Use a password manager to remember them.

Multifactor Authentication (MFA)

- MFA (two-factor): Confirms Our Identities.
- Highly Impactful Defense Against Cyber Attacks.
- Enable on EVERY account and Device possible.



Email



Banking



Social Media



**Online
Purchases**



Identities



Multifactor Authentication



Software Updates

- Install Updates to fix Security Risks.
 - Mobile Phones, Computers/ Tablets, Operating Systems, Software, Web Browsers, Watches, **Network and Security Equipment, IoT**
- Time is Critical once Vulnerabilities are known.
- Turn on Automatic Updates
- Watch for Notifiers – Not every update can be automatically installed

Automatic Updates



Home Network Security

Webcam

- Cover cameras when not in use.



Web Browser

- Ensure transit security encryption, usually with a lock icon in the address bar.



External Storage

- Back up data on external drives or portable media.



ISP Router Management

- Change Default Password
- Enable Firewall
- Enable Network Address Translation (NAT)



Wireless Access Point/Router

- Use WPA3 or WPA2/3 with protected management frames.
- Update with the latest patches, preferably through automatic updates.
- Schedule weekly reboots.



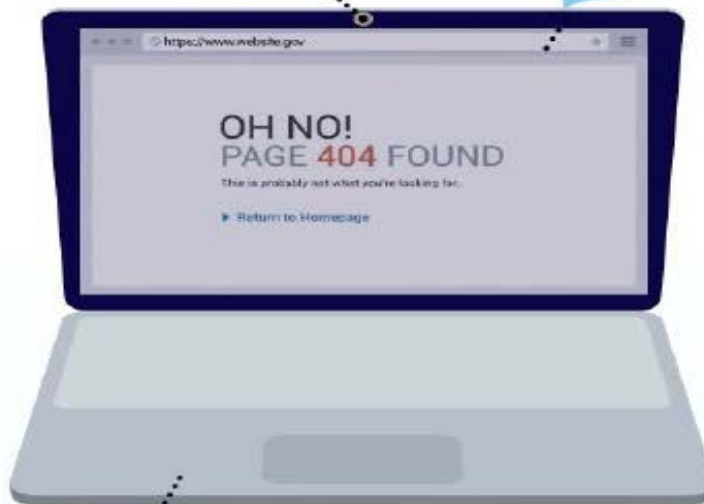
Home Assistance

- Limit nearby sensitive conversations.
- Mute microphones when not in use.



Laptop/Computer

- Utilize a non-privileged "user" account for everyday activities.
- Update with the latest patches, preferably through automatic updates.



[NSA-Best Practices For Securing Your Home Network](#)

Change Default Password - - - Restart Often

Mobile Device Security

- Enable User Authentication (Passcode)
- Install Updates
- Restart Phone Often (Memory Dump)
- Create backups
- Reinstall From backups Occasionally (After Foreign Travel or Loss of Control)
- Only Download Apps from Legitimate Sources
- Limit Remote Sharing
- Limit Public Exposure
- Change Device Name



CISA Services



Cybersecurity Resources

Partnership Development

- Outreach Activities
- Informational Exchanges (individual, group, etc.)
- Committees and Working Groups support
- Symposiums/ Conferences/ Webinars/ Cyber Camps

Stakeholder Preparedness

- Cybersecurity Workshops
- Technical Exchange
- Introductory Visits and Cyber Protective Visits (CPVs)
- [Cyber Exercises support/ Tabletop Exercises](#)
- [Awareness and Cyber Threat Training/ Briefings](#)

Assessments

- [Cybersecurity Performance Goals assessments \(CPGs\)](#)
- Ransomware Readiness Assessments (RRAs)
- Cyber Resilience Reviews (CRRs)
- External Dependency Management Assessments (EDMs)

Vulnerability Scanning

- [Cyber Hygiene Service \(Public Attack Surface\)](#)
 - [Known Exploitable Vulnerabilities \(KEV\)](#)
- Web Application Scanning
- Penetration Testing



Ransomware Vulnerability Warning Pilot (RVWP)

A new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors.

- Leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks.

- CISA's Cyber Hygiene Vulnerability Scanning
- Known threat vectors
- Administrative Subpoena Authority
- Homeland Security Act of 2002



Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
 - Public release under Freedom of Information Act requests,
 - Public release under State, local, tribal, or territorial disclosure laws,
 - Use in civil litigation and
 - Use in regulatory purposes.



Vulnerability Scanning by CISA (Cyber Hygiene)

Known exploited vulnerabilities are easy access for attackers, with incidents averaging \$100,000 in damages for small and medium businesses.



CISA's [free](#) vulnerability scanning service helps [identify exposed assets and exploitable vulnerabilities](#) and is proven to reduce risk for participating organizations.

[Avoid costly disruptions](#) with early detection and action. Through weekly reports and timely alerts, we will help you [act before others take advantage](#).

Auto enrollment with CISA [Ransomware Vulnerability Warning](#)



BY THE NUMBERS

- 7,200+ current customers nationwide
- Over 3 Million vulnerabilities found and fixed
- On average a 40% reduction in risk and exposure by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first 90 days

GETTING STARTED

Email vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

Vulnerability Scanning Report

High Level Findings

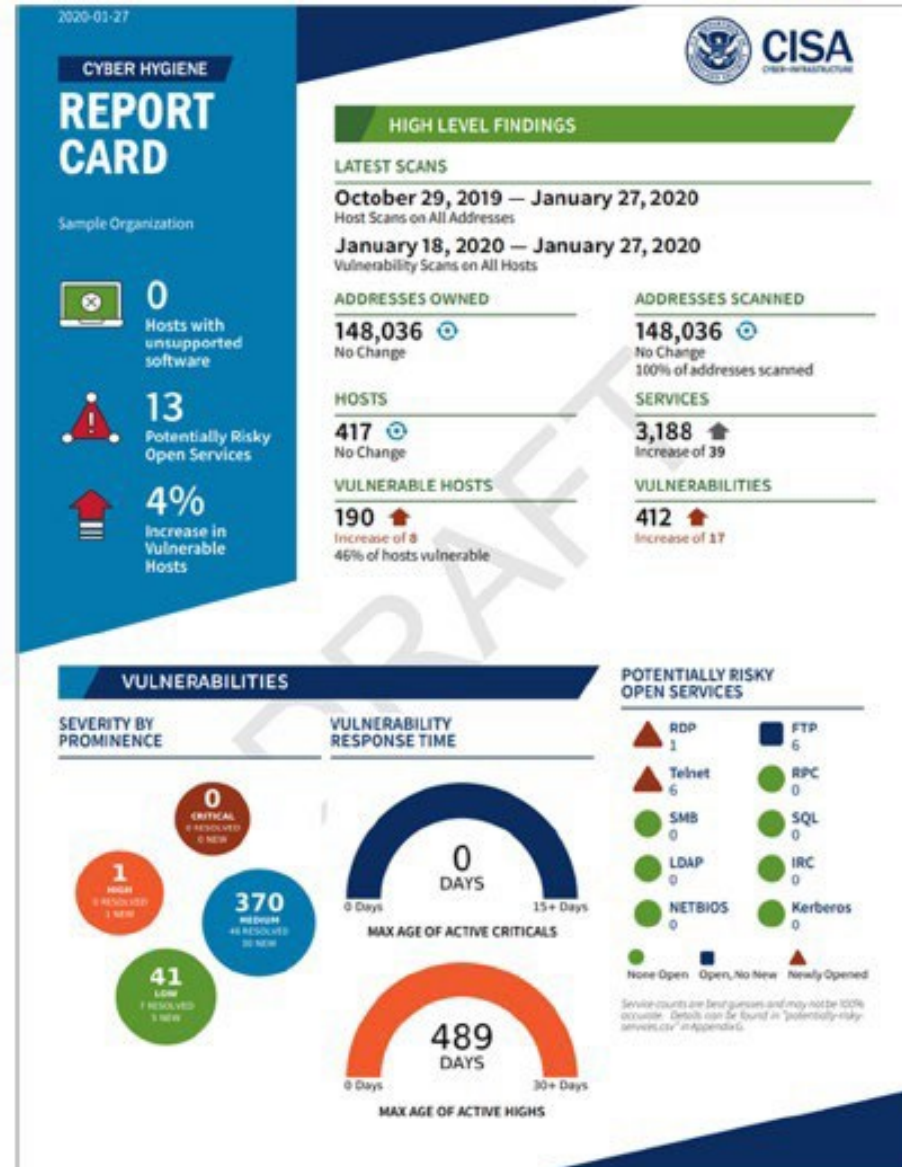
- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



Dashboard Coming Soon



Cyber Performance Goals (CPG)

- A common baseline of cybersecurity practices that all critical infrastructure entities should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.
- IT and operational technology (OT) cybersecurity practices that meaningfully reduce the likelihood and impact of known risks and adversary techniques
- Informed by real-world threats and adversary tactics, techniques, and procedures (TTPs)
- Aids in identifying areas for potential future investment



| 1.A Asset Inventory | ID.AM-1 | CURRENT ASSESSMENT |
|--|---------|--------------------------------------|
| COST: \$\$\$\$ IMPACT: HIGH COMPLEXITY: MEDIUM | | <input type="checkbox"/> IMPLEMENTED |
| TTP or Risk Addressed <ul style="list-style-type: none">• Hardware Additions (T1200)• Exploit Public-Facing Application (T0819, ICS T0819)• Internet Accessible Device (ICS T0883) | | <input type="checkbox"/> IN PROGRESS |
| Recommended Action <p>Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.</p> | | <input type="checkbox"/> SCOPED |
| | | <input type="checkbox"/> NOT STARTED |

CPG Effectiveness – Cyber Hygiene Service

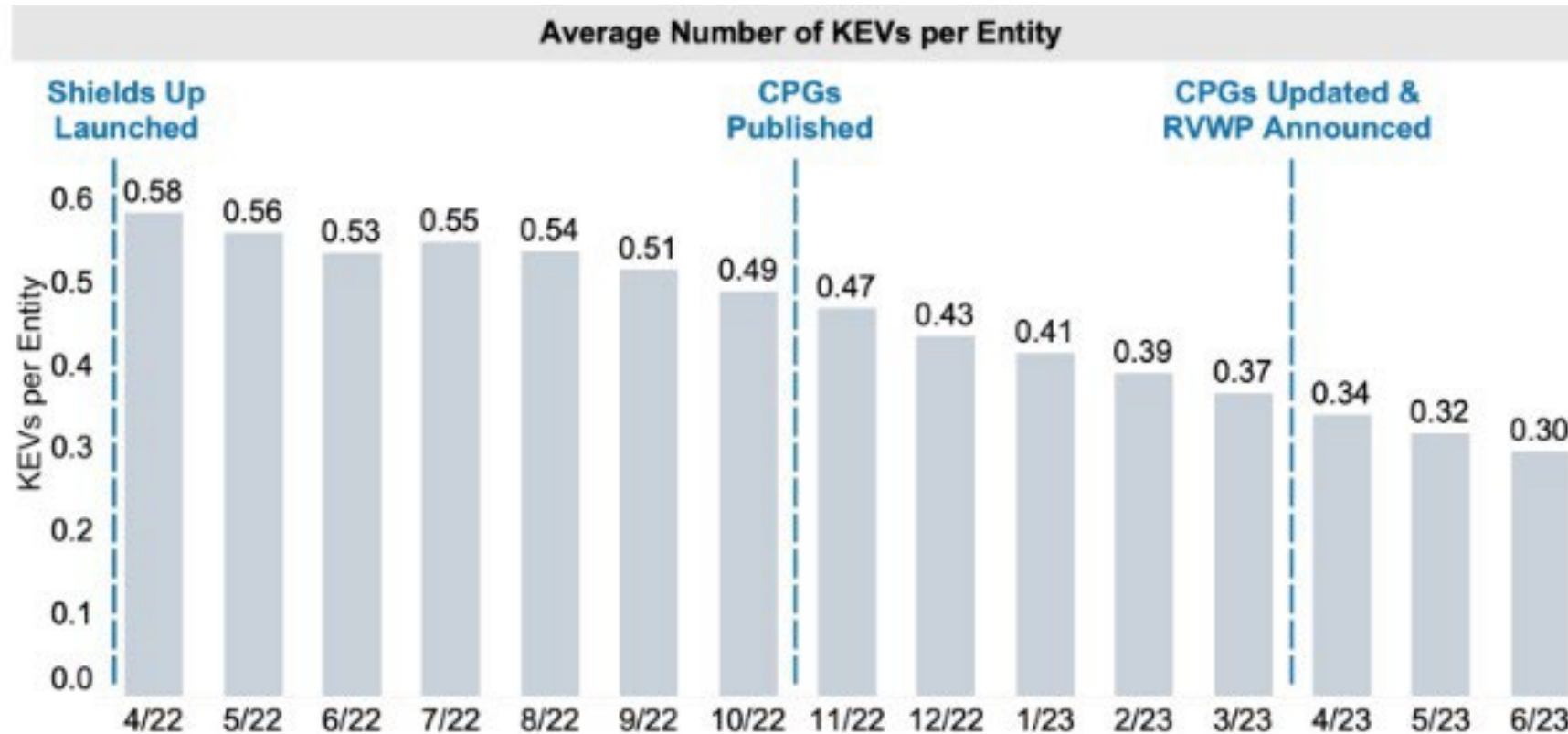


Figure 1: With publication of the CPGs, organizations enrolled in vulnerability scanning continued to demonstrate reductions in KEVs on their networks.



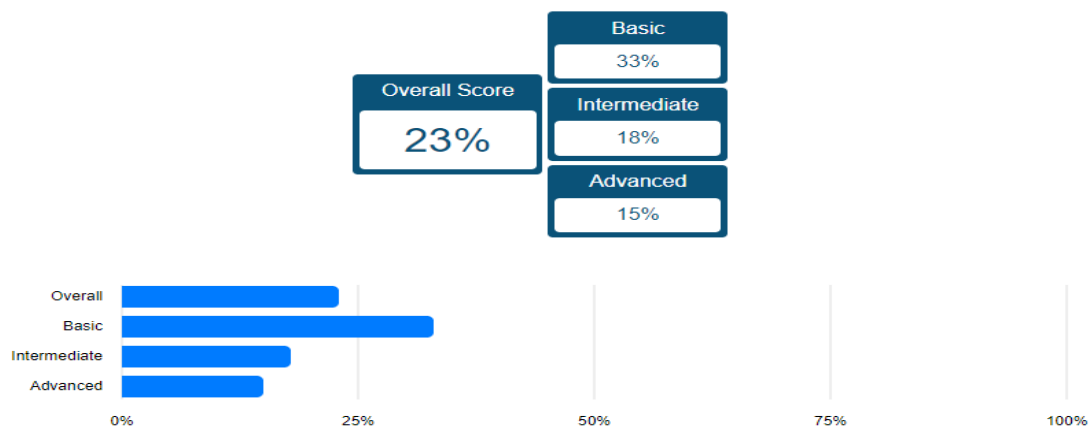
Ransomware Readiness Assessment

- To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA).

Ransomware Readiness Report - CSET

File Edit View Window

Percentage of Practices Performed



Scores are calculated as the percentage of "Yes" answers.



These charts represent the answer distribution overall and across all tiers.

Overall



23% Yes
15% No
63% Unanswered

Basic



33% Yes
28% No
39% Unanswered

Intermediate



18% Yes
6% No
76% Unanswered

Advanced



15% Yes
8% No
77% Unanswered

CISA No-Cost Cybersecurity Tools

[Water and Wastewater Cybersecurity | CISA](#)

[Free Cybersecurity Services & Tools | CISA](#)

[**Known Exploited Vulnerabilities Catalog | CISA**](#)

[**Cyber Hygiene Vulnerability Scanning | CISA**](#)

[Ransomware Vulnerability Warning Pilot \(RVWP\) | CISA](#)

[**Cross-Sector Cybersecurity Performance Goals | CISA**](#)

[Downloading and Installing CSET | CISA](#)

[Logging Made Easy | CISA](#)

[Untitled Goose Tool](#)

[**Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA**](#)

[**Secure Cloud Business Applications \(SCuBA\) Project | CISA**](#)

[GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines](#)

[Hybrid Identity Solutions Guidance \(HISG\)](#)

[**Subscribe to Updates and Alerts from CISA | CISA**](#)

https://www.cisa.gov/sites/default/files/publications/FINAL-CSSO-Protective_DNS-Fact_Sheet.pdf

[CIS Critical Security Controls Version 8 \(cisecurity.org\)](#)

[Information Security Policy Templates | SANS Institute](#)

[**Secure Our World | CISA – Home and Business Best Practices and Awareness Tools**](#)

[**Malware Next-Generation Analysis | CISA**](#)



Malcolm Components



Report an Incident

- CISA: cisa.gov/report ; report@cisa.gov, (888) 282-0870
- FBI/ Internet Crime Complaint Center (IC3): ic3.gov



Final Thoughts: Cyber Threat Mitigations

- Secure Access – Passwords and MFA for Remote Access
 - Change Default Passwords
- Reduce Attack Surface (Configuration Control)
 - Asset Identification – Vulnerability Patch Management
- Network Segmentation
- Aggressive Logging and Threat Hunting
- Firewall Whitelisting/ Allow List (IP and Apps) (Outbound and Inbound)
- Backups- 3-2-1 Method



No-Cost CISA Cybersecurity Services

- **Preparedness Activities**

- Cybersecurity Assessments
- Cybersecurity Training and Awareness
- Cyber Exercises and “Playbooks”
- Information / Threat Indicator Sharing
- National Cyber Awareness System
- Vulnerability Notes Database
- Information Products and Recommended Practices



- **Response Assistance**

- 24/7 Response assistance and malware analysis
- Incident Coordination
- Threat intelligence and information sharing

- **Cybersecurity Advisors** – Regionally deployed advisors

- Incident response coordination
- Public Private Partnership Development
- Advisory assistance and cybersecurity assessments

CISA Contact Information

Colin Glover
Ryan Lewis

colin.glover@cisa.dhs.gov
ryan.lewis@cisa.dhs.gov

CISA URL

<https://www.cisa.gov>

To Report a Cyber Incident to CISA

Call 1-888-282-0870
Email CISAservicedesk@cisa.dhs.gov
visit <https://www.cisa.gov>