FLORIDA RURAL WATER ASSOCIATION

2970 Wellington Circle • Tallahassee, FL 32309-6885
Telephone: 850-668-2746 ~ Fax: 850-893-4581

The Florida Rural Water Association is conducting a Drinking Water Security and Vulnerability Assessment program with Water Utilities throughout the State of Florida. The anticipated benefits will be the strengthening of Florida's water systems against cybersecurity, intrusion, malevolent acts, natural disasters, terrorism, vandalism, etc. and it will benefit the stakeholders of Florida in the same manner. By assisting systems in identifying areas of vulnerability, including vulnerable areas within the SCADA systems, all systems within Florida will benefit.

We concluded a 4 month program on January 31, 2019 performing evaluations of 25 water utility systems, both drinking water and wastewater. Of the 25 Utility systems that was reviewed for vulnerabilities the total number of vulnerabilities discovered were 1567. The following outlines the actual number of vulnerabilities, by category, the percentage of vulnerabilities identified in those 23 categories that exceeded the total number as greater than 9%.

Of the 25 systems that were reviewed the total number of vulnerabilities that were 9% or greater are presented below with the following 4 categories that were identified as the highest risk of these Utilities. (It must be mentioned that all plants tend to have their own unique vulnerabilities and most plant vulnerabilities were not the same or considered to be standard throughout these 25 Utility systems.)

1. **Water Systems:** These questions are related only to the daily operations of the Water Plant, however; there are many subcategories within the water systems such as CCTV, physical security, manual locks and keys, incident response, personnel identification and control, product liability, personnel protective equipment, etc. The total number of questions was 45 for each plant and the total count of vulnerabilities was 154 for the 25 plants at 9.83% of the total vulnerabilities. The following bullets provide a sampling on just a few of the general types of vulnerabilities that are being referred to in this category:

   - There is not another water Utility in proximity to tie into so there is no reciprocating agreement with another utility company in place. There also is no agreements in place with companies that can provide bottled water so they are totally reliable on their own utility plant for water.
   - This system has only one source of groundwater. The new well field is not used due to high sodium chlorides, TDS, and conductivity.
   - The auxiliary generator could be located in a flood zone so it could become susceptible to failure in high water situations.
   - Wells are high in sodium/chloride/conductivity, TDS have been abandoned in the past or removed from service and monitored for MCL reduction. This is a critical concern that is monitored by the Project Manager and Operator.
   - This Utility would not be able to provide storing carryover supply surpluses as there is no storage system available.
   - Critical infrastructure in the Utility potentially lies within the 200 year floodplain. The auxiliary generator at the Office and storage tanks may be below the 200 year flood plain.
   - The system does not monitor raw water quality to determine appropriate treatment.

- Records, maps, and other sensitive information are not labeled confidential however they do not leave the office.
- Digital copies of system maps are not recognized as being stored off-site should the office be destroyed by a hurricane or storm.
- It's noted that vehicles are not locked and secured at all times.
- There is not an alarm system that will detect unauthorized entry.

2. **Information Security** This category consists of the vulnerabilities of computer systems and the concern of hackers and malevolent intent or other security breaches that can cause system failures or compromises. (Software Integrity is a separate category as is Network Protection Practices.) The total number of questions was 35 for each plant and the total count of vulnerabilities was 158 for the 25 plants at 10.08% of the vulnerabilities. The following bullets provide a sampling on just a few of the general types of vulnerabilities that are being referred to in this category:

- The IT department should be in charge of all roles and responsibilities for information security across the Utility's organization. The main county IT department should provide training on the dangers and prevention of hackers entering into the SCADA system
- System Security- There is not a formal document that provides an overview of the security requirements for agency information systems and describes the security controls in place for meeting those requirements.
- Configuration change control- changes made to information systems may not be controlled and documented. These are changes that should be reviewed and in accordance with written policy and procedures, including a process for emergency changes.
- Vulnerability Scanning- a regular occurring process using specialized scanning tools and techniques that evaluates the configuration, patches and services for known vulnerabilities should be employed.
- Risk assessments-a review process is not established at planned intervals or implemented to insure the continuing stability and effectiveness of the utilities approach to managing information security.
- Position Categorization – procedures for identifying system access needs by job function and screening criteria for individuals performing those functions are not in place.
- Disaster Recovery Planning- A disaster recovery plan (DRP) is not in place that supports the current business continuity needs of the Utility.

    - Recovery based on critical and sensitive business needs
    - Location of regular backups of systems and data, with documentation.
    - Regularly updated information about where copies of the plan reside, including appropriate off-site locations.
    - They should provide training for the appropriate personnel.

- Information back-up. Backup copies of information and software should be completed on a routine schedule, tested regularly and stored off-site.

3. **Product Liability**: This unique category addresses questions regarding the safe handling and hazards of chemicals and the processes for quality control, safety and liability. The total number of questions was 26 for each plant and the total count of vulnerabilities was 179 for the 25 plants at 11.42% of the total vulnerabilities. The following bullets provide a sampling on just a few of the general types of vulnerabilities that are being referred to in this category:

- The Maintenance supervisor must coordinate all product safety activity. There is not a committee or group to address product safety or liability.

- There is not a process to identify, evaluate and store all hazardous chemicals. All products upon delivery are not evaluated to verify that they meet all regulatory requirements.
- This Utility does not have a quality assurance control procedures that are documented and reviewed.
- There is currently not a process to verify that instruction manuals and package labels are useful, understandable and available to the user.
- The labels on the deliverables are considered by the Utility to be acceptable to meet applicable industry and government safety standards.
- Product Safety and liability is not an influencing factor when selecting packaging of products.
- Packaging is designed to protect against leaks and spills but this is not considered when selecting the product.
- There has not been a discussion with suppliers about procedures to ensure the security of their products. The plant managers accept this at their own risk and responsibility.
- There is not a system in place to assure that field personnel are well qualified and trained.
- The utility does not have procedures for an efficient product recall.
- All products upon delivery are not evaluated to verify that they meet all regulatory requirements.
- The utility does not obtain certificates of product liability insurance from suppliers.
- The utility does not have an effective quality assurance organization.

4. **Red Flag Rules (Identity theft)** These questions are more related to the HR and Billing Department and are centered around the processes to ensure that the utility's customers information is safeguarded and proper follow ups are performed to notify victims about potential data breaches. There are many protocols to be put in place and good firewall protection from hackers is critical. The total number of questions was 31 for each plant and the total count of vulnerabilities was 187 for the 25 plants at 11.93% of the total vulnerabilities. The following bullets provide a sampling on just a few of the general types of vulnerabilities that are being referred to in this category:

- Wide adherence is not approved by the City Council/Board of Directors.
- The Utility does not enforce senior management oversight of the program.
- The Utility does not incorporate all existing relevant policies and procedures.
- The Utility does not define or document our defined "Red Flags" and the procedures to detect and respond to them.
  - HIPAA Data Security
  - Fraud and abuse
- The Utility does not ensure that they have flagged and investigate and properly report address discrepancies to the appropriate agencies.
- The Utility has not incorporated documentation which outlines the specific requirements for comprehensive education and competency testing of all appropriate agencies.
- The Utility does not sufficiently guard all customers identifying documents from those that do not have a need to know.
- They do not include the appropriate triggers and follow up steps to notify victims about potential data breaches.
- The Utility has not incorporated protocols for reviewing our Red Flag Rule program effectiveness and modifying it as necessary after our initial implementation.
- The Utility has not taken the necessary steps as a leadership team to inspire each one of the employees to do everything they can to guard their customers identity's.

The Vulnerability Assessment program was considered to be a big success. However the representation of only 25 systems was short of providing the FDEP with a total cross section of utilities in the State of Florida to set benchmarks and attempt to standardize the questions for all Florida Utilities, so it was determined to go forward. Additional funding was invested to the Florida Drinking Water and Wastewater Industry. Along with funding being allocated for the Vulnerability Assessment Reports there was additional funds set aside for 5 plants to have the computer Penetration Tests performed and Social Engineering/Phishing test done. In laymen terms this is better known as “hacking computer systems”. We hired a professional “hacker” to conduct these tests.

Penetration and Phishing Test Briefing:

When setting up for a test, we submitted a “Rules of Engagement” (ROE) document which needed to be filled out and agreed to by each of the Utilities. When we received back the ROE from the first plant that committed to the test, they requested that they did not want to participate in the Social Engineering/Phishing test, this test was therefore not performed at this system by their request. It also must be mentioned that two plants selected only had two individuals that had access to their SCADA systems that used e-mail so a Social Engineering/Phishing Test would not prove to be very accurate as the employees would have had foreknowledge that a test was to be conducted and thus skew the results.

One of the other sites provided 13 employee’s to participate in the Social Engineering/Phishing Test and the remaining two provided over 100 employee’s which gave us a good number to select random addresses and perform a successful test. No employees gave out any information during the test. However, a few did click on links in some of the e-mails. The overall exposure is low for the sampling tested and we could only recommend to continue Security Awareness Training as this is key to preventing hackers from entering the systems.

Penetration Test results

We encountered two Utilities out of the five that were tested and that the Penetration Test produced results of entry to their SCADA systems. So based on a small sample size 40% of water utilities that were tested had vulnerabilities.

Three utilities were engaged during the period of 2/16 to 2/17 to perform the Scope and Attack Scenarios. The test was designed to emulate an external attacker attempting to breach their network perimeter. The risk of compromise from an external source was rated as Medium. While there were no vulnerabilities discovered in the VPN interface itself, the penetration tester was able to log on to the VPN using credentials found in a publicly available data breach database. From here, the penetration tester was able to access internal network resources. Mitigation recommendation were further detailed in the report and patching this compromise went into effect by this Utility.

One Utility was engaged during the period of 2/9 to 2/10 to perform the Scope and Attack Scenario. The risk of compromise from an external source was rated high for this Utility. What makes this particular assessment a very strategic outcome is the fact that a company that manages and provides the SCADA “package” for the Utility was very keen on the outcome of this test as they anticipated that there could be remediation requirements for their system. They were very proactive to see the outcome of this Penetration test. This “Managed SCADA Company” provides packaged systems not only to many Utilities in Florida but they provide packaged systems all over the country. In brief by chaining several vulnerabilities and misconfigurations, the Penetration tester was able to glean sensitive customer data and execute code in the context of a low-privileged user on one of the third party provider's web servers. There were several vulnerabilities that could be easily exploited on the system and detailed recommendations for remediation of the vulnerabilities were summarized in the final report. The third party company that managed the SCADA system was very proactive to resolving the 8 vulnerabilities that were identified. Two items that considered to be rated as high, one medium and five low. There were no critical items of major concern. The most serious issue was related to their "ticket system". They immediately started on a course of remediation and anticipate this to be completed by March 15th, 2019. The other high vulnerability issue was related to login credentials and the company is now developing plans to migrate all users to a more robust credential requirement. This transition is targeted to be in effect by May 1, 2019.

FRWA will continue to provide this Vulnerability Assessment service at no charge and you may contact us if interested in this program that will help on reducing vulnerabilities at your water utility.

The following is information about the NRWA Guidance & Interpretation of the 23 Safe Drinking Water Act Provisions Of the "America's Water Infrastructure Act of 2018"

On October 23, 2018, President Donald J. Trump signed into law the "America's Water Infrastructure Act" (AWIA).

Some of the relevant provisions in the 23 new "Safe Drinking Water Act" that we regard are:

Section 2013. Community water system risk and resilience; replaces the provisions in SDWA regarding anti-terrorism activities and instead, in line with existing water system practices, creates requirements for assessing risks from malevolent acts, including terrorism, and resilience to natural hazards and emergency response plans to those threats by community water systems serving more than 3,300 persons.

New Technical Assistance Provisions

Section 2013 COMMUNITY WATER SYSTEM RISK AND RESILIENCE

(1) In general. -- Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system.
(2) Authority to recognize. -- Consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995, the Administrator shall recognize technical standards that are developed or adopted by third-party organizations or voluntary consensus standards bodies that carry out the objectives or activities required by this section as a means of satisfying the requirements under subsection (a) or (b).
(5) Grants for small systems. -- For each fiscal year, the Administrator may use not more than $10,000,000 from the funds made available to carry out this subsection to make grants to community water systems serving a population of less than 3,300 persons, or nonprofit organizations receiving assistance under section 1442(e), for activities and projects undertaken in accordance with the guidance provided to such systems under subsection (e) of this section.

New Risk Assessments and Emergency Response Plans: The enacted legislation includes a new requirement that community water systems serving more than 3,300 persons revise their Vulnerability Assessments and Emergency Response Plan. The new "risk and resilience" assessments are broader in scope than the 2001 Vulnerability Assessments (see Chapter 6). However, the requirement is limited to mandating that eligible community water systems "submit to the Administrator a certification that the system has conducted an assessment…." Similar to the 2001 Vulnerability Assessments' law, EPA is limited from reviewing the content of the assessments in order to provide maximum flexibility and prevent unnecessary federal regulation.

Significant New Mandates and Rulemakings:

Section 2013 COMMUNITY WATER SYSTEM RISK AND RESILIENCE:
Each CWS serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system. Each CWS covered shall submit to the Administrator a certification that the system has conducted an assessment by June 30, 2021, in the case of systems serving a population greater than 3,300 but less than 50,000. Each CWS covered shall review the assessment at least once every 5 years and submit to the Administrator a certification of completion. Each CWS serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates findings of the assessment and certify to the Administrator no later than 6 months after completion of the assessment.

"SEC. 1433. COMMUNITY WATER SYSTEM RISK AND RESILIENCE."

(a) Risk and Resilience Assessments.—
"(1) IN GENERAL.—Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system. Such an assessment—
"(A) shall include an assessment of—
"(i) the risk to the system from malevolent acts and natural hazards;
"(ii) the resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;
"(iii) the monitoring practices of the system;
"(iv) the financial infrastructure of the system;
"(v) the use, storage, or handling of various chemicals by the system; and
"(vi) the operation and maintenance of the system; and
"(B) may include an evaluation of capital and operational needs for risk and resilience management for the system.
"(2) BASELINE INFORMATION.—The Administrator, not later than August 1, 2019, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information on malevolent acts of relevance to community water systems, which shall include consideration of acts that may—
"(A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or
"(B) otherwise present significant public health or economic concerns to the community served by the system. "
"(3) CERTIFICATION.—
"(A) CERTIFICATION ---Each community water system described in paragraph (1) shall submit to the Administrator a certification that the system has conducted an assessment complying with paragraph (1). Such certification shall be made prior to---

"(i) March 31, 2020, In the case of systems serving a population of 100,000 or more.

"(ii) December 31, 2020, In the case of systems serving a population of 50,000 or more but less than 100,000; and "(iii) June 30, 2021, In the case of systems serving a population greater than 3,300 but less than 50,000;

"(B) REVIEW AND REVISION.—Each community water system described in paragraph (1) shall review the assessment of such system conducted under such paragraph at least once every 5 years after the applicable deadline for submission of its certification under subparagraph (A) to determine whether such assessment should be revised. Upon completion of such a review, the community water system shall submit to the Administrator a certification that the system has reviewed its assessment and, if applicable, revised such assessment.

(4) CONTENTS OF CERTIFICATIONS.—A certification required under paragraph (3) shall contain only—

(A) information that identifies the community water system submitting the certification;

(B) the date of the certification; and

(C) a statement that the community water system has conducted, reviewed, or revised the assessment, as applicable.

(5) PROVISION TO OTHER ENTITIES.—No community water system shall be required under State or local law to provide an assessment described in this section (or revision thereof) to any State, regional, or local governmental entity solely by reason of the requirement set forth in paragraph (3) that the system submit a certification to the Administrator.

"(b) Emergency Response Plan.—Each community water system serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates findings of the assessment conducted under subsection (a) for such system (and any revisions thereto). Each community water system shall certify to the Administrator, as soon as reasonably possible after the date of enactment of America's Water Infrastructure Act of 2018, but not later than 6 months after completion of the assessment under subsection.

(c)Therefore: to meet the dates for the certification to the Administrator for the Emergency Response Plan timing the following dates and population count would require the certification to the Administrator shall be made prior to---

"(i) September 30, 2020, In the case of systems serving a population of 100,000 or more.

"(ii) June 30, 2021, In the case of systems serving a population of 50,000 or more but less than 100,000.

"(iii) December 31, 2021, In the case of systems serving a population greater than 3,300 but less than 50,000.

The emergency response plan shall include— "(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;

"(2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;

"(3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and

“(4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

“(c) Coordination.—Community water systems shall, to the extent possible, coordinate with existing local emergency planning committees established pursuant to the Emergency Planning and Community Right-To-Know Act of 1986 (42 U.S.C. 11001 et seq.) when preparing or revising an assessment or emergency response plan under this section.

“(d) Record Maintenance.—Each community water system shall maintain a copy of the assessment conducted under subsection (a) and the emergency response plan prepared under subsection (b) (including any revised assessment or plan) for 5 years after the date on which a certification of such assessment or plan is submitted to the Administrator under this section.

“(e) Guidance To Small Public Water Systems.—The Administrator shall provide guidance and technical assistance to community water systems serving a population of less than 3,300 persons on how to conduct resilience assessments, prepare emergency response plans, and address threats from malevolent acts and natural hazards that threaten to disrupt the provision of safe drinking water or significantly affect the public health or significantly affect the safety or supply of drinking water provided to communities and individuals.