Indiana Department of Environmental Management

Indiana Water Environment Association – Government Affairs Committee

Meeting Minutes

Conference Call

March 12, 2021

1:30 PM – 3:00 PM

Agenda:

1. Introductions
    a. Paul Higginbotham (IDEM), Martha Clark-Mettler (IDEM), Camille Meiners (IFA), Tim Healy (Greely-Hansen), Andrea Alexander (South Bend), Brandi Wallace (Fort Wayne), Brandon Koltz (Koltz Consulting), Fred Andes (BT Law), Brian Neilson (HWC) and Brady Dryer (CEI).

2. IFA-SRF Update
    a. State Fiscal Year (SFY) 2021 (July 1, 2020 to June 30, 2021)
    b. Wastewater SRF
        i. Large Systems - $140M
        ii. Small Systems - $135M
    c. Drinking Water SRF - $55M
    d. 2021 PER Deadlines
        i. Early deadline for bonus points – May 1, 2021
        ii. Regular deadline – June 15, 2021
        iii. Subject to change in 2022 for FY 2022 (July 1, 2021 to June 30, 2022)
    e. Wastewater Administrator Position
        i. Shelley Love was retained by IDEM Drinking Water Branch
        ii. Jacob Schmicker has assumed position with IFA SRF
    f. IFA Regional Meetings
        i. Attendance tracked and required for SRF Financing.
        ii. Current schedule found here: https://www.in.gov/ifa/regional-planning-meetings/
        iii. Indiana Section AWWA is hosting a Regional Meeting on April 14th, 2021
        iv. Schedule for remainder of 2021 will be established.
    g. American Rescue Act and Infrastructure Stimulus Status
        i. Details forthcoming in the next several weeks.
3. COVID-19 Wastewater Testing
    a. IFA/OneWater Report now available here: https://www.in.gov/ifa/files/Indiana-Wastewater-Monitoring-Report-2020.pdf

4. IDEM Staffing Updates
    a. Dale Schnaith retired in January 2021 as Facilities Construction Permits Section Chief, position posted and interviews/selection ongoing.
    b. Samantha Groce is now the Wastewater Inspections Section Chief
    c. Amari Farren will be OWQ Enforcement Section Chief
    d. Permits Branch - Municipal and Industrial Sections are fully staffed.

5. Nutrient Water Quality Standard Update
    a. EPA has revisited discussions with IDEM regarding the development of numeric nutrient Water Quality Criteria

6. Asset Management/Cybersecurity Implementation
    a. Applies to new and expanded WTPs and WWTPs
    b. Both Drinking Water and Wastewater Guidance Final (attached with updated links to guidance)
    c. Requires certification that permittee has the following:
        i. Life Cycle Cost analysis
        ii. Capital Asset Management Plan
        iii. Cybersecurity Plan
    d. No certifications received by agency as of November 10, 2020
    e. Several reminders sent to impacted facilities that have requested/received Preliminary Effluent Limitations for new or expanded WWTPs.
    f. See attached IDEM/EPA outreach following FL Water Treatment Plant Cyber-Attack.

7. Federal NPDES Rule Update
    a. Requires use of updated Municipal NPDES Renewal Forms
    b. See link for proposed NPDES Renewal Forms: https://www.epa.gov/npdes/npdes-application-forms
    c. IDEM requested feedback on forms found at link above.
    d. IDEM to assemble Work Group to review/discuss implementation and changes.

8. EPA POTW Secondary Treatment Questionnaire Status
    a. No formal update provided
    b. Information immediately below from November 10, 2020 IDEM-IWEA GAC meeting:
        i. < 10% participation rate
        ii. Recent reminder sent by EPA

iii. Additional info found here: https://www.epa.gov/eg/potw-nutrient-survey

9. EPA Region 5 State Per and Polyfluoroalkyl Substances (PFAs) Drinking Water and Water Quality Standards
    a. Only Drinking Water Systems Monitoring in IN
    b. Large System Monitoring Complete (>100,000 Population Served)
    c. Medium Systems (50,000 to 99,999 Population Served) Ongoing
    d. Focus on surface water systems with samples collected at raw water intake and after treatment to determine removal efficiencies.
    e. Surface water monitoring on hold to follow states/EPA
    f. ORSANCO is monitoring PFAs

10. Water Quality Criteria for Metals Status
    a. Environmental Rules Board (ERB) consideration of final adoption on May 12, 2021: https://www.in.gov/idem/legal/2355.htm
    b. No Aluminum included.
    c. Minor re-organization of Water Quality Standard tables and comparison (current vs. proposed) available here: https://www.in.gov/idem/cleanwater/2329.htm
    d. Reminder of upcoming Triennial Review of Water Quality Standards

11. 2012 RWQC Update
    a. October 28, 2020 - Citizens Petition public hearing conducted at 1:30 PM: https://www.in.gov/idem/legal/2438.htm
    b. November 18, 2020 - ERB members were asked to submit questions to IDEM and Petitioners tin order to clarify positions and continue discussions. The formation of a Work Group was also agreed upon. https://www.in.gov/idem/legal/files/rules_erb_20201118_summary.pdf
    c. February 10, 2021 – The Petitioners requested additional time to address questions issued by the ERB. IDEM and the Petitioners agreed to meet as a group to discuss questions, solutions, implementation and report back to the ERB at the May 12, 2021 meeting.

12. CSO Compliance
    a. Region 5/National Trends
        i. Region 5 has hired a new CSO Lead
        ii. Indiana has been nationally recognized for Wet Weather Limited Use Subcategory for CSO impacted waters.
    b. Integrated Planning, etc.
        i. Existing plans were discussed as integrated (Evansville)
        ii. Additional integrated plans in the works

c. 2020 Financial Capability Guidance
    i. Can be reviewed here: https://www.epa.gov/waterfinancecenter/proposed-2020-financial-capability-assessment-clean-water-act-obligations
    ii. Currently under review by Biden Administration
    iii. IDEM would allow flexibility if communities opted to utilize.

13. Compliance/Enforcement Updates
    a. See attached Early Warning and Sewer Ban Lists
    b. National SSO compliance initiative
    c. Environmental Justice is often discussed in EPA forums.

14. Operator Certification Rule Work Group Update
    a. 2nd Notice Forthcoming
    b. Changes to enhance recruitment.
    c. Changes to clarify experience, equivalency and education.
    d. See attached survey results regarding industry perception and challenges.

15. Construction/MS4 General Permit and Program Update
    a. General Permit Public Notice
        i. Numerous comments received.
        ii. Final notice to be determined.
    b. Audits expected in 2021 and details to follow.

16. 2020 IDEM/Legislative Updates
    a. SB 389 Repeals State Wetland Law
        i. Most pressing/time-consuming for IDEM
        ii. IDEM is looking to work with legislature on compromise.
    b. SB 271 Agency Bill
        i. Goal to modernize certain processes i.e. remove tax exemptions from IDEM's purview and 303(d) posting for public comment.
    c. IDEM Permit Fees – 1st public notice forthcoming.

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: A21-042A

February 11, 2021

Compromise of U.S. Water Treatment Facility

SUMMARY

On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment plant. The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cyber-security weaknesses, including poor password security, and an outdated operating system. Early information indicates it is possible that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system. Onsite response to the incident included Pinellas County Sheriff Office (PCSO), U.S. Secret Service (USSS), and the Federal Bureau of Investigation (FBI).

The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have observed cyber criminals targeting and exploiting desktop sharing software and computer networks running operating systems with end of life status to gain unauthorized access to systems. Desktop sharing software, which has multiple legitimate uses—such as enabling telework, remote technical support, and file transfers—can also be exploited through malicious actors' use of social engineering tactics and other illicit measures. Windows 7 will become more susceptible to exploitation due to lack of security updates and the discovery of new vulnerabilities. Microsoft and other industry professionals strongly recommend upgrading computer systems to an actively supported operating system. Continuing to use any operating system within an enterprise beyond the end of life status may provide cyber criminals access into computer systems.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov or your local WMD Coordinator. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

THREAT OVERVIEW

Desktop Sharing Software

The FBI, CISA, EPA, and MS-ISAC have observed corrupt insiders and outside cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors. In addition to adjusting system operations, cyber actors also use the following techniques:

- Use access granted by desktop sharing software to perform fraudulent wire transfers.
- Inject malicious code that allows the cyber actors to
    - Hide desktop sharing software windows;
    - Protect malicious files from being detected; and,
    - Control desktop sharing software startup parameters to obfuscate their activity.
- Move laterally across a network to increase the scope of activity.

TeamViewer, a desktop sharing software, is a legitimate popular tool that has been exploited by cyber actors engaged in targeted social engineering attacks, as well as large scale, indiscriminate phishing campaigns. Desktop sharing software can also be used by employees with vindictive and/or larcenous motivations against employers.

Beyond its legitimate uses, TeamViewer allows cyber actors to exercise remote control over computer systems and drop files onto victim computers, making it functionally similar to Remote Access Trojans (RATs). TeamViewer's legitimate use, however, makes anomalous activity less suspicious to end users and system administrators compared to RATs.

Windows 7 End of Life

On January 14, 2020, Microsoft ended support for the Windows 7 operating system, which includes security updates and technical support unless certain customers purchased an Extended Security Update (ESU) plan. The ESU plan is paid per-device and available for Windows 7 Professional and Enterprise versions, with an increasing price the longer a customer continues use. Microsoft will only offer the ESU plan until January 2023. Continued use of Windows 7 increases the risk of cyber actor exploitation of a computer system.

Cyber actors continue to find entry points into legacy Windows operating systems and leverage Remote Desktop Protocol (RDP) exploits. Microsoft released an emergency patch for its older operating systems, including Windows 7, after an information security researcher discovered an RDP vulnerability in May 2019. Since the end of July 2019, malicious RDP activity has increased with the development of a working commercial exploit for the vulnerability. Cyber actors often use misconfigured or improperly secured RDP access controls to conduct cyber-attacks. The xDedic Marketplace, taken down by law enforcement in 2019, flourished by compromising RDP vulnerabilities around the world.

MITIGATIONS

General Recommendations

The following cyber hygiene measures may help protect against the aforementioned scheme:

- Update to the latest version of the operating system (e.g. Windows 10).
- Use multiple-factor authentication.
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured and secure.
- Audit network configurations and isolate computer systems that cannot be updated.
- Audit your network for systems using RDP, closing unused RDP ports, applying multiple-factor authentication wherever possible, and logging RDP login attempts.
- Audit logs for all remote connection protocols.
- Train users to identify and report attempts at social engineering.
- Identify and suspend access of users exhibiting unusual activity.

Water and Wastewater Systems Security Recommendations

The following physical security measures serve as additional protective measures:

Install independent cyber-physical safety systems. These are systems that physically prevent dangerous conditions from occurring if the control system is compromised by a threat actor.

- Examples of cyber-physical safety system controls include:
  - Size of the chemical pump
  - Size of the chemical reservoir
  - Gearing on valves
  - Pressure switches, etc.

The benefit of these types of controls in the water sector is that smaller systems, with limited cybersecurity capability, can assess their system from a worst-case scenario. The operators can take physical steps to limit the damage. If, for example, cyber actors gain control of a sodium hydroxide pump, they will be unable to raise the pH to dangerous levels.

TeamViewer Software Recommendations

For a more secured implementation of TeamViewer software:

- Do not use unattended access features, such as “Start TeamViewer with Windows” and “Grant easy access.”
- Configure TeamViewer service to “manual start,” so that the application and associated background services are stopped when not in use.
- Set random passwords to generate 10-character alphanumeric passwords.
- If using personal passwords, utilize complex rotating passwords of varying lengths. **Note:** TeamViewer allows users to change connection passwords for each new session. If an end user chooses this option, never save connection passwords as an option as they can be leveraged for persistence.

- When configuring access control for a host, utilize custom settings to tier the access a remote party may attempt to acquire.
- Require remote party to receive confirmation from the host to gain any access other than "view only." Doing so will ensure that, if an unauthorized party is able to connect via TeamViewer, they will only see a locked screen and will not have keyboard control.
- Utilize the 'Block and Allow' list which enables a user to control which other organizational users of TeamViewer may request access to the system. This list can also be used to block users suspected of unauthorized access.

Attention Indiana Drinking Water Contacts

The Indiana Department of Environmental Management is forwarding additional information from the Environmental Protection Agency regarding the February 5, 2021 cyber intrusion at a Florida public water supply. Below is an the EPA advisory which contains a list of possible mitigation steps utilities can implement to bolster their cyber security. The **EPA**, **IDEM**, and **InWARN** ask that you be vigilant if you have remote access capability at your systems. If you have any questions about this IDEM notice, do not hesitate to contact Travis Goodwin at 317-775-5473 or by email at: Tgoodwin1@idem.IN.gov.

EPA Advisory

The FBI, DHS, US Secret Service, and the Pinellas County Sheriff's Office have issued a joint situational report that concerns the water sector. EPA is providing critical information from this report to the WSCC and GCC for awareness. EPA recommends that all water systems implement the mitigation measures listed at the end of this report where applicable.

Background

On 5 February 2021, unidentified cyber actors obtained unauthorized access, on two separate occasions, approximately five hours apart, to the supervisory control and data acquisition (SCADA) system used at a local municipality's water treatment plant. The unidentified actors accessed the SCADA system's software and altered the amount of sodium hydroxide, a caustic chemical, used as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal.

The unidentified actors accessed the water treatment plant's SCADA controls via remote access software, TeamViewer, which was installed on one of several computers the water treatment plant personnel used to conduct system status checks and to respond to alarms or any other issues that arose during the water treatment process. All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system. Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.

Recommended Mitigation

- Restrict all remote connections to SCADA systems, specifically those that allow physical control and manipulation of devices within the SCADA network. One-way unidirectional monitoring devices are recommended to monitor SCADA systems remotely.
- Install a firewall software/hardware appliance with logging and ensure it is turned on. The firewall should be secluded and not permitted to communicate with unauthorized sources.

- Keep computers, devices, and applications, including SCADA/industrial control systems (ICS) software, patched and up-to-date.
- Use two-factor authentication with strong passwords.
- Only use secure networks and consider installing a virtual private network (VPN).
- Implement an update and patch management cycle. Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers.

Attention Indiana Drinking Water and Wastewater SCADA Security Contacts

The Indiana Department of Environmental Management maintains a listing of SCADA security contacts for municipal water and wastewater facilities. IDEM is reaching out to you as one of these contacts to provide a recent cybersecurity **emergency directive** and **alert** issued by the Department of Homeland Security's Cyber Security & Infrastructure Security Agency (CISA). This information is specific to vulnerabilities associated with **Microsoft Exchange** products. This information is intended to provide mitigation information to utilities who may be using Microsoft Exchange products, the information may or may not apply to your specific utility. If you have any questions about this IDEM notice, do not hesitate to contact Travis Goodwin at 317-775-5473 or by email at: Tgoodwin1@idem.IN.gov.

CISA has issued Emergency Directive (ED) 21-02 and Alert AA21-062A addressing critical vulnerabilities in Microsoft Exchange products. Successful exploitation of these vulnerabilities allows an attacker to access on-premises Exchange servers, enabling them to gain persistent system access and control of an enterprise network.

CISA strongly recommends organizations examine their systems to detect any malicious activity detailed in Alert AA21-062A.

Review the following resources for more information:

- CISA Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
- AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities
- Microsoft Security Blog Post: Multiple Security Updates Released for Exchange Server

Attention Indiana Drinking Water and Wastewater SCADA Security Contacts

The Indiana Department of Environmental Management maintains a listing of SCADA security contacts for municipal water and wastewater facilities. Considering the recent cyber intrusion at a Florida public water supply, IDEM is reaching out to you as one of these contacts with some detailed information about the Oldsmar, FL incident, as well as a list of recent cybersecurity advisories issued by the Department of Homeland Security's Cyber Security & Infrastructure Security Agency (CISA). Below is link to the CISA directory of advisories as well as brief descriptions and links to the 23 recently added advisories related to specific Industrial Control System vulnerabilities. This information is intended to provide mitigation information to utilities who may be using any of the vulnerable ICS products, the advisories may or may not apply to your specific utility. If you have any questions about this IDEM notice, do not hesitate to contact Travis Goodwin at 317-775-5473 or by email at: Tgoodwin1@idem.IN.gov.

CISA releases 23 Industrial Control Systems Advisories

02/09/2021 10:00 AM EDT

ICS-CERT has released the following 23 advisories today, February 9, 2021. Click on the links below for detailed information on these Industrial Control Systems vulnerabilities.

GE Digital HMI/SCADA iFIX

This advisory contains mitigations for Incorrect Permission Assignment for Critical Resource vulnerabilities in the GE Digital HMI/SCADA iFIX software component.

Advantech iView

This advisory contains mitigations for SQL Injection, Path Traversal, and Missing Authentication for Critical Function vulnerabilities in the Advantech iView device management application.

Siemens SINEMA Server & SINEC NMS

This advisory contains mitigations for a Path Traversal vulnerability in Siemens SINEMA server and SINEC NMS products.

Siemens RUGGEDCOM ROX II

This advisory contains mitigations for Improper Input Validation, NULL Pointer Dereference, Out-of-bounds Write, Insufficient Verification of Data Authenticity, Improper Certificate Validation, and Out-of-bounds Read vulnerabilities in Siemens RUGGEDCOM ROX II products.

Siemens TIA Administrator

This advisory contains mitigations for an Improper Access Control vulnerability in Siemens TIA Administrator products.

Siemens JT2Go and Teamcenter Visualization

This advisory contains mitigations for Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Stack-based Buffer overflow, Out-of-Bounds Write, Type Confusion, Untrusted Pointer Dereference, and Incorrect Type Conversion or Cast vulnerabilities in Siemens JT2Go and Teamcenter Visualization software.

Siemens SCALANCE W780 and W740

This advisory contains mitigations for an Allocation of Resources Without Limits or Throttling vulnerability in Siemens SCALANCE W780 and W740 industrial wireless LAN products.

Siemens SIMARIS Configuration

This advisory contains mitigations for an Incorrect Default Permissions vulnerability in Siemens SIMARIS configuration electrical planning software.

Siemens SIMATIC WinCC Graphics Designer

This advisory contains mitigations for an Authentication Bypass Using an Alternate Path or Channel vulnerability in Siemens WinCC Graphics Designer visualization software.

Siemens DIGSI 4

This advisory contains mitigations for an Incorrect Default Permissions vulnerability in Siemens DIGSI 4 software.

Siemens SCALANCE X Switches (Update A)

This updated advisory is a follow-up to the original advisory titled ICSA-20-012-02 Siemens SCALANCE X Switches that was published January 12, 2021, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for a Use of Hard-coded Cryptographic Key vulnerability in Siemens SCALANCE X switches.

Siemens JT2Go and Teamcenter Visualization (Update A)

This updated advisory is a follow-up to the original advisory titled ICSA-21-012-03 Siemens JT2Go and Teamcenter Visualization that was published January 12, 2021, to the ICS webpage on us-cert.cisa.gov.

This advisory contains mitigations for a Type Confusion, Improper Restriction of XML External Entity Reference, Out-of-bounds Write, Heap-based Buffer Overflow, Stack-based Buffer Overflow, Untrusted Pointer Dereference, and Out-of-bounds Read vulnerabilities in Siemens JT2Go and Teamcenter Visualization software products.

Siemens SCALANCE X Products (Update A)

This updated advisory is a follow-up to the original advisory titled ICSA-21-012-05 Siemens SCALANCE X Products that was published January 12, 2021, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for Missing Authentication for Critical Function, and Heap-based Buffer Overflow vulnerabilities in Siemens SCALANCE X switches.

Siemens Embedded TCP-IP Stack Vulnerabilities-AMNESIA33 (Update A)

This updated advisory is a follow-up to the original advisory titled ICSA-20-343-05 Siemens Embedded TCP/IP Stack Vulnerabilities–AMNESIA:33 that was published December 8, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for an Integer Overflow vulnerability in Siemens SENTRON and SIRIUS products.

Siemens Industrial Products (Update C)

This updated advisory is a follow-up to the advisory update titled ICSA-20-252-07 Siemens Industrial Products (Update B) that was published December 8, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for an Exposure of Sensitive Information to an Unauthorized Actor vulnerability in several Siemens industrial products.

Siemens UMC Stack (Update E)

This updated advisory is a follow-up to the advisory update titled ICSA-20-196-05 Siemens UMC Stack (Update D) that was published December 8, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for Unquoted Search Path or Element, Uncontrolled Resource Consumption, Improper Input Validation vulnerabilities in Siemens UMC components.

Siemens Climatix (Update A)

This updated advisory is a follow-up to the original advisory titled ICSA-20-105-04 Siemens Climatix that was published April 14th, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for cross-site scripting and basic XSS vulnerabilities in Siemens Climatix controllers.

Siemens SCALANCE & SIMATIC (Update D)

This updated advisory is a follow-up to the advisory update titled ICSA-20-105-07 Siemens SCALANCE & SIMATIC (Update C) that was published September 8, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for a resource exhaustion vulnerability in Siemens SCALANCE and SIMATIC products.

Siemens Industrial Products SNMP (Update C)

This updated advisory is a follow-up to the advisory update titled ICSA-20-042-02 Siemens Industrial Products SNMP Vulnerabilities (Update B) that was published August 11, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for data processing errors and NULL pointer dereference vulnerabilities in various Siemens industrial products, including SCALANCE, SIMATIC, and SIPLUS.

Siemens SCALANCE X Switches (Update A)

This updated advisory is a follow-up to the original advisory update titled ICSA-20-042-07 Siemens SCALANCE X Switches that was published February 11, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory contains mitigations for a protection mechanism failure vulnerability in Siemens SCALANCE X switches.

Siemens Industrial Real-Time (IRT) Devices (Update E)

This updated advisory is a follow-up to the advisory update titled ICSA-19-283-01 Siemens Industrial Real-Time (IRT) Devices (Update D) that was published August 11, 2020, to the ICS webpage on us-cert.gov. This advisory includes mitigations for an improper input validation vulnerability in Siemens Industrial Real-Time (IRT) devices.

Siemens SCALANCE X Switches (Update B)

This updated advisory is a follow-up to the advisory update titled ICSA-19-225-03 Siemens SCALANCE X Switches (Update A) that was published August 20, 2019, to the ICS webpage on us-cert.cisa.gov. This updated advisory includes mitigations for an insufficient resource pool vulnerability reported in Siemens SCALANCE X Switches.

Siemens SCALANCE X (Update B)

This updated advisory is a follow-up to the advisory update titled ICSA-19-162-04 Siemens SCALANCE X (Update A) that was published January 14, 2020, to the ICS webpage on us-cert.cisa.gov. This advisory includes mitigations for a storing passwords in a recoverable format vulnerability reported in the Siemens SCALANCE X switches.

INDIANA DEPARTMENT OF ENVIRONMENTAL MANAGEMENT
We Protect Hoosiers and Our Environment.
100 N. Senate Avenue • Indianapolis, IN 46204
(800) 451-6027 • (317) 232-8603 • www.idem.IN.gov
Eric J. Holcomb, *Governor*
Bruno L. Pigott, *Commissioner*

Applicability and Implementation of IC 13-18-26: Wastewater Treatment Plants

Certification Requirements for Wastewater Permitting:

Amendments to Indiana Code 13-18-26, which went into effect on July 1, 2019, require certain NPDES permit applicants to certify that they have prepared and completed a life cycle cost-benefit analysis, a capital asset management plan, and a cybersecurity plan. The certification must be submitted to IDEM along with the NPDES permit application.

The requirements of IC 13-18-26 are applicable to the following NPDES permitting actions:

1. A permit for a new wastewater treatment plant with an average design flow greater than .1 MGD. The definition of "wastewater treatment plant" under IC 13-11-2-258(b) excludes industrial wastewater facilities.
2. A permit for the modification or expansion of a wastewater treatment plant greater than .1 MGD that increases the average design flow. The renewal of an NPDES permit that does not increase average design flow does not require a certification.

Due to the time and resources necessary to complete the plans and analyses, if an applicant cannot meet the certification requirements at the time of application submittal, IDEM will work with the applicant on a transitional basis up to June 1, 2020. After June 1, 2020, IDEM will not issue a permit to an applicant that is subject to IC 13-18-26 if the required certification is not included with the application packet, as required by IC 13-18-26-1(b).

Certification Example:

Attached to this applicability memo is an example certification that meets the requirements of IC 13-18-26. A permit applicant may use this form, or develop their own form that meets the statutory requirements. Please note that the certification must be notarized.

Five-Year Review:

The permittee must review the life cycle cost-benefit analysis, capital asset management plan, and cybersecurity plan at least once every five years. If any of the plans or analyses are revised during the five-year review, the permittee must submit a new certification to IDEM with its NPDES renewal application.

Guidance on Developing Analyses and Plans:

IC 13-18-26 describes what must be included in the life cycle cost-benefit analysis, capital asset management plan, and cybersecurity plan. Similar analyses and plans are required by the Indiana Finance Authority's State Revolving Fund (SRF) Loan Program under a different statute. IDEM is providing the following links to SRF guidance documents with information permit applicants may find helpful in meeting the requirements of IC 13-18-26. Please refer to IC 13-18-26, a copy of which is attached to this memo, for the specific requirements applicable to the certification submitted to IDEM.

EXAMPLE

IC 13-18-26 Certification of Completion
Wastewater

Indiana Code 13-18-26 requires the permit applicant to certify that the following documents have been prepared and completed:

- A Life Cycle Cost-Benefit Analysis, as described in IC 13-18-26-3;
- A Capital Asset Management Plan, as described in IC 13-18-26-4; and
- A Cybersecurity Plan, as described in IC 13-18-26-5.

The certification of completion must be submitted to IDEM along with the permit application, and must be notarized. The plans and analyses must be reviewed and revised (as necessary) at least once every five years. A new certification must be submitted to IDEM (with the NPDES renewal application) if any plan or analysis is revised during the five-year review.

I hereby certify that I am an authorized representative for the permit applicant and pursuant to IC 13-18-26, the permit applicant has developed and completed a life cycle cost-benefit analysis; a capital asset management plan; and a cybersecurity plan that meet the requirements of IC 13-18-26-3, IC 13-18-26-4, and IC 13-18-26-5. To the extent required under IC 13-18-26-6, the plans and analyses are available for public inspection.

_____	_____	_____
Permit Applicant (Printed)	Signature	Date
_____	_____	_____
Authorized Representative (Printed)	Signature	Date
_____	_____	
Notary (Printed)	Signature	

My Commission Expires: _____

(seal)

INDIANA DEPARTMENT OF ENVIRONMENTAL MANAGEMENT
We Protect Hoosiers and Our Environment.
100 N. Senate Avenue • Indianapolis, IN 46204
(800) 451-6027 • (317) 232-8603 • www.idem.IN.gov
Eric J. Holcomb
Governor
Bruno L. Pigott
Commissioner

Applicability and Implementation of IC 13-18-26: Permit Applications for Community Public Water System (PWS) Treatment Plants.

Certification Requirements for PWS Permitting:

Amendments to Indiana Code 13-18-26, which went into effect on July 1, 2019, require certain Community PWS permit applicants to certify that they have prepared and completed a life cycle cost-benefit analysis, a capital asset management plan, and a cybersecurity plan. The certification must be submitted to IDEM along with the PWS permit application under IC 13-18-16.

The requirements of IC 13-18-26 are applicable to the following PWS permitting actions:

1. A permit for a new PWS treatment plant, defined by IC 13-11-2-264, for a community water system.
2. A permit for the modification or expansion of a community PWS treatment plant that increases the system design capacity of the plant.

A system does not increase system design capacity if it is applying for a permit or submitting a notice of intent for:

1. The installation of new water mains.
2. The replacement of an existing drinking water well.
3. Chemical treatment that does not increase system design capacity.
4. Any other treatment improvements, process changes or modifications that do not increase system design capacity.

The requirements of IC 13-18-26 do not apply to noncommunity PWSs, including transient and nontransient noncommunity PWS.

Due to the time and resources necessary to complete the plans and analyses, if an applicant cannot meet the certification requirements at the time of application submittal, IDEM will work with the applicant on a transitional basis up to October 1, 2020. After October 1, 2020 IDEM will not issue a permit to an applicant that is subject to IC 13-18-26 if the required certification is not included with the application packet, as required by IC 13-18-26-1(b).

Certification Example:

Attached to this applicability memo is an example certification that meets the requirements of IC 13-18-26. A permit applicant may use this form, or develop their own form that meets the statutory requirements. Please note that the certification must be notarized.

Five-Year Review:

The permittee must review the life cycle cost-benefit analysis, capital asset management plan, and cybersecurity plan at least once every five years. If any of the plans or analyses are revised during the five-year review, the permittee must submit a new certification to IDEM.

EXAMPLE

IC 13-18-26 Certification of Completion
Drinking Water
PWSID No. _____

Indiana Code 13-18-26 requires the permit applicant to certify that the following documents have been prepared and completed:

- A Life Cycle Cost-Benefit Analysis, as described in IC 13-18-26-3;
- A Capital Asset Management Plan, as described in IC 13-18-26-4; and
- A Cybersecurity Plan, as described in IC 13-18-26-5.

The certification of completion must be submitted to IDEM along with the permit application, and must be notarized. The plans and analyses must be reviewed and revised (as necessary) at least once every five years. A new certification must be submitted to IDEM if any plan or analysis is revised during the five-year review.

I hereby certify that I am an authorized representative for the permit applicant and pursuant to IC 13-18-26, the permit applicant has developed and completed a life cycle cost-benefit analysis; a capital asset management plan; and a cybersecurity plan that meet the requirements of IC 13-18-26-3, IC 13-18-26-4, and IC 13-18-26-5. To the extent required under IC 13-18-26-6, the plans and analyses are available for public inspection.

_____	_____	_____
Permit Applicant (Printed)	Signature	Date
_____	_____	_____
Authorized Representative (Printed)	Signature	Date
_____	_____	
Notary (Printed)	Signature	

My Commission Expires: _____

(seal)

IC 13-18-26 Chapter 26. Permit and Permit Application Conditions for Water and Wastewater Treatment Plants

IC 13-18-26-1 Certificate of completion required

Sec. 1. (a) Except as provided in subsection (c), a permit required under IC 13-18-16 for the operation of a public water system may not be issued unless the application contains the certification of completion required under section 2 of this chapter.

(b) Except as provided in subsection (c), the department may not issue a permit required under environmental management laws for the discharge from a wastewater treatment plant, as defined in IC 13-11-2-258(b), unless the application contains the certification of completion required under section 2 of this chapter.

(c) The requirement of a certification of completion under section 2 of this chapter does not apply to the following:

(1) A noncommunity public water system that has fewer than fifteen (15) service connections used by year-round residents.

(2) A noncommunity public water system that regularly serves fewer than twenty-five (25) year-round residents.

(3) A permit for the modification or expansion of a drinking water treatment plant that does not increase system design capacity.

(4) A permit for a wastewater treatment plant with an average design flow of not more than one hundred thousand (100,000) gallons per day.

(5) A permit for the modification or expansion of a wastewater treatment plant that does not increase average design flow.

(6) The renewal of an NPDES permit for the discharge from a wastewater treatment plant that does not include a modification or expansion as described in subdivision (5).

As added by P.L.126-2018, SEC.6. Amended by P.L.15-2019, SEC.12.

IC 13-18-26-2 Certification that documents have been prepared

Sec. 2. A permit described in section 1(a) or 1(b) of this chapter may not be issued unless the applicant submits, along with the permit application, a certification that all of the following documents have been prepared and are complete under the requirements of this chapter:

(1) A life cycle cost-benefit analysis, as described in section 3 of this chapter.

(2) A capital asset management plan, as described in section 4 of this chapter.

(3) A cybersecurity plan, as described in section 5 of this chapter.

As added by P.L.126-2018, SEC.6. Amended by P.L.15-2019, SEC.13.

IC 13-18-26-3 Life cycle cost-benefit analysis

Sec. 3. A life cycle cost-benefit analysis must include a comparison of the alternatives of:

(1) meeting the water supply or wastewater service needs of the community or area served or proposed to be served through the operation of the water and wastewater treatment plant, as:

(A) owned and operated; or

(B) proposed to be owned and operated;

according to the terms of the permit application; and

(2) meeting the water supply or wastewater service needs of the community or area

served or proposed to be served through one (1) or more other potential means.
As added by P.L.126-2018, SEC.6.

IC 13-18-26-4 Capital asset management plan

Sec. 4. A capital asset management plan must include all of the following:

(1) A plan to annually review infrastructure needs of the water or wastewater treatment plant.

(2) A detailed engineering analysis of asset conditions and useful life, to be used to develop an infrastructure inspection, repair, and maintenance plan.

(3) An analysis of customer rates necessary to support the capital asset management plan, including emergency repairs.

(4) A certification that the water or wastewater treatment plant has:

(A) a certified operator;

(B) a corporate officer or system manager; and

(C) access to an engineer, either on staff or by contract.

As added by P.L.126-2018, SEC.6.

IC 13-18-26-5 Cybersecurity plan

Sec. 5. A cybersecurity plan must provide for the protection of the water or wastewater treatment plant from unauthorized use, alteration, or destruction of electronic data.
As added by P.L.126-2018, SEC.6.

IC 13-18-26-6 Completion, periodic revision, and public disclosure of analysis and plans

Sec. 6. (a) The analyses and plans described in sections 3, 4, and 5 of this chapter must be:

(1) complete under the requirements of this chapter at the time an application for a permit described in section 1(a) or 1(b) of this chapter is submitted;

(2) reviewed and revised at least once every five (5) years, for as long as the permit holder operates the water treatment plant or wastewater treatment plant; and

(3) except for customer specific data, including information excluded from public access under IC 5-14-3-4(a), or for a cybersecurity plan required under section 5 of this chapter, made publicly available.

(b) A certification that the analyses and plans described in sections 3, 4, and 5 of this chapter are complete under the requirements of this chapter must be submitted to the department:

(1) under section 2 of this chapter at the time an application for a permit described in section 1(a) or 1(b) of this chapter is submitted; and

(2) at least once every five (5) years after an application for a permit described in section 1(a) or 1(b) of this chapter is submitted, when the analysis and plans are reviewed and revised.

(c) A certification submitted to the department under this chapter must be notarized.
As added by P.L.126-2018, SEC.6. Amended by P.L.15-2019, SEC.14.

IC 13-18-26-7 Denial of permit application for failure to include notarized certification

Sec. 7. Failure to include a notarized certification with an application for a permit described in section 1(a) or 1(b) of this chapter constitutes grounds for denial of the permit application.
As added by P.L.126-2018, SEC.6. Amended by P.L.15-2019, SEC.15.

Revised Links 04/08/21

Asset Management Plan:

Checklist: https://www.in.gov/ifa/srf/files/AMP-Checklist-for-Borrowers-July-2018.pdf

Guidance: https://www.in.gov/ifa/srf/files/AMP-Guidance-Packet-update-9-17-2019.pdf

Cost Benefit Analysis (see Chapter 4):

https://www.in.gov/ifa/srf/files/ww-per-requirements-july-2018-2.pdf

Cyber Security Checklist (see Appendix C):

https://www.in.gov/ifa/srf/files/AMP-Guidance-Packet-update-9-17-2019.pdf