CYBER RISKS & RESOURCES FOR WATER & WASTEWATER UTILITIES

Abad Cabassa
Cyber Security Advisor (CSA) for Connecticut
Cybersecurity and Infrastructure Security Agency (CISA)

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

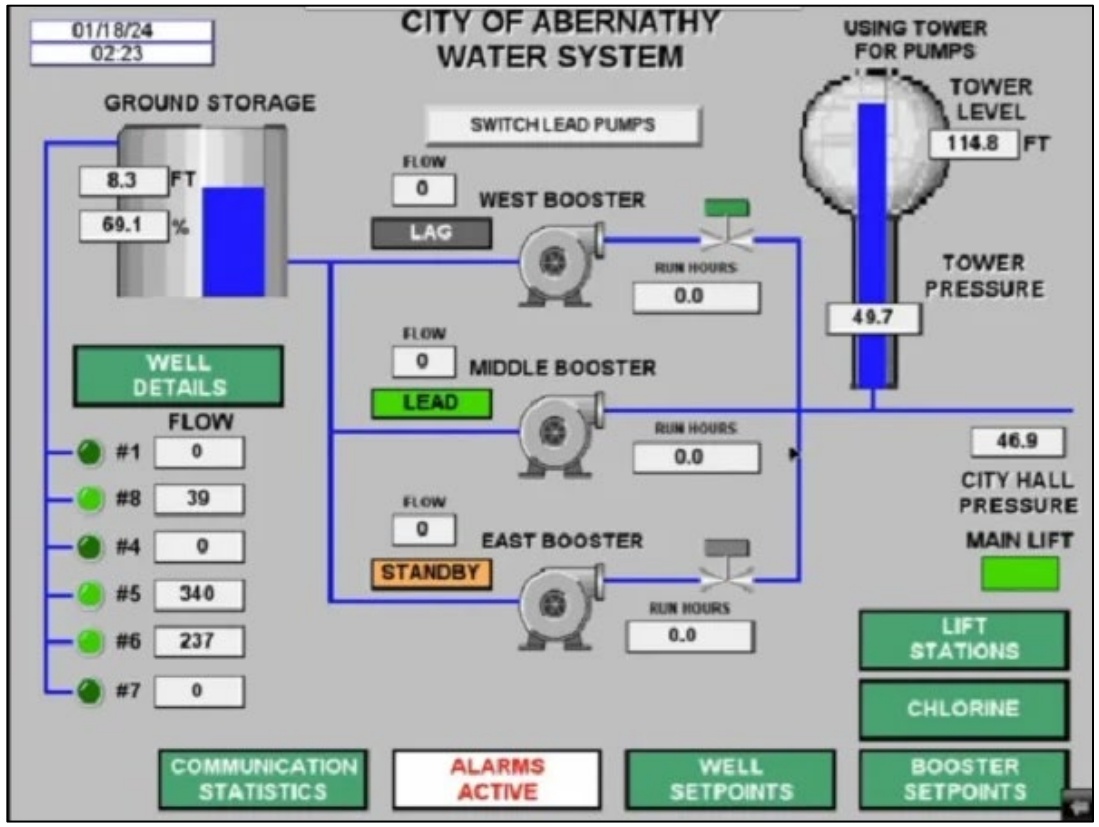
Threats to Water and Wastewater Sector



Cyber Actors of Russia Reborn (CARR)



Muleshoe, TX Water Tower



Screenshot of Abernathy, TX Water System HMI

Muleshoe's city manager, said, "I would have never thought that somebody tied to the Russian military would target Muleshoe." after an attack that resulting in a storage tank overflow.

State Actors Targeting Operational Technology

Nation-State cyber actors continue to target critical infrastructure in the United States in response to ongoing conflicts around the world.

Their goal is to gain remote access to internet exposed human-machine interface (HMI) devices and cause disruptions to operations.

- Modify usernames/passwords
- Modify parameters and instrument settings
- Disable alarms
- Restart or shutdown the device



State Actors Targeting Operational Technology

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

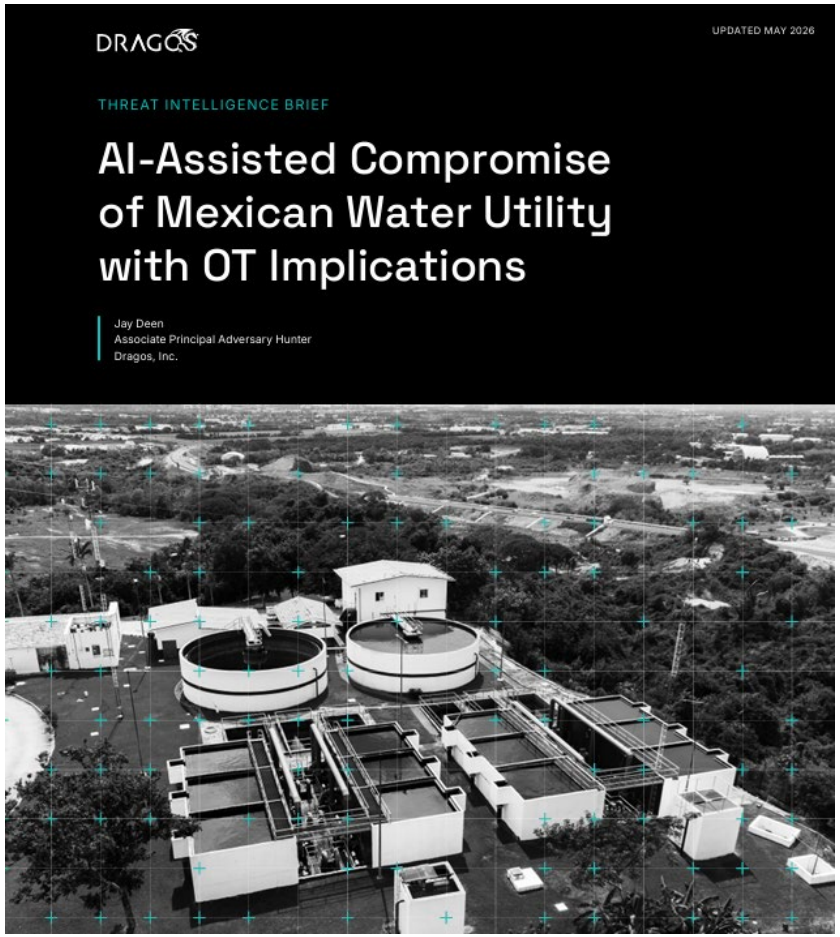


"[This is] a world where a war in Asia will be accompanied by very serious threats for Americans. The explosion of pipelines, the pollution of water systems, the derailing of our transportation systems, the severing of our communications, specifically to incite panic and societal chaos and to deter our ability to marshal military might and citizen will."

Attacks Using Super Intelligence

The malicious actor used commercially available SI throughout the attack cycle to:

- Enumerate the internal network and identify the critical systems.
- Analyze the control server and identify methods for gaining access.
- Research vendor documentation and create a credential list to brute force the password.
- Develop a modular piece of malware that was used for post-compromise activity and was constantly adapted throughout the attack.



Insider Threat

PRESS RELEASE

Former Stoughton Water Department Employee Arrested for Tampering With Drinking Water

Berwick Sewer District employees plead guilty

Charges involve tampering and falsifying records

John Doyle jdoyle@seacoastonline.com

Published 3:54 p.m. ET April 10, 2018 | **Updated 4:29 p.m. ET April 10, 2018**

Vulnerability Snapshot

The Water and Wastewater Systems Sector remains a prime target for cyber threats, with recent findings revealing critical vulnerabilities and exposures

CISA's Vulnerability Snapshot on the Water and Wastewater Systems Sector, published August 2026 and covering January 1, 2026- March 31, 2026:

- At least 14 entities exposed services with 7 unique known exploited vulnerabilities (KEVs), all linked to ransomware activity.
- 23 entities exposed high-risk vulnerable services to the internet; Remote Desktop Protocol (RDP) was the most exposed, increasing risk of unauthorized access and disruption. **101 entities** exposed OT/industrial control systems (ICS) and other networked devices to the internet, highlighting the need for Zero Trust Network Access (ZTNA) solutions.
- 97 distinct network edge devices were identified as valuable initial access points for threat actors, including Chinese government-sponsored groups; security hardening and monitoring are essential.

Common Tactics Used by Malicious Actors



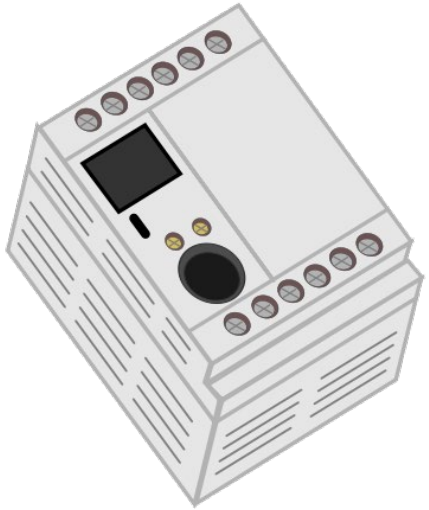
Mapping the Attacks…



Discovery of exposed PLCs (Shodan, Censys, etc.)



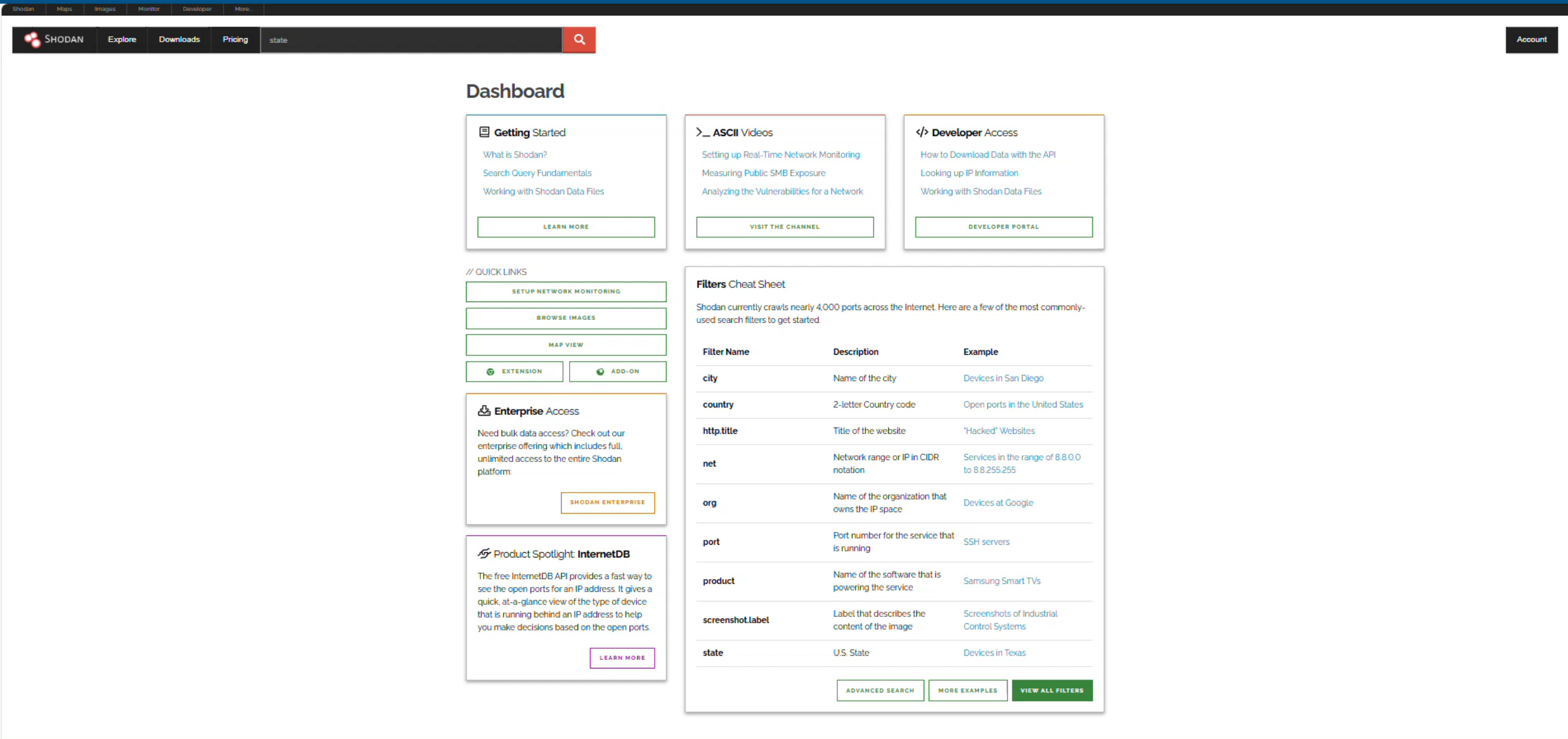
Direct access via vulnerabilities discovered



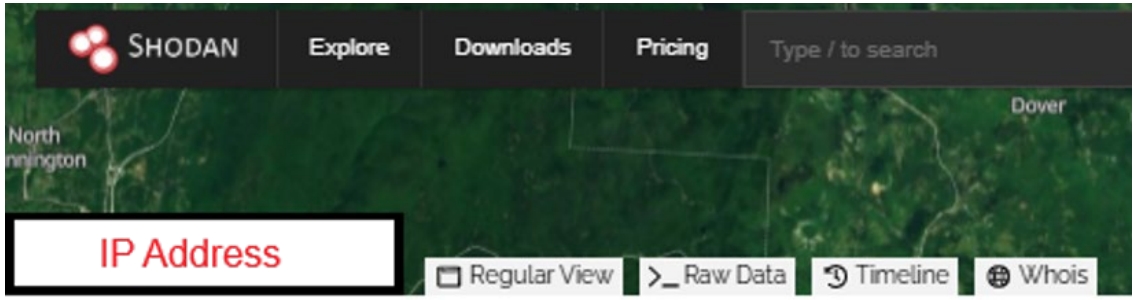
Change IP addresses
Set/modify passwords
Change set points / alarms
Lock out operators

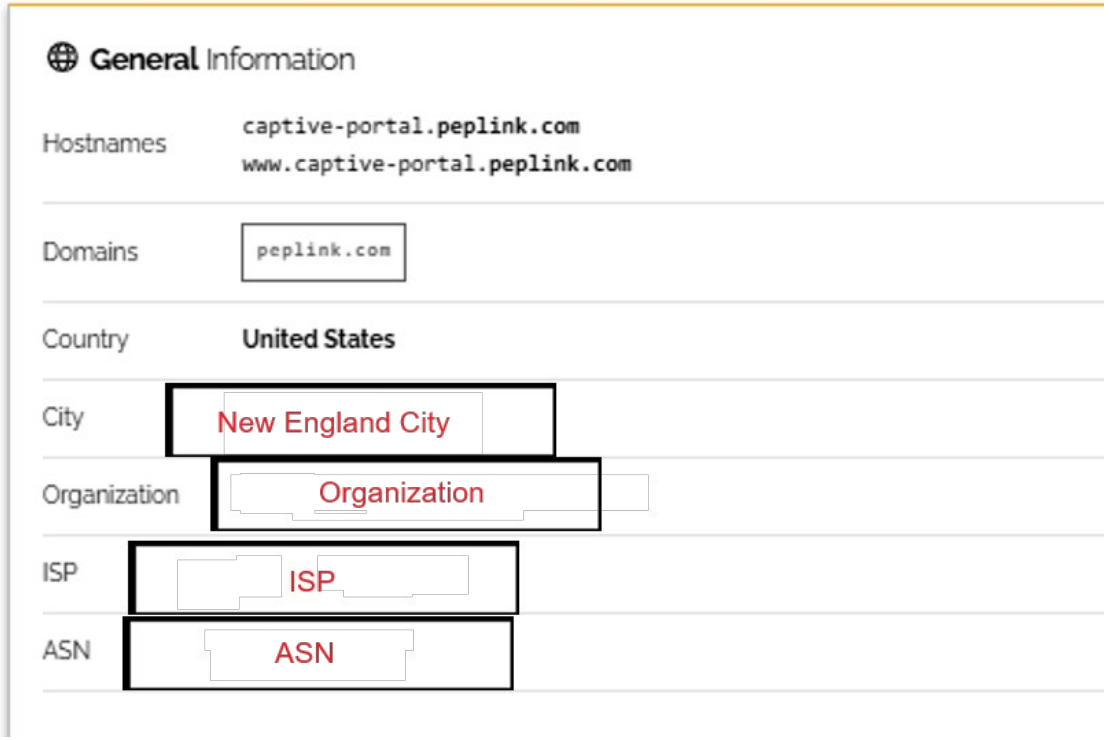
Abad Cabassa
November 5, 2026

This is not a sophisticated attack…



This is not a sophisticated attack…

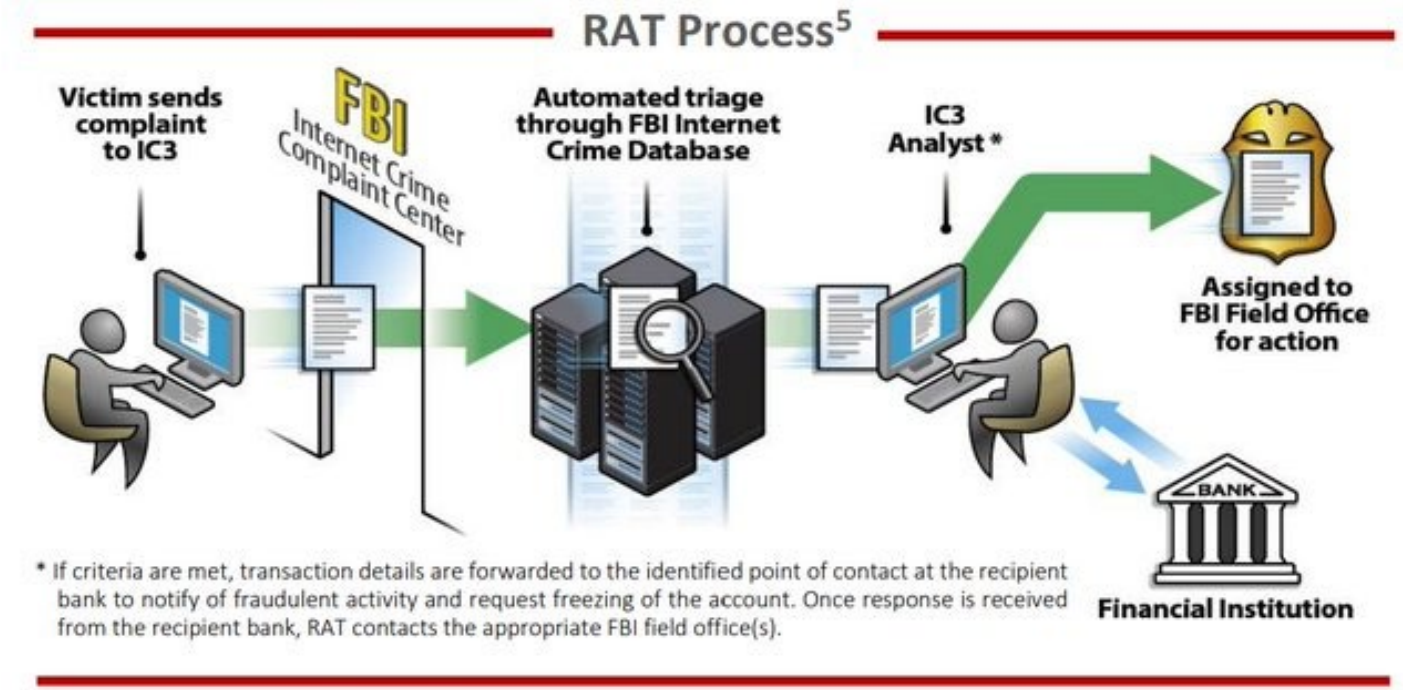






Abad Cabassa
November 5, 2026

Internet Crime Complaint Center (IC3)



The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

SA Jeffrey D Nelson
FBI New Haven – CY-1
(203) 777-6311 (O)
(917) 439-5703 (C)
jdnelson2@fbi.gov

https://ic3.gov

Internet Crime Complaint Center (IC3)

Mitigations and Tools



What Every WWS Leader Should Know

Ensure that your organization is aware of and applying best practices for ICS cybersecurity.



Every leader should be asking:

1. What's at risk – have we prioritized our assets and identified the potential consequences if our control system was compromised?
2. Who is the single manager ultimately responsible for cybersecurity, and do we rely on third-party support?
3. Is our ICS environment protected from the Internet and how have we validated that?
4. Do we have remote access to our ICS network? If so, why do we need it, and how is it protected?
5. Are we reading the available resources and applying the recommended best practices for cybersecurity

Protect Your Networks from the Internet

Is your control system connected directly to the Internet?

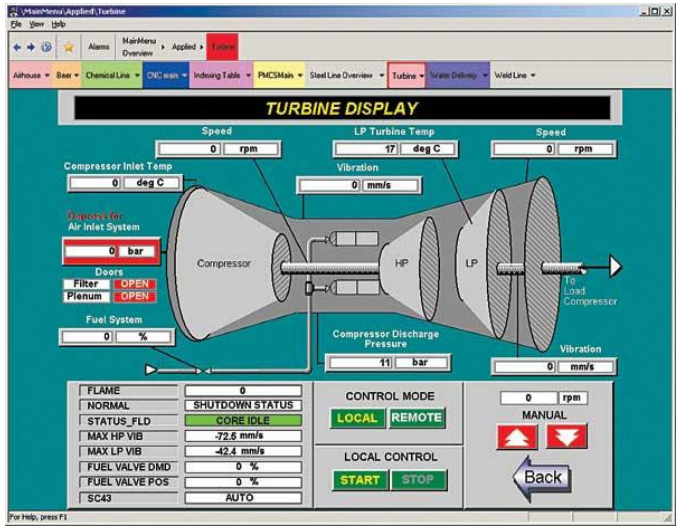
- Do not allow direct connectivity from the Internet into your ICS network(s):
  - The ICS network must be protected from direct access using reliable defensive measures and authentication requirements.
  - Segregate your network by zones according to the work breakdown of your organization.



Direct Access

for

Intruders



Immediate PLC-Focused Mitigations

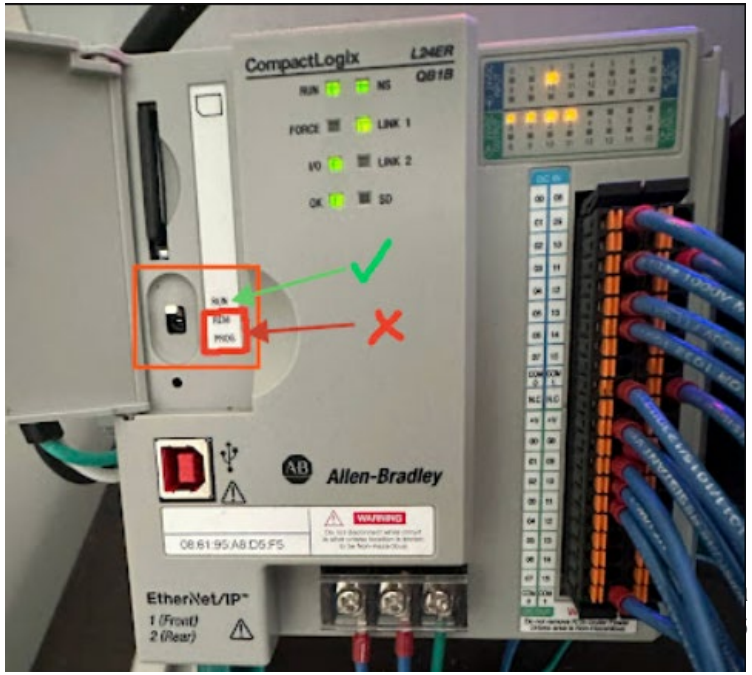
Immediate steps to follow:

- Remove PLCs/OT from access to the public Internet
- Route any necessary remote access via a secured VPN/gateway (never direct to PLC)
- Change default credentials; enforce strong password policies
- IP whitelisting for known engineering workstations



Recovery and vendor guidance

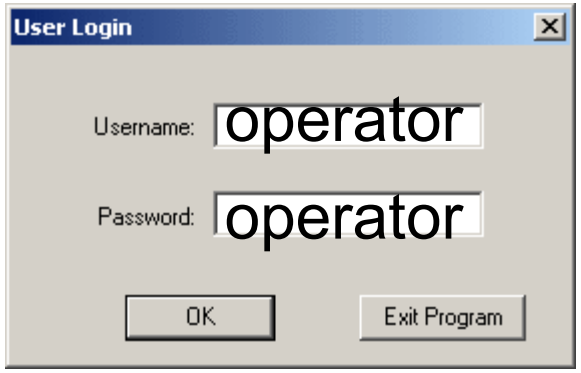
- Maintain clean offline backups of PLC images for rapid restore
- Rockwell Micrologix: follow vendor ‘Restoring Access’ notice
- Set controllers to RUN mode per vendor guidance; apply latest firmware



Passwords and Shared Accounts

- Unique credentials for all users
- No password reuse
- Complex-ish passwords
- View only access | password to make changes
- No stickered passwords
- No passwords stored on systems unencrypted
- MFA for remote access solutions





Abad Cabassa
November 5, 2026

MSP & Integrator Unity

- Identify risks and exposure
- Assess and coordinate cyber hygiene practices
- Coordinate backup and recovery requirements
- Identify any missing or unidentified security capabilities
- Assess the ability to operate manually
- Identify if and how your integrator / MSP is storing sensitive information





Abad Cabassa
November 5, 2026

Cybersecurity Performance Goals Assessment

- Voluntary and confidential
- Identify gaps
- Recommend resources
- Report to share with leadership

- Capture return on investment
- Track improvements
- Justification for grant requests

1.A Asset Inventory	ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED:** Hardware Additions (T1200) Exploit Public-Facing Application (T0819, ICS T0819) Internet-accessible device (ICS T0883) **RECOMMENDED ACTION:** 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. **FREE SERVICES AND REFERENCES:** Cyber Hygiene Services, "Stuff Off Search" Guide or email vulnerability@cisa.DHS.gov		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

Cyber Hygiene (CyHy) Scanning

Continually assess Internet-accessible systems for known vulnerabilities and provide actionable reports to partners.

OVERALL PROCESS

Planning

- Request service (Existing Cyber Hygiene Customers)
- Provide target list (scope)
- Confirm scanning schedule
- Pre-scan notification

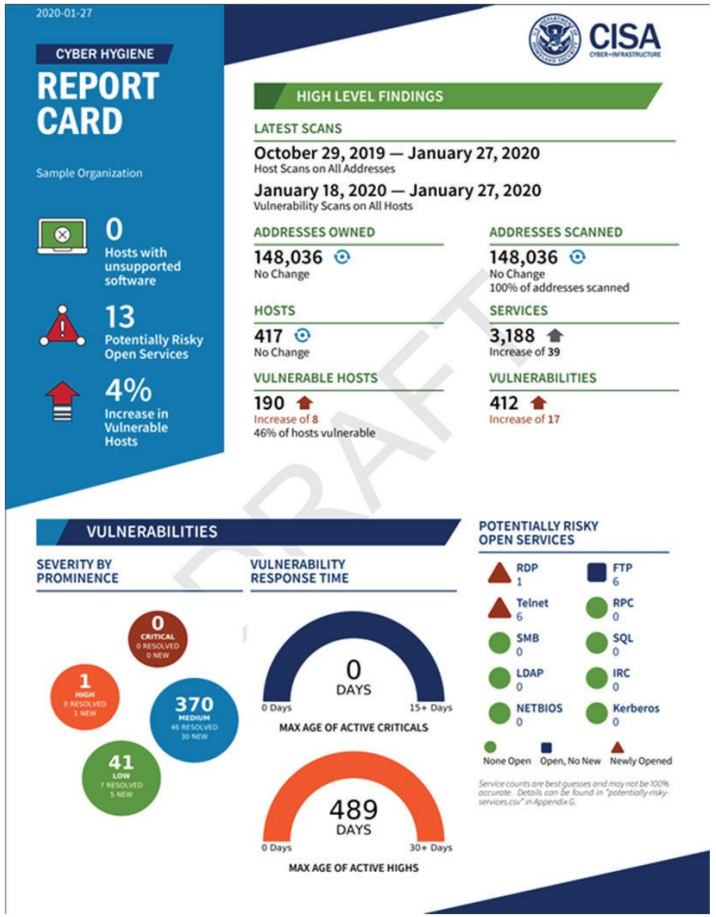
Execution

- Initial discovery scan of submitted list
- Conduct vulnerability scan

Reporting

- Provide detailed report of findings
- Follow on discussion (if necessary) to review

Email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.

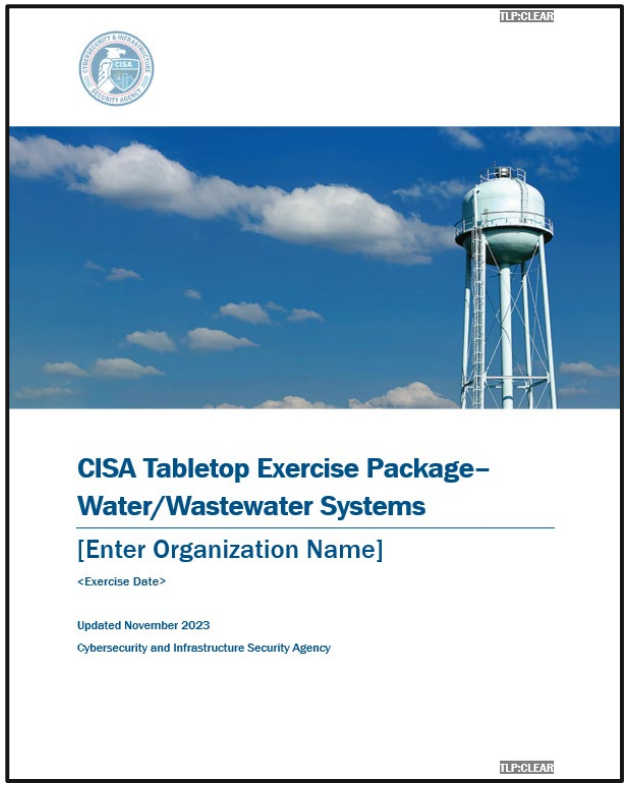


CISA Tabletop Exercise Package (CTEP)

Designed to assist critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders.

- **24 cybersecurity scenarios**
- **68 physical security scenarios**

Day 50
A system alarm alerts facility operators of several control valves opening and closing at random times throughout <service area>, causing a shutdown of operations due to automatic emergency fail safes. Technicians attempting to access the malfunctioning ICS/SCADA devices notice administrative account credentials were changed without their knowledge, inhibiting their access to the devices. During physical inspection of the failed components, technicians discover there is no physical reason for the failure.



Industrial Control Systems (ICS) Training

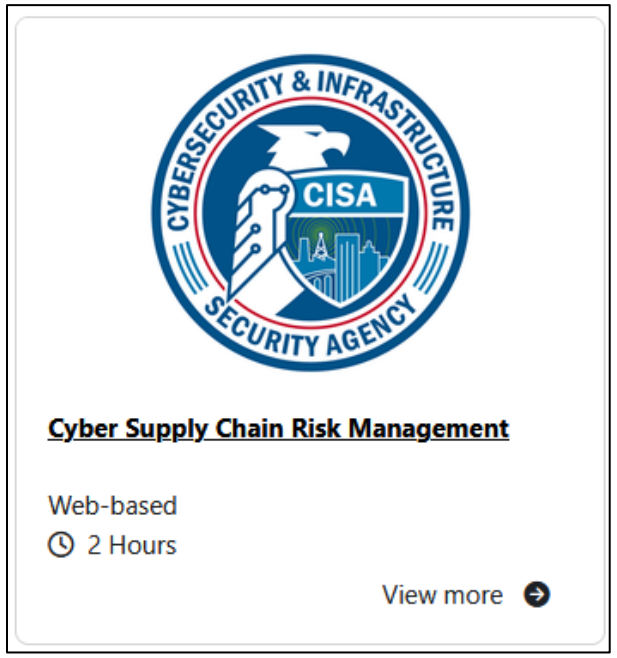
Instructor Led Training

- Introduction to Control Systems Cybersecurity (101) - 4 hrs
- Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- ICS Cybersecurity (301L) - 4 days **in person**
  - ICS Cybersecurity (301V) – 12 hrs
- ICS Evaluation (401L) - 3 days **in person**
  - ICS Evaluation (401V) – 20 hrs

Virtual Learning Portal

- ICS Cybersecurity Landscape for Managers
- Mapping IT Defense-in-Depth Security Solutions to ICS
- 13 additional courses on demand





Abad Cabassa
November 5, 2026

OT and ICS Cybersecurity Advisories

- OT / ICS specific alerts
- Sector specific alerts
- Equipment / software manufacture alerts
- Establish a formal risk registrar and vulnerability tracker
- Prioritize mitigations based on risk
- Pay attention to geopolitical concerns



Abad Cabassa
November 5, 2026

CAN YOU GO MANUAL??







Manual Operation Considerations

- How long can your staff operate during manual operations
- Regulatory requirements / concerns
- How long until you can recover
- Downstream impacts
- Are OT / SCADA services in the cloud?



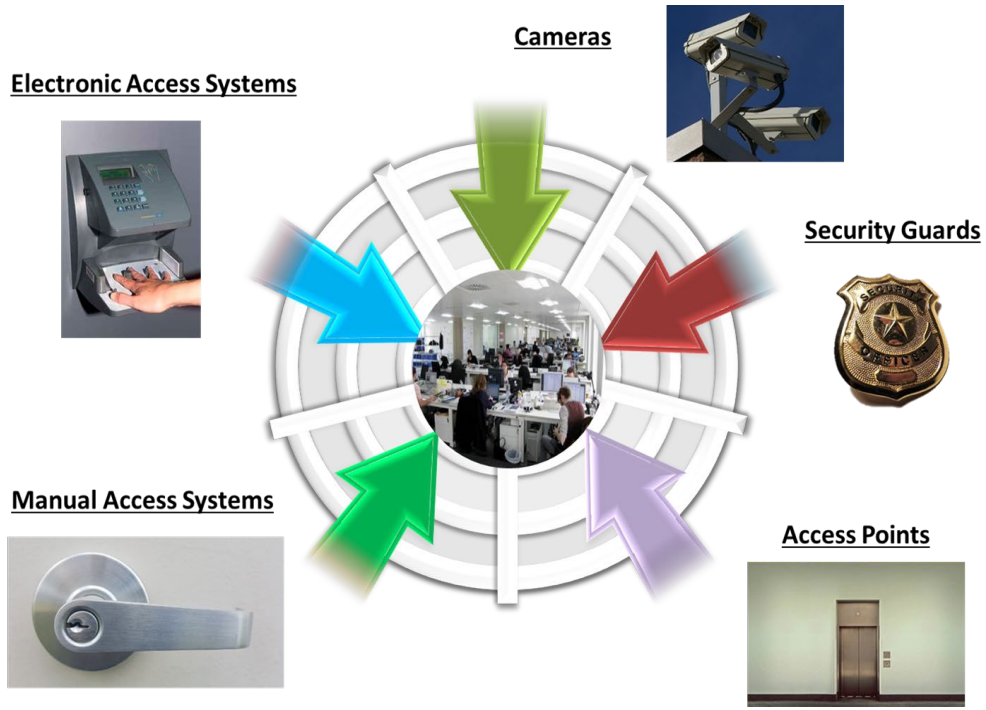


Abad Cabassa
November 5, 2026

Common Physical Security Vulnerabilities

Based on activities by CISA Protective Security Advisors:

- Lack of designated security manager.
- No written security, emergency management or business continuity plans.
  - Lack of access control & perimeter security
  - Suspicious package procedures
  - Mass notification procedures
  - Active Shooter procedures
  - Training and exercising
- Lack of alarm and video surveillance systems
- Missed opportunities to collaborate with Law Enforcement and Fusion Centers
- Lack of employee background and recurring checks
- Etc..



Additional Resources



Water ISAC:
Free for under 10,000 connections.
Contact Robert from MDC
rschwarm@themdc.com

How to Qualify

Key criteria to qualify for the Community Defense Program:

- US and Canada-based water, electric, and/or natural gas utility.
- Must not be owned by a parent company that exceeds $100 Million US in revenue.

Resource Links

https://www.cisa.gov/resources-tools/resources/considerations-critical-infrastructure-operators-working-third-party-ics-integrators

https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

https://www.cisa.gov/resources-tools/resources/cisa-learning

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

https://www.cisa.gov/resources-tools/services/malcolm

https://www.cisa.gov/resources-tools/resources/considerations-critical-infrastructure-operators-working-third-party-ics-integrators

https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

https://www.cisa.gov/about/regions/region-1

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

Checklist

- ❑ Establish a printed contact list containing internal and external contacts to use during an incident.
- ❑ Assess if your systems are directly connected to the internet. If so, assess the use of a VPN or disconnection.
- ❑ Assess if there are cloud services employed to support plant operations. If so, assess the risks.
- ❑ Establish routine assessments. Consider a cyber and physical security assessment from your local Security Advisors. Abad.Cabassa@CISA.DHS.GOV
- ❑ Streamline vulnerability discovery and cataloging. Consider signing up for CISA Cyber Hygiene (CyHy) scanning services.
- ❑ Develop an incident response plan DR / BC. Test it regularly.
- ❑ Assess the use and risks of default or shared credentials.
- ❑ Document and practice manual operations.
- ❑ Continuously assess if vendors and suppliers are meeting your cybersecurity goals and requirements.
- ❑ Establish communication with product vendors to learn of best practices.
- ❑ Assess supply chain risks.
- ❑ Ensure the workforce is well trained.
- ❑ Touch base with risk managers to review any applicable cyber insurance policies for capabilities and requirements.
- ❑ Maintain printed copies of all critical documents.

DEFEND TODAY,
SECURE TOMORROW

Cybersecurity Advisor for Connecticut

Abad Cabassa

Email: abad.cabassa@cisa.dhs.gov

Cell: (202) 880-5294

Protective Security Advisor for Connecticut

Mike Kowal

Email: michael.kowal@cisa.dhs.gov

Cell: (202) 431-3682