



AlphaGuardian™

OPERATIONAL TECHNOLOGY SECURITY MADE SIMPLE



Operational Technology (OT) Primer

Key Acronyms and Terms:

ICS (Industrial Control System)

SCADA (Supervisory Control and Data Acquisition)

PLC (Programmable Logic Controller)

VFD (Variable Frequency Drive)

DCS (Distributed Control System)

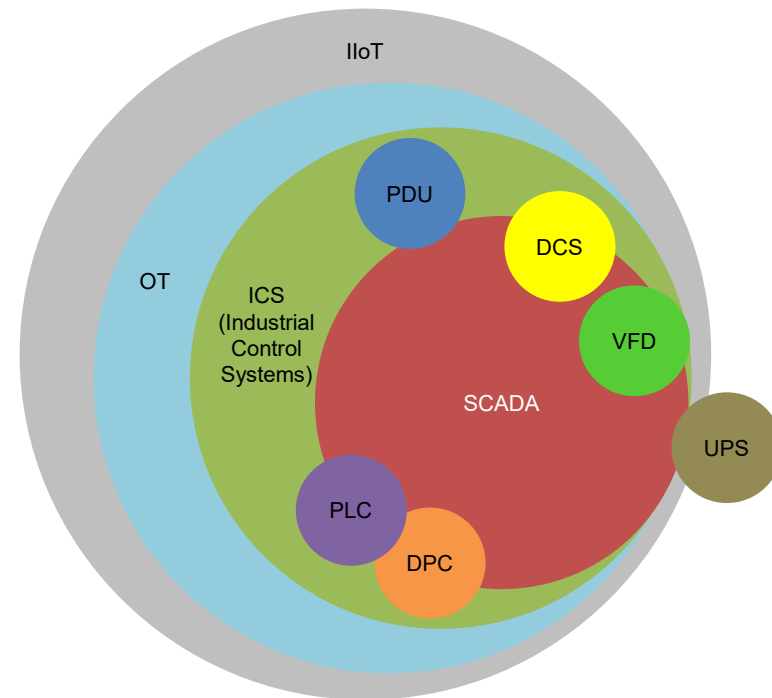
DPC (Discrete Process Control System)

UPS (Uninterruptable Power Supply)

PDU (Power Distribution Unit)

OT (Operational Technology)

IIoT (Industrial Internet of Things)





National Security Memorandum on Critical Infrastructure Security and Resilience

MAY 3, 2024 - This week, the White House released **National Security Memorandum 22 (NSM-22)** to secure and enhance the resilience of U.S. critical infrastructure from all hazards for generations to come. This is a crucial effort to strengthen and modernize U.S. risk management, including through engagement with international partners and allies.

The White House launched this whole-of-government effort to protect the President's investments in U.S. infrastructure in the face of threats from our adversaries, the changing climate, strategic competition, and supply chain shocks. Public-private collaboration is essential to this modernization effort, which also affirms a commitment to delivering minimum security and resilience standards for every critical infrastructure sector.

The Bureau of Counterterrorism is the Department's lead in the whole-of-government effort to counter terrorism abroad and to secure the United States against foreign terrorist threats. The Department of State is working to advance the objectives of the NSM through ongoing engagement, collaboration and capacity building efforts with foreign governments, and international organizations, to strengthen the security and resilience of critical infrastructure globally.

[White House Announcement](#)

[National Security Memorandum on Critical Infrastructure Security and Resilience](#)



EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation’s Drinking Water - May 20, 2024

WASHINGTON – Today, May 20, the U.S. Environmental Protection Agency issued an [enforcement alert](#) outlining the urgent cybersecurity threats and vulnerabilities to community drinking water systems...

... Today's alert emphasizes the importance of EPA’s ongoing inspection and enforcement activities under [Safe Drinking Water Act section 1433](#). The agency will increase the number of planned inspections and, where appropriate, will take civil and criminal enforcement actions, including in response to a situation that may present an imminent and substantial endangerment. Inspections will ensure that water systems are meeting their requirements to regularly assess resilience vulnerabilities, including cybersecurity, and to develop emergency response plans...

America's Water Infrastructure Act Section 2013: Risk and Resilience Assessments and Emergency Response Plans

On **October 23, 2018**, **America’s Water Infrastructure Act (AWIA)** was signed into law. AWIA Section 2013, which amended Section 1433 of the Safe Drinking Water Act (SDWA), requires community (drinking) water systems (CWSs) **servicing more than 3,300 people** to develop or update **risk and resilience assessments (RRAs)** and **emergency response plans (ERPs)**. The law specifies the components that the RRAs and ERPs must address, and establishes deadlines by which water systems must certify to EPA completion of the RRA and ERP. The [Federal Register Notice for New Risk Assessments and Emergency Response Plans for Community Water Systems](#) is available.

AWIA Section 2013 also states that EPA should provide guidance and technical assistance to water systems that serve less than 3,301 people on how to conduct RRAs and ERPs, though these systems are not required to certify completion to EPA.

Certification Deadlines

*ERP certifications are due six months from the date of the RRA certification. The dates shown above are certification dates based on a utility submitting a RRA on the final due date.

Population Served	Previous RRA Deadline	Next 5-Year Submission Cycle RRA Deadline
≥100,000	March 31, 2020	March 31, 2025
50,000-99,999	December 31, 2020	December 31, 2025
3,301-49,999	June 30, 2021	June 30, 2026

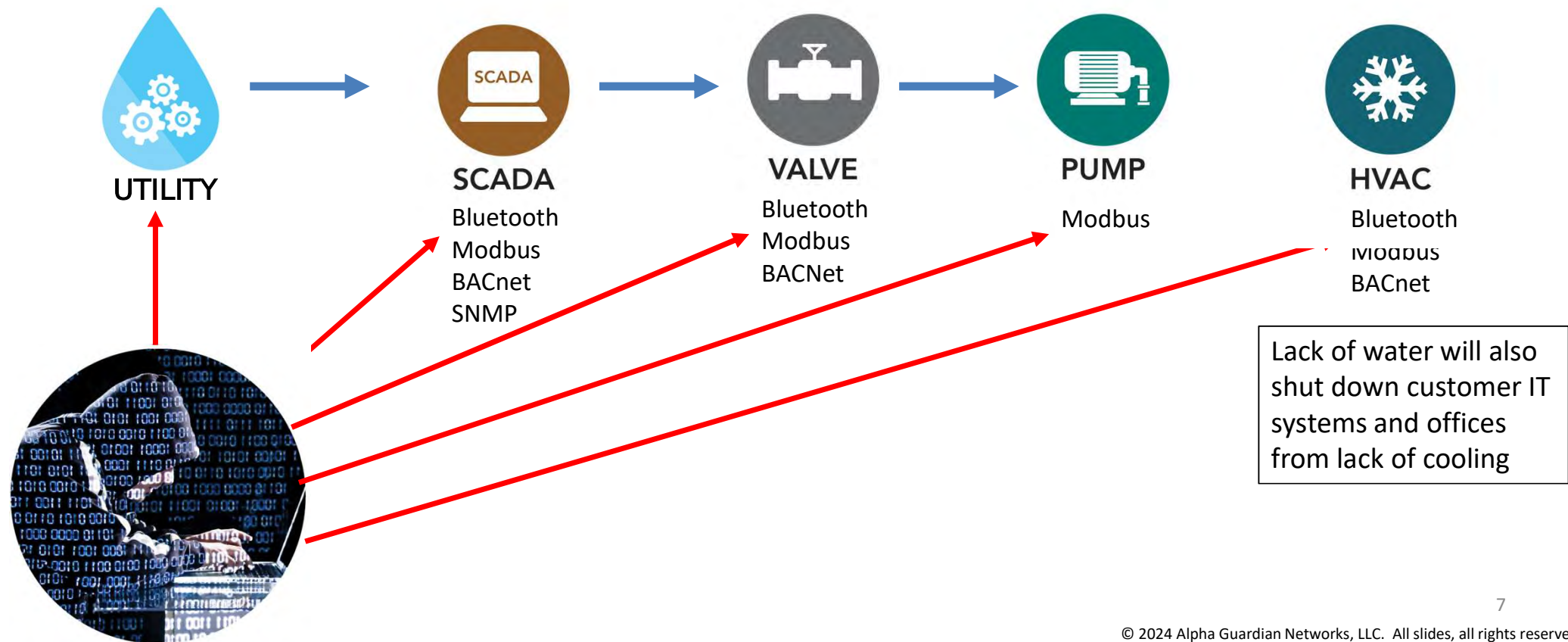
Population Served	Previous ERP Deadline*	Next 5-Year Submission Cycle ERP Deadline*
≥100,000	September 30, 2020	September 30, 2025
50,000-99,999	June 30, 2021	June 30, 2026
3,301-49,999	December 31, 2021	December 31, 2026

Part I Current Threat Landscape for Small U.S. Sites with SCADA, ICS, and/or OT

Scary Slides

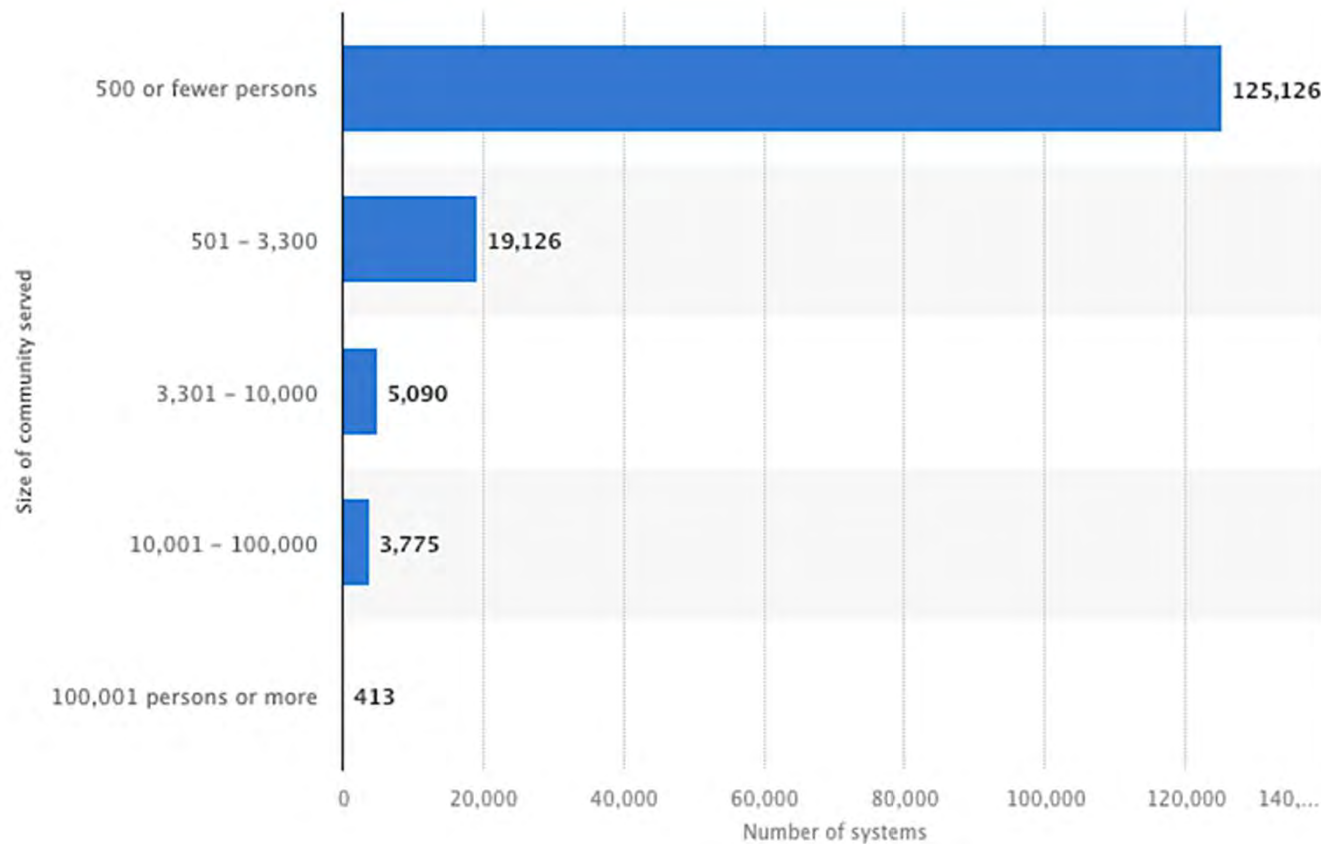
Water Supply Kill Chain For Water Systems

Shutting Down Water Can Kill Potable Water Use and Customer Cooling Systems As Well



Cyberattacks on Rural Water Systems Threaten the Country

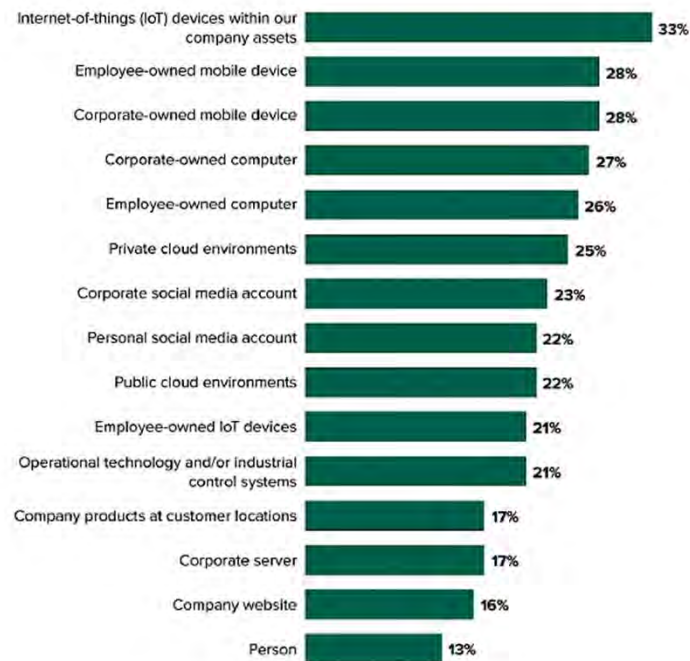
Rural Public Water Systems Make up About 95% of a Water Systems in the U.S.



Cyberattacks Use OT/IoT as a Major Source of Data Breaches

Data Breaches Use OT and IoT Systems as Part of a Multi-Staged Attack Sequence

"Which of the following was targeted as a part of this external attack?"
(Multiple responses accepted)



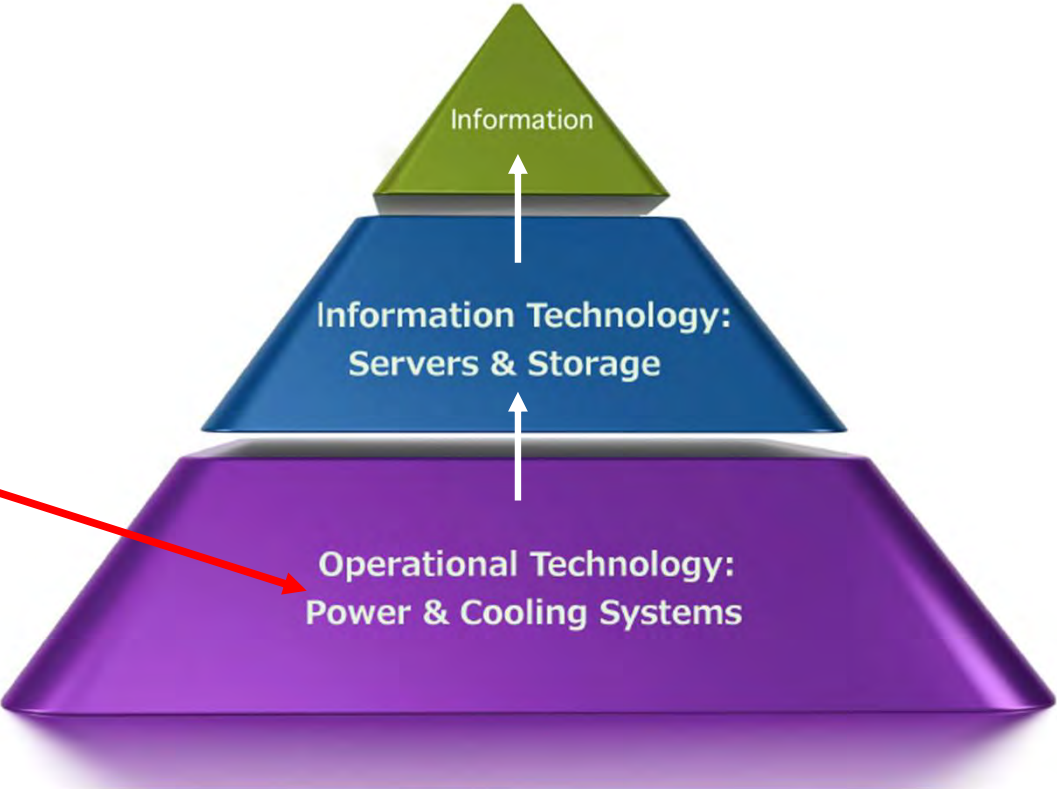
Base: 490 global security decision-makers with network, data center, app security, or security ops responsibilities who experienced an external attack when their company was breached
Source: Forrester's Security Survey, 2022

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

- **Vulnerable IoT:** "UPSs make up 55% of connected devices that are vulnerable to cyber security breaches. The need to review and update cyber protections is even more critical in the UPS management of distributed hybrid environments, which combine edge computing networks with the Internet of Things (IoT), on-premise infrastructure and multiple clouds" – [Schneider Electric APC blog July 1, 2021](#)
- "The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE) said they 'are aware of threat actors gaining access to a variety of internet-connected uninterruptable power supply (UPS) devices.'" – [ZDNet March 30, 2022](#)
- **Vulnerable Operational Technology:** Programmable Logic Controllers (PLC's) are ranked as the #1 most vulnerable target among OT systems
- "PLC cybersecurity isn't just an essential precaution, it has become a vital element...PLC's have never been designed with security in mind. Anyone with the skills and equipment could upload, download, delete or modify programs." [The Rising Important of PLC Cybersecurity – Engineering.com, July 19, 2023](#)

OT/IoT Cyberattacks Create a Path to IT Systems and Data

An attack on any critical OT/IoT unit gives a direct path to IT Systems and their Information



Threat Landscape – Public Water Systems

China, Russia & Iran Are Actively Targeting Critical Infrastructure

Water and All Critical Infrastructure Systems Are Targeted For Cyberattacks by Our Enemies

[2023 Annual Threat Assessment](#),
Office of Director of National Intelligence.



“China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. . . China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States...”

“...Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities” and that,“...Russia is particularly focused on improving its ability to target critical infrastructure.”

“Iran’s growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data. Iran’s opportunistic approach to cyber attacks makes critical infrastructure owners in the United States susceptible to being targeted...”

-

Water System Attacks Are Now Pervasive and Threaten Lives

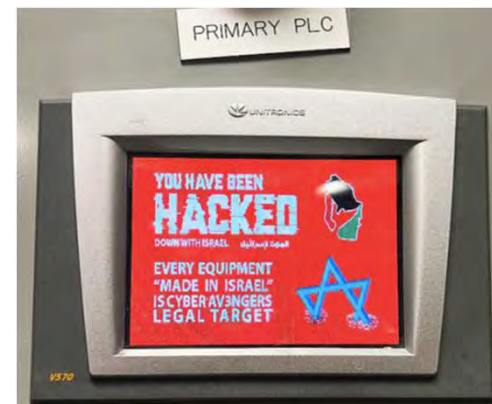
Russia Is Behind Most of the Latest Attacks and Their Latest Malware Is Life Threatening

- [May 2024, Wichita City Water & Other Systems Attacked](#) – Russian group attack on Municipal Services in Wichita, KS
- [April 2024, Indiana Water System Attacked](#) – Russian group attack on Tipton, IN water facility
- [January 2024, 3 West Texas Water Systems Attacked](#) – Russian attacks on Muleshoe, TX and 2 nearby water systems
- [December 2023, Attacks In Multiple States](#) - Iranian attacks on Aliquippa, PA and sites in multiple states.
- [November 2023, Multiple Sites in North/East Dallas](#) - Russian- affiliated attack on multiple systems north of Dallas, TX

Tipton, Indiana SCADA system shutdown by Russia



Aliquippa, Pennsylvania PLC Takeover by Iran



Water System Attacks Are Now Pervasive and Threaten Lives

Most Water Systems Are Poorly Secured

Recent cyber attacks on water systems in the US focus on poorly secured sites of all sizes:

- [October 2024, Camden, NJ Water System Hacked](#) – “...currently unable to predict the full impact.”
- [September 2024, Kansas Water System Attack](#) - Ransomware attack on rural Kansas water system
- [May 2024, Wichita, KS Water System Attacked](#) – City given ~10 days to pay ransom or have personal info. leaked
- [May 2024 KC, MO Cyberattack Still a Mystery](#) -Water payment, other services down, stolen data found on dark web
- [April 2024, Indiana Water System Attacked](#) – Russian group attack on Tipton, IN water facility
- [January 2024, 3 West Texas Water Systems Attacked](#) – Russian attacks on Muleshoe, TX and 2 nearby water systems
- [December 2023, Attacks In Multiple States](#) - Iranian attacks on Aliquippa, PA and other sites in multiple states.
- [November 2023, Multiple Sites in North/East Dallas](#)- Russian- affiliated attack on multiple systems north of Dallas, TX
- [July 2023, Discovery Bay, CA](#) – SF Bay Area water treatment facility was remotely disabled by Chinese-paid infiltrator

[May 20, 2024 EPA Water System Cybersecurity Bulletin:](#)

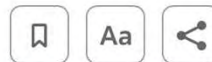
[70 percent of all U.S. water systems do not fully comply with requirements in the Safe Drinking Water Act and some have critical cybersecurity vulnerabilities, such as default passwords that have not been updated and single logins that can easily be compromised.](#)

Technology

US disrupts Chinese hacking campaign targeting critical infrastructure, officials say

By Zeba Siddiqui

January 31, 2024 1:24 PM PST · Updated 5 days ago



Jan 31 (Reuters) - U.S. officials said on Wednesday they disrupted a sweeping Chinese cyber-spying operation that targeted critical American infrastructure entities and could be used against the United

<https://www.reuters.com/technology/us-disrupts-chinese-botnet-targeting-critical-infrastructure-fbi-says-2024-01-31/>

Some Good News...
January 31, 2024:

"This operation disrupted the efforts of (People's Republic of China) state-sponsored hackers to gain access to U.S. critical infrastructure that (China) would be able to leverage during a future crisis"

-Assistant Attorney General Matthew Olsen of the Justice Department's National Security Division said in a statement.

This Trick is No Treat

[Flipper Zero](#) is a wireless hacking device that can find the pairing code to any Bluetooth Device and can find the SSID code to any Wi-Fi Device.

More IoT/OT devices are using Bluetooth and Wi-Fi, allowing a malicious actor to access any Bluetooth or Wi-Fi device on your network and then backtrack into your Ethernet network – with no authentication.

With a long distance antenna, Bluetooth has been hacked from 1.5 miles and Wi-Fi from over 3 miles. There is no need for to be close to your site to attack your systems.

Knowing what traffic is on your network at all times is the key to stopping the attackers.



Why Are OT/IoT Devices So Vulnerable?

All the Most Common OT/IoT Protocols Still Fail to Meet Security Standards

- **Modbus:**

“The Modbus protocol lacks the ability to authenticate a user and hence middle-man attacks can easily take place in Modbus” – California Energy Commission

Adding a secure Transport Layer Secure (TLS) option to Modbus is helpful but, it is not backward compatible.
- **BACnet:**

“BACnet secure brings cybersecurity and IT-acceptant to Operational Technology (OT) networks. It adds a secure communications layer and requires device authentication using certificates...Older BACnet devices will not meet the significant computing resource requirements needed to make them compatible with a firmware update to BACnet.” - Siemens
- **SNMP:**

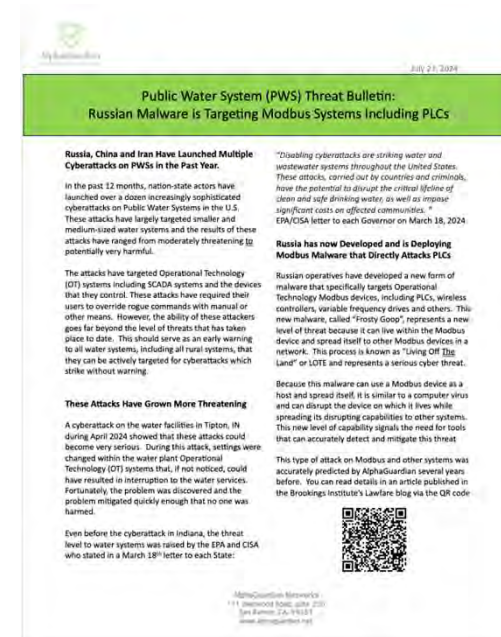
“When either SNMPv1 or SNMPv2 are employed, an adversary could sniff network traffic to determine the community string. This compromise could enable a man-in-the-middle or replay attack. - CISA

“SNMPv3 fails to provide its advertised security guarantees...These vulnerabilities are implementation agnostic and demonstrate a fundamental flaw in the current protocol” Dr. Patrick Traynor

New ICS Malware Targeting Critical Infrastructure

7/23/2024 – The Hacker News

- We now have proof of a very destructive strain of malware that was purpose-built just for Modbus systems.
- It has the capability of living on its own (Living Off The Land LOTL) within a Modbus device
- It can travel between itself and any other Modbus device and can infect and cause harm to other Modbus devices in a network
- It is being actively used in critical infrastructure sites to wreak havoc



"...this malware can potentially disrupt operations in all industrial sectors by affecting legacy and modern systems."

Russia Has Now Launched The Most Destructive OT Malware

Russia's Frosty Goop Malware Specifically Targets Modbus Devices, The Heart of Water Systems

- [July 2024, Russians deploying Modbus specific malware to shut down critical utilities in Ukraine.](#)
- This malware can be used to target any Modbus system in any mission critical facility to shut it down instantly.
- Water systems rely on Modbus-based systems such as Programmable Logic Controllers (PLCs), Valves, etc.

```
TCP 66 49374 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49374 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49374 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 66 Query: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
Nodbus_ 73 Response: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
TCP 66 49375 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49375 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49375 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 66 Query: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
Nodbus_ 83 Response: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
TCP 66 49376 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49376 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49376 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 66 Query: Trans: 1; Unit: 254, Func: 6: Write Single Register
Nodbus_ 66 Response: Trans: 1; Unit: 254, Func: 6: Write Single Register
TCP 66 49377 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49377 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49377 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 87 Query: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
Nodbus_ 66 Response: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
```

Malware reads monitoring data from Modbus Registers to surveil the system conditions

Malware then writes commands to Modbus Registers to shut-off systems

Programmable Logic Controllers Are Easy to Attack

Operational Technology Protocols Have Little Security and Actually Broadcast Their Presence

[REDACTED] 186
Water
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: 19 [REDACTED]

[REDACTED] 9.167
City of Danville
United States, Danville

SNMP:
Uptime: 237171660
Description: **Siemens**, SIMATIC NET, SCALANCE W734-1 RJ45
Service: 72
Versions:
1
3
Name: sysName Not Set
Ordescr: **SIEMENS** - AUTOMATION-SYSTEM-MIB
Engineid Format: octets
Contact:...

[REDACTED] .91
4.myvzw.co
Service Provider Corporation
United States, Franconia

ICS

Ladder Logic Runtime: ProCon0S V4.0.0332 Jun 27 2008
PLC Type: Bristol: CWM V04:92:00 06/27
Project Name: DDISON_CM
Boot Project:
Project Source Code: ADDISON_CM

[REDACTED] 9.123
119.myvzw.c
om
Service Provider Corporation
United States, Chicago

ICS

Unitronics PCOM:
Model: V1210
Hardware Version: A
OS Version: 4.11
OS Build: 2
UID Master: 1
PLC Name: OPTIPUMP
PLC Unique ID: 15477338

SCADA Systems Are Easy Attack

System Control And Data Acquisition Systems in Public Water Systems Are Easy to Find and Attack

173.19
rrcs-173-1
om
CITY OF L
United
ics

Instance ID: 99
Object Name: Compass_99
Location: unknown
Vendor Name: Alerton
Application Software: 1.5.20160627.0 - BACnet: **Tridium** 3.8.38.6
Firmware: 3.8.39
Model Name: Compass
Description: Compass NBT - Internal BACnet device

49.88.142
88-142.machlink.com
e Power and Water
United States, Muscatine

HTTP/1.1 200 OK
Server: HTTP - Reliable **Controls** Embedded Web Server
Connection: close
Content-encoding: gzip
Cache-Control: max-age=20, must-revalidate
ETag: "000003efe205180e221a"
Content-Type: text/html; charset=utf-8
Content-Length: 1007

gin
.49.32
Carthage Water and Electric
United States, Carthage

HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
connection: close
server: **Niagara** Web Server/1.1

Which of these devices do you have (and what communication protocol are they using)?

SCADA (Supervisory Control and Data Acquisition)

PLC (Programmable Logic Controller)

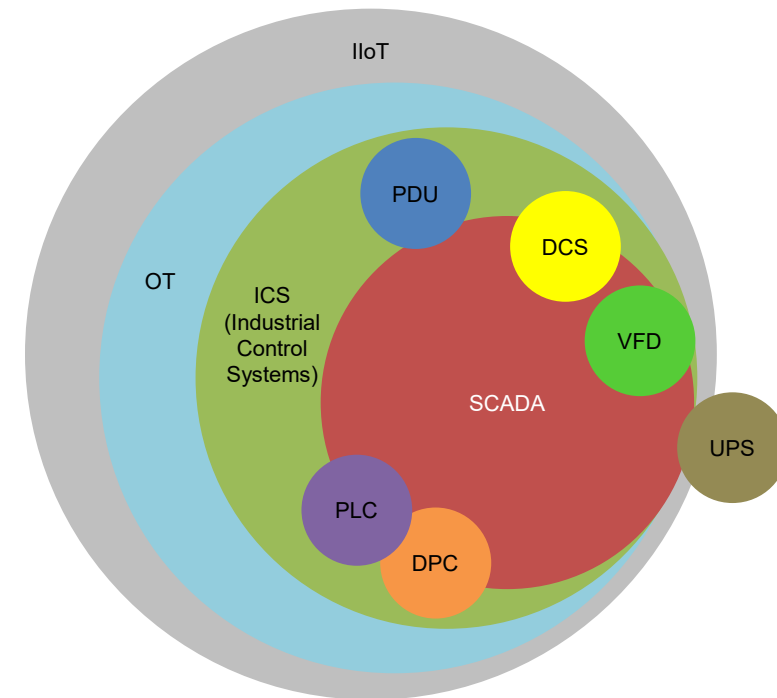
VFD (Variable Frequency Drive)

DCS (Distributed Control System)

DPC (Discrete Process Control System)

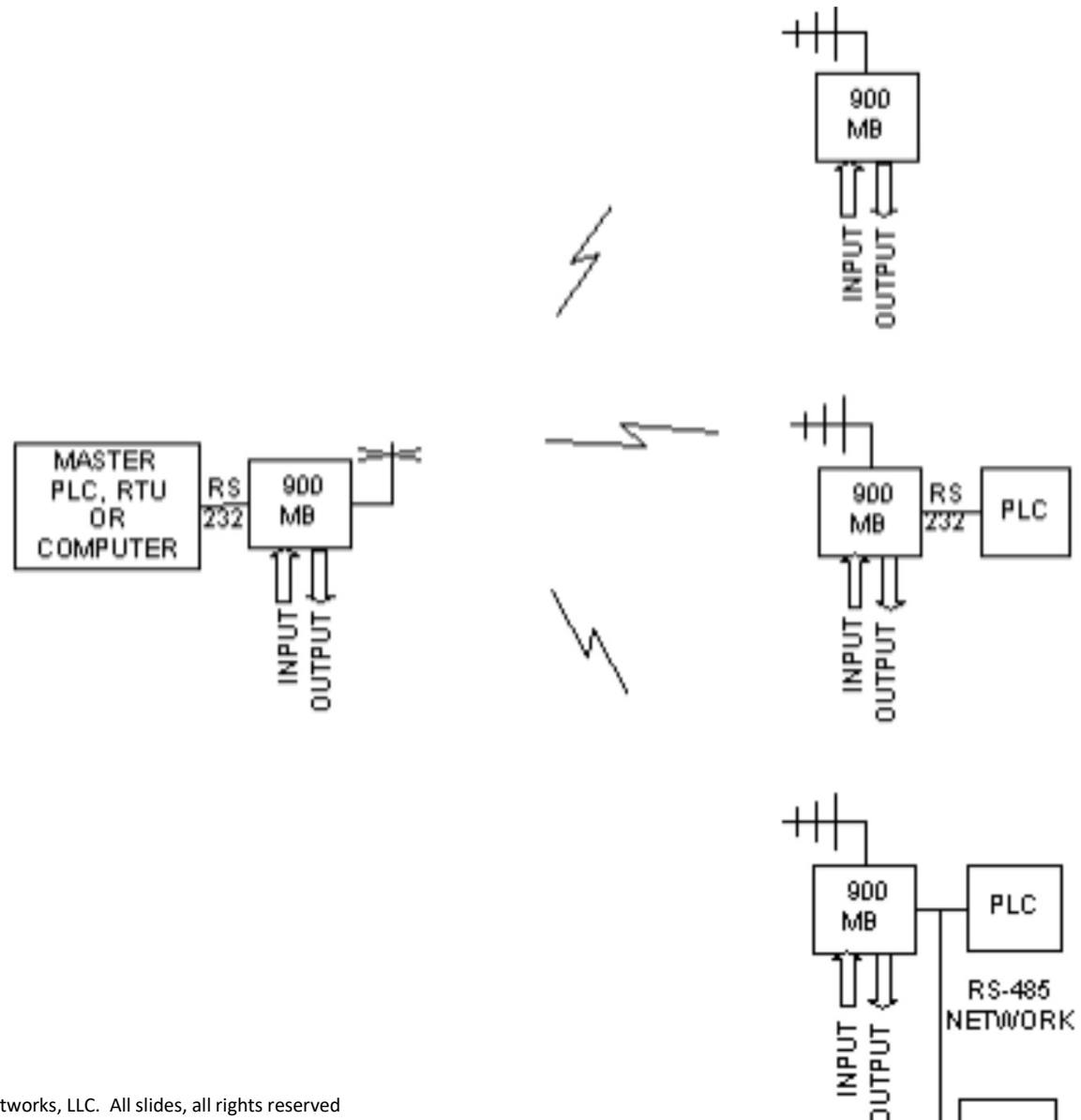
UPS (Uninterruptable Power Supply)

PDU (Power Distribution Unit)



Is Radio Communication Safe?

- It Depends



Newly Discovered Threat with Unsecured Wireless Devices

Site Using Site Radar OT Cyber Threat Discovery & Response Discovered Severe Flaws With Multiple Brands of Wireless Controllers

66.172.1.100
Northwest
Unit
ics

Product name: 1766-L32AWA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60d6023a
Device type: Programmable Logic Controller
Device IP: 192.168.1.4

Banner Engineering

66.172.1.100
Northwest
Unit
ics

HTTP/1.0 200 OK
Content-type: text/html



66.172.1.100
Northwest
Unit
ics

Manufacturer: Red Lion Controls
Model: CR3000-07000

“A username and password will be sent when logging into the webserver if the user defines the DXM Controller to use authentication. See the DXM Configuration Tool documentation to set up the authentication...The username and password authentication use the facilities of the HTTP protocol.” – [Banner DMX Wireless Controller API Manual](#)

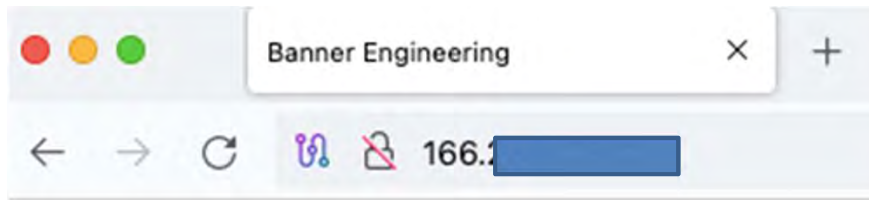
Banner Engineering ScriptBasic

```
193  
194 'Get GPS satellite info, PRN, Elevation, Azimuth, Signal Strength.  
195 = FUNCTION GetGPS_SatelliteInfo  
196 LOCAL x, y, NumOfSatellites, SatInfo  
197 NumOfSatellites = GETREG(GPS_NumSatellites_reg, ModSID, HoldingReg)  
198  
199 = IF NumOfSatellites > 12 THEN  
200   NumOfSatellites = 0  
201 END IF  
202 PRINT "\n\nSatellite Info: Number of Satellites being tracked :", NumOfSatellites, "\n\n"  
203 WrErr = SETREG (SatDataStart, NumOfSatellites, LocalReg, HoldingReg)  
204  
205 = FOR x = 1 to NumOfSatellites  
206   RdErr = MULTIGET(Sat_PRN_reg[x, 1], 8, ModSID, HoldingReg)  
207   SatInfo[x, 1] = MBREGIN(0)  
208   SatInfo[x, 2] = MBREGIN(2)  
209   SatInfo[x, 3] = MBREGIN(4)  
210   SatInfo[x, 4] = MBREGIN(6)  
211 NEXT x  
212 = FOR x = 1 to NumOfSatellites  
213   PRINT "\t PRN:", SatInfo[x, 1], "\t Elev:", SatInfo[x, 2], "\t Azim:", SatInfo[x, 3], "\t SignalStr:", SatInfo[x, 4], "\n\n"  
214 NEXT x
```


With a quick search, we were able to quickly find Banner units (about 20) online via the Censys browser. While their name makes them difficult to sort out because using the name “Banner” in the Shodan or other searches tends to bring up web banners, we did find a few.

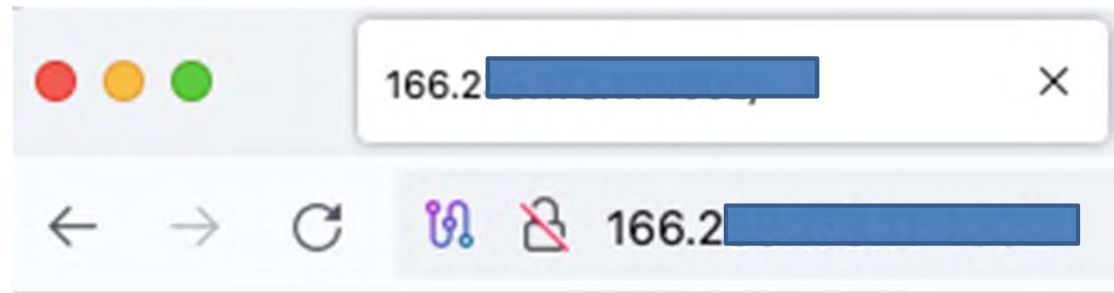
All had port 80 wide open and several showed a serial port (ASY port in SCADA code lingo) in use, which appeared to be tied to the wireless port for the unit. In short, you could penetrate these units both from the wireless side (if you had the tools) and the Ethernet side via the Internet.

Its quite simple.



Welcome!

Hello and welcome to the Banner Engineering gateway!



ASY Port 2 in use by MODEM

How About Cellular Modems?

“Security flaws in Telit Cinterion cellular modems, widely used in sectors including industrial, healthcare, and telecommunications, could allow remote attackers to execute arbitrary code via SMS.”

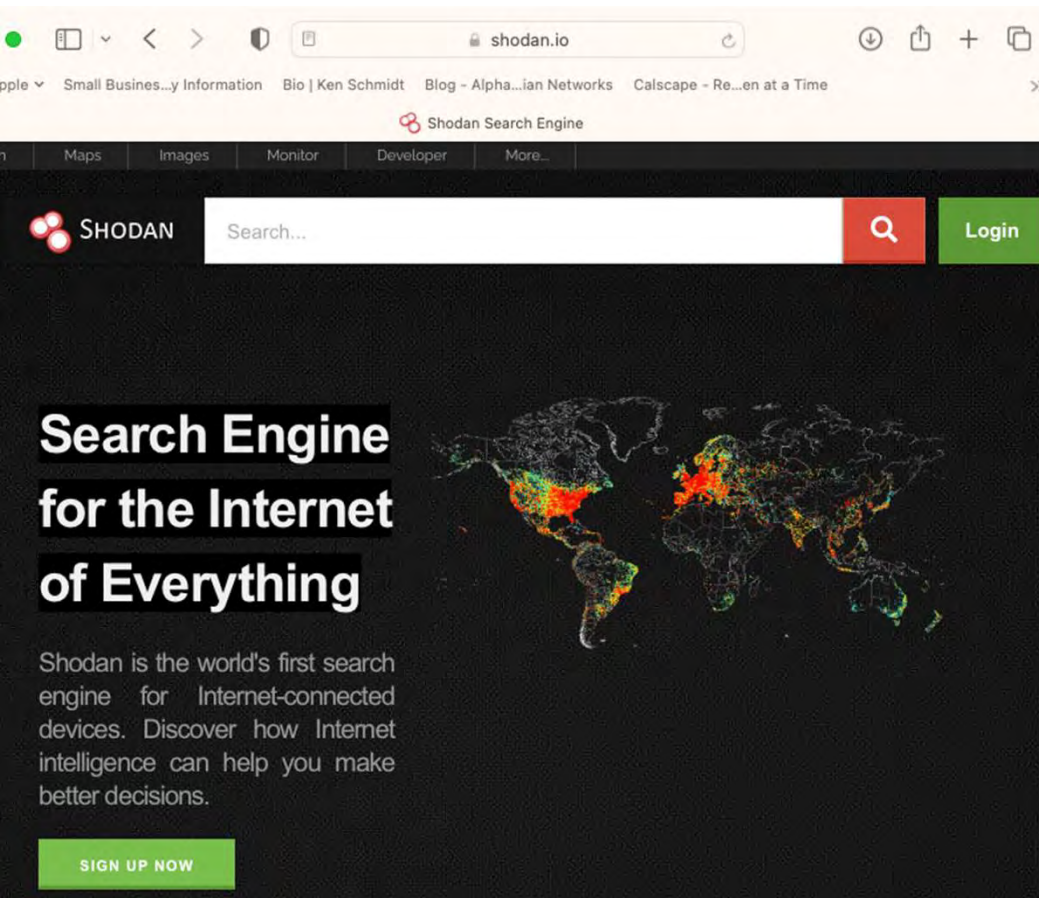
“...a threat actor could exploit them to take control of vulnerable Telit Cinterion devices.”

Is Radio Communication Safe?

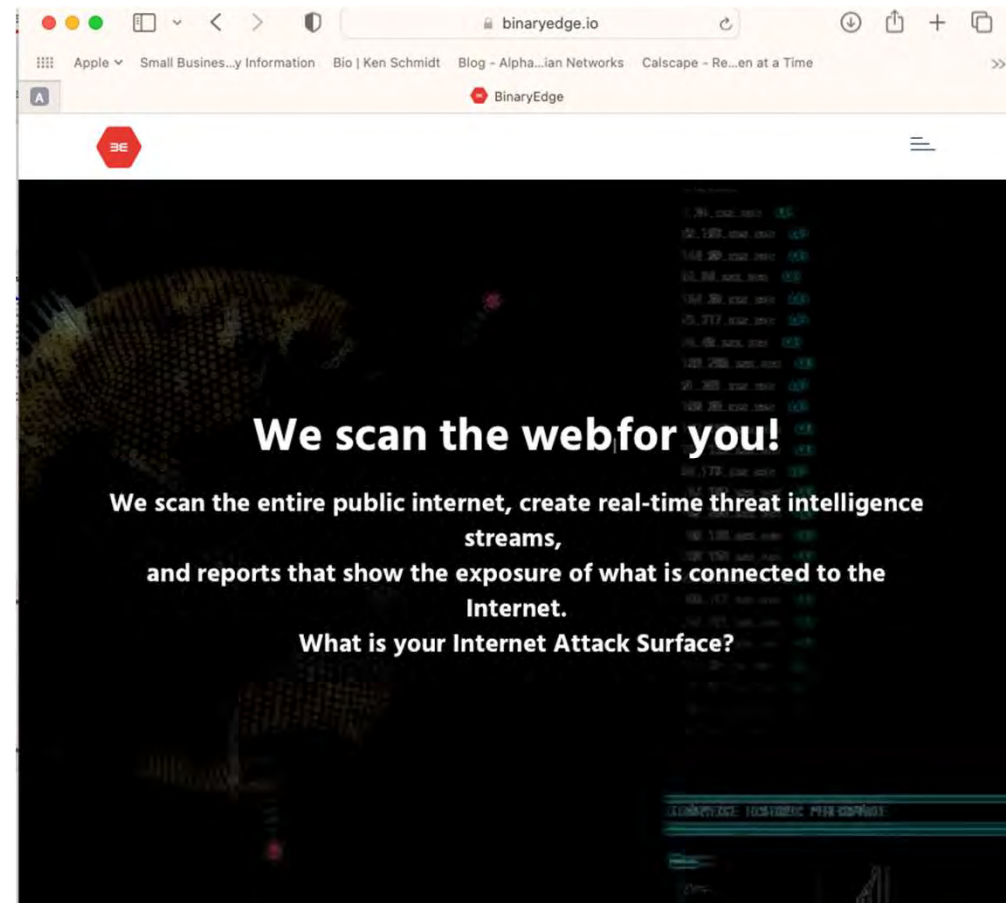
- It Depends
 - Find out if your wireless radios have been hacked
 - Find out if your radio communications use encryption (and which level of encryption)
 - Look into upgrades and alternatives for current radio communication

Individual OT Devices Are Also Easy To Discover And Attack

OT Protocols Broadcast Their Presence, Making Them Easy to Find and Attack



The screenshot shows the homepage of Shodan Search Engine. The browser address bar displays "shodan.io". The page features a search bar with the text "SHODAN" on the left, "Search..." in the center, a magnifying glass icon on the right, and a green "Login" button. Below the search bar is a world map with various regions highlighted in red, orange, and yellow, indicating discovered devices. The main heading reads "Search Engine for the Internet of Everything". A sub-heading states: "Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions." A green "SIGN UP NOW" button is located at the bottom left.



The screenshot shows the homepage of BinaryEdge. The browser address bar displays "binaryedge.io". The page features a dark background with a large, stylized fish-like graphic. The main heading reads "We scan the web for you!". Below this, the text states: "We scan the entire public internet, create real-time threat intelligence streams, and reports that show the exposure of what is connected to the Internet. What is your Internet Attack Surface?". The background also shows a list of IP addresses and their associated data, such as "192.168.1.1" and "192.168.1.2".

Individual OT Devices Are Also Easy To Discover And Attack

OT Protocols Broadcast Their Presence, Making Them Easy to Find and Attack

206.214.122.186

Mayfield Electric & Water
Systems

 United States, Mayfield

ICS

Product name: 1766-L32BAAA B/15.04
Vendor ID: **Rockwell** Automation/Allen-Bradley
Serial number: 0x4064ffba
Device type: Programmable Logic Controller
Device IP: 192.168.10.199

 **69.49.88.142** 

machnet-88-142.machlink.com
Muscatine Power and Water

 United States, Muscatine

```
HTTP/1.1 200 OK
Server: HTTP - Reliable Controls Embedded Web Server
Connection: close
Content-encoding: gzip
Cache-Control: max-age=20, must-revalidate
ETag: "000003efe205180e221a"
Content-Type: text/html; charset=utf-8
Content-Length: 1007
```

12.138.200.155

CURRY WATER AUTHORITY
INC

 United States, Moody

ICS

Product name: 1769-L36ERM/A LOGIX5336ERM
Vendor ID: **Rockwell** Automation/Allen-Bradley
Serial number: 0xd02f40e1
Device type: Programmable Logic Controller
Device IP: 192.168.4.13

 **Login** 

162.249.49.32
Carthage Water and Electric

 United States, Carthage

```
HTTP/1.1 200 OK
content-type: text/html; charset=UTF-8
connection: close
server: Niagara Web Server/1.1
```

Firewalls Alone Are NOT Enough

Firewalls are Often Misconfigured and Actually Invite Cyberattacks While Giving False Sense of Security

66.211.16.100

host-66-211-16-100.cpws.net
Columbia Power and Water
Systems
United States, Columbia

Check Point **Firewall:**
Firewall Host: CPFirewall02
SmartCenter Host: CPManage.trh.com

209.152.146.84

Marshall Municipal Utilities
United States, St. Louis

Check Point **Firewall:**
Firewall Host: BPUS006NEF002
SmartCenter Host: UZNEF001-DMS-ITST01

 **SonicWall - Authentication** 

64.60.196.186
64-60-196-186.static-ip.telepacif
ic.net
Central Basin Municipal Water
United States, Fullerton

HTTP/1.0 200 OK
Server: **SonicWALL**
Expires: -1
Cache-Control: no-cache
Content-type: text/html; charset=UTF-8;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' 'unsafe-inli

 **DELL SonicWALL - Authentication** 

66.207.1.107
mpw-1-107.machlink.com
Muscatine Power and Water
United States, Muscatine

HTTP/1.0 200 OK
Server: **SonicWALL**
Expires: -1
Cache-Control: no-cache
Content-type: text/html; charset=UTF-8;

Dell **SonicWALL:**
SonicOS Version: 5.x
Serial Number: C0EAE4526740

CISA Releases Three Industrial Control

CISA <CISA@messages.cisa.gov> to me



You are subscribed to Industrial Control Security Agency. This information has re

[CISA Releases Three Industrial](#)

10/31/2023 08:00 AM EDT

CISA released three Industrial Control System information about current security issues

- ICSA-23-304-02 [INEA ME RTU](#)
- ICSA-23-304-03 [Zavio IP Cam](#)
- ICSA-23-208-03 [Mitsubishi Ele](#)

CISA encourages users and administrative mitigations.

This product is provided subject to this [N](#)

Having tro

You are subscribed to updates from the [Cybersecurity and Infrastructure Security Agency](#) (CISA)

Filters

What are you looking for?

Sort by (optional)

Release Date

APPLY

Advisory Type

- ICS Advisory
- ICS Alert

Release Year

Vendor

- Schneider Electric (148)
- Siemens (633)
- Rockwell Automation (122)
- Advantech (81)
- Mitsubishi Electric (75)
- Other (54)
- Moxa (53)
- GE (52)
- Delta Electronics (51)
- Hitachi Energy (42)
- ABB (41)

Cybersecurity Alerts & Advisories

[View Cybersecurity Advisories Only](#)

[View Advisory Definitions](#)

Filters: ICS Advisory X ICS Alert X Schneider Electric X

Clear all filters

DEC 13, 2022 ■ ICS ADVISORY | ICSA-22-347-02

[Schneider Electric APC Easy UPS Online](#)

AUG 11, 2022 ■ ICS ADVISORY | ICSA-22-223-03

[Schneider Electric EcoStruxure, EcoStruxure Process Expert, SCADAPack RemoteConnect for x70](#)

JUL 12, 2022 ■ ICS ADVISORY | ICSA-22-055-03

[Schneider Electric Easergy P5 and P3 \(Update A\)](#)

MAR 31, 2022 ■ ICS ADVISORY | ICSA-22-090-01

[Schneider Electric SCADAPack Workbench](#)

FEB 15, 2022 ■ ICS ADVISORY | ICSA-22-046-01

[Schneider Electric IGSS](#)

DEC 21, 2021 ■ ICS ADVISORY | ICSA-21-348-02

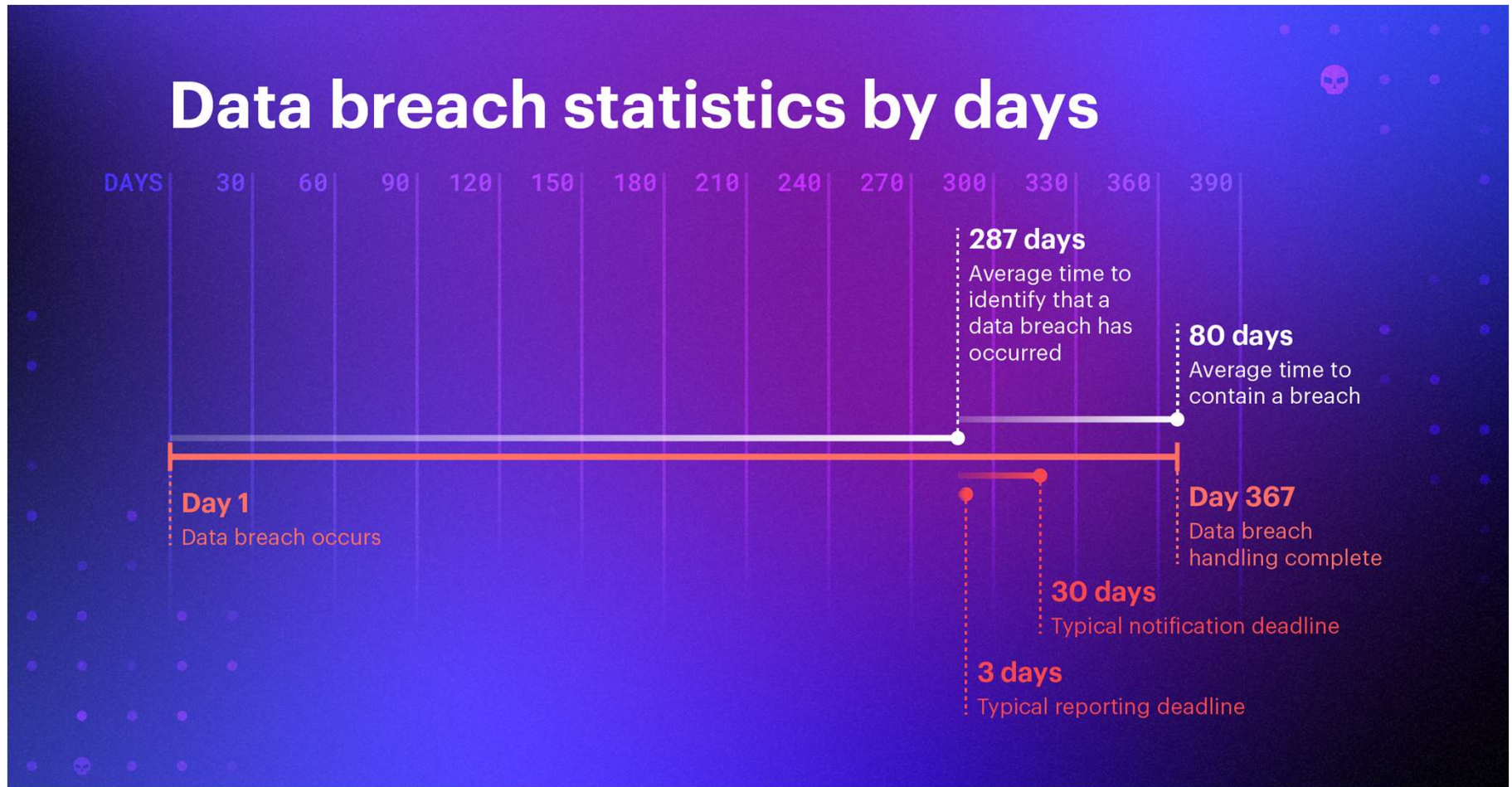
[Schneider Electric Rack PDU \(Update A\)](#)

DEC 02, 2021 ■ ICS ADVISORY | ICSA-21-336-01

Some Good News...

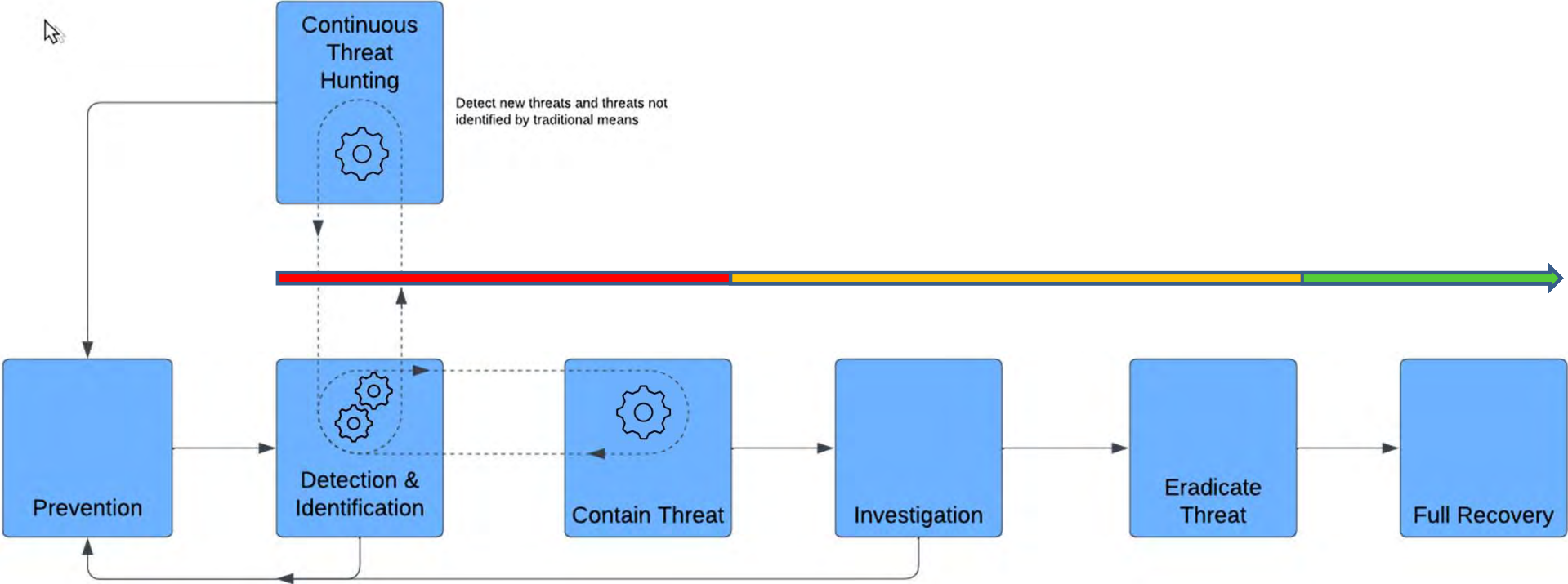
If You Have Visibility,
You Can Know About a New Attack...

The Faster You Know About a New Attack, the Better

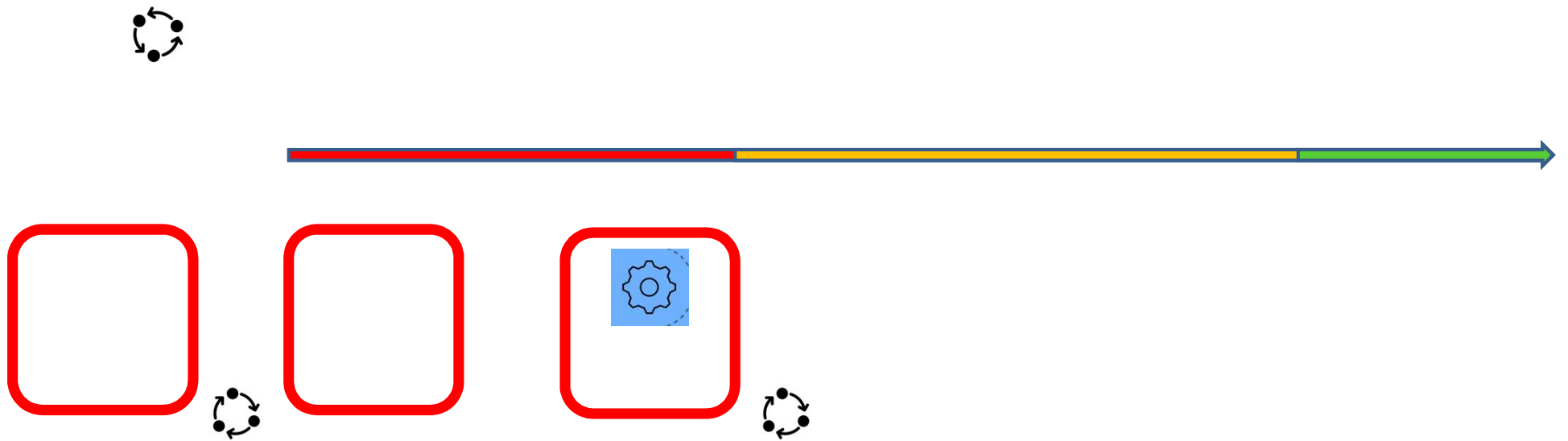


Source: <https://www.varonis.com/blog/data-breach-statistics>

“Dwell Time”



Hunt, Contain, Eradicate



Continuously Improve Prevention (and Hunting)

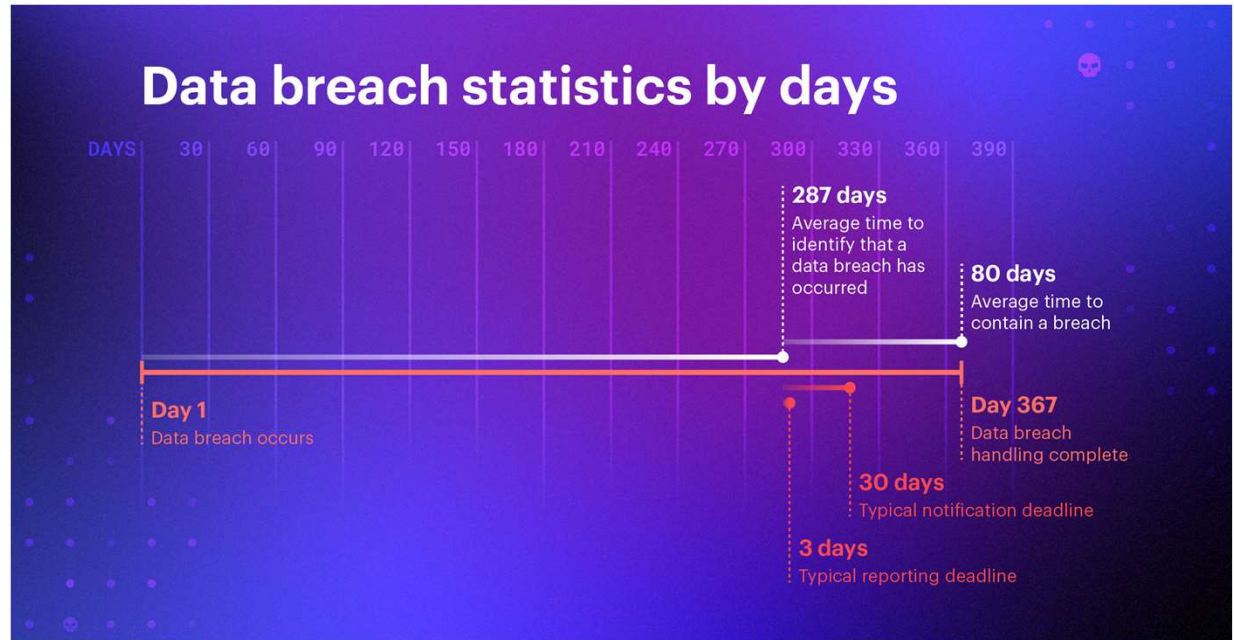
China, Russia & Iran Are Actively Targeting Critical Infrastructure

“China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. . . China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States...”

→ Some, perhaps most, cyber attacks on OT from the PRC (People’s Republic of China) are about gaining operational control capability, for use at a later date.

Infiltrate → Gain Operational Control Capability → Hide Your Presence → ???

[2023 Annual Threat Assessment](#),
Office of Director of National Intelligence.



You Can't Fight What You Can't See and Understand

Giving Users Clear Visibility of OT Network Problems and Potential Attacks Is Job # 1

“Threat hunting is important because sophisticated threats can get past automated cybersecurity. Although automated security tools...should be able to deal with roughly 80% of threats, you still need to worry about the remaining 20%.

Given enough time and resources, they will break into any network and avoid detection for up to 280 days on average. Effective threat hunting helps reduce the time from intrusion to discovery, reducing the amount of damage done by attackers.

Attackers often lurk for weeks, or even months, before discovery. They wait patiently to siphon off data and uncover enough confidential information or credentials to unlock further access, setting the stage for a significant data breach.”

○ - IBM



CISA Knows These Problems and Is a Great Resource

The Cybersecurity and Infrastructure Security Agency Is Focused on IoT/OT Security Problems

The screenshot shows the CISA website's "Cybersecurity Alerts & Advisories" page. At the top left is the CISA logo and the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and "AMERICA'S CYBER DEFENSE AGENCY". To the right is a search bar. Below the header is a navigation menu with "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". A red button labeled "REPORT A CYBER ISSUE" is on the right. Below the navigation is a breadcrumb trail "Home / News & Events" and social media share icons for Facebook, Twitter, LinkedIn, and Email. The main content area has a "Filters" section on the left with a search box, a "Sort by (optional)" dropdown set to "Release Date", and an "APPLY" button. The main heading is "Cybersecurity Alerts & Advisories". Below it are links for "View Cybersecurity Advisories Only" and "View Advisory Definitions". The "Filters" section shows "ICS Advisory" and "ICS Alert" as active filters, with a "Clear all filters" button.

https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95&f%5B1%5D=advisory_type%3A97

CISA: Free Cybersecurity Services and Tools:

<https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools>

**PART II: How Small PWSs can Defend
Themselves While Also Affordably Addressing
Current and Future Government Compliance**

CISA

CISA's Free Cyber Vulnerability Scanning for Water Utilities

<https://www.wtrinfo.gov/resources/tools/resources/cisa-free-cyber-vulnerability-scanning-water-utilities>



FREE CYBER VULNERABILITY SCANNING FOR WATER UTILITIES

WATER SECTOR COORDINATING COUNCIL



OVERVIEW

Drinking water and wastewater systems are an essential community lifeline. It is important to protect your system from cyberattacks to maintain its vital operations. You can reduce the risk of a cyberattack at your utility by externally scanning your networks for vulnerabilities caused by publicly facing devices. The Cybersecurity and Infrastructure Security Agency (CISA) can help your drinking water and wastewater system identify and address vulnerabilities with a no cost [vulnerability scanning service](#) subscription. CISA, the Water Sector Coordinating Council, and the Association of State Drinking Water Administrators encourage drinking water and wastewater utilities to use this service.

BENEFITS

CISA's vulnerability scanning can help your utility identify and address cybersecurity weaknesses that an attacker could use to impact your system. The benefits of this service include:

- Identifying internet-accessible assets
- Identifying vulnerabilities in your utility's assets connected to the internet, including [Known Exploited Vulnerabilities](#) and internet-exposed services commonly used for initial access by threat actors and some ransomware gangs
- Weekly reports on scanning status and recommendations for mitigating identified vulnerabilities
- Significant reduction in identified vulnerabilities in the first few months of scanning for newly enrolled water utilities
- Ongoing detection and reporting with continuous scanning for new vulnerabilities



HOW DOES IT WORK?

CISA uses automated tools to conduct vulnerability scanning on your external networks. These tools look for vulnerabilities and weak configurations that adversaries could use to conduct a cyberattack. CISA's scanning provides an

cisa.gov | central@cisa.dhs.gov | @CISAgov | @CISACyber | cisa.gov | As of August 24, 2023

Free Cyber Vulnerability Scanning for Water Utilities

external, non-intrusive review of internet-accessible systems. The scanning does not reach your private network and cannot make any changes. CISA will send you weekly reports with information on known vulnerabilities found on your internet-accessible assets, week-to-week comparisons, and recommended mitigations. Figure 1 shows an example of the Report Card included in the weekly report. You will also receive ad-hoc alerts for any urgent findings.

CISA does not share any attributable information without written and agreed consent from the stakeholder. CISA summarizes aggregate, anonymized data to develop non-attributable reports for analysis purposes. Figure 2 summarizes the phases in CISA's vulnerability scanning enrollment.

Pre-Planning	Planning	Execution	Reporting
Stakeholder: <ul style="list-style-type: none"> Requests vulnerability scanning service Signs and returns documents 	Stakeholder: <ul style="list-style-type: none"> Provides target list (scope) 	CISA: <ul style="list-style-type: none"> Performs initial scan of submitted scope Rescans stakeholder's target list at the following intervals based on highest severity of identified vulnerabilities: <ul style="list-style-type: none"> ⇒ 12 hours for "critical" and "known exploited" ⇒ 24 hours for "high" ⇒ 4 days for "medium" ⇒ 6 days for "low" ⇒ 7 days for "no vulnerabilities" 	CISA: <ul style="list-style-type: none"> Sends ad-hoc alerts within 24 hours of detecting a new "urgent" finding Delivers weekly report to stakeholder Provides detailed findings in consumable format to stakeholder Provides vulnerability mitigation recommendations to stakeholder

Figure 2: Phases of Vulnerability Scanning Enrollment

HOW CAN I GET STARTED?

- Email vulnerability@cisa.dhs.gov with the subject line "Requesting Vulnerability Scanning Services." Include the name of your utility, a point of contact with an email address, and the physical address of your utility's headquarters.
- CISA will reply with a Service Request Form and Vulnerability Scanning Acceptance Letter to obtain the necessary information about your utility and your authorization to scan your public networks.
- Scanning typically begins within 10 days of receiving all completed forms.

WHO CAN I CONTACT WITH QUESTIONS ABOUT VULNERABILITY SCANNING?

Reach out to us at vulnerability@cisa.dhs.gov

WHERE CAN I GET ADDITIONAL CYBERSECURITY RESOURCES?

CISA, the Environmental Protection Agency (EPA), and water sector partners have developed numerous tools and resources that water utilities can use to increase their cybersecurity. Visit:

- CISA: cisa.gov/water
- EPA: <https://www.epa.gov/water/riskassessment/epa-cybersecurity-water-sector>
- Water Information Sharing and Analysis Center (WaterISAC): waterisac.org
- American Water Works Association: awwa.org/cybersecurity

cisa.gov | central@cisa.dhs.gov | @CISAgov | @CISACyber | cisa.gov | As of August 24, 2023

CISA



CISA Region 10



<https://www.cisa.gov/about/regions/region-10>

CISA Oregon Contacts

Cybersecurity

Leslie Ann Kainoa

Cybersecurity State Coordinator

Leslie.kainoa@cisa.dhs.gov

503-462-5626

Christopher Ross

Cybersecurity Specialist

Christopher.ross@cisa.dhs.gov

503-979-4368

Physical Security

Tom Wilder

Protective Security Advisor

Thomas.wilder@cisa.dhs.gov

907-519-8356

Chass Jones

Protective Security Coordinator

Chass.jones@cisa.dhs.gov

503-507-8822

Jason Salfen

Protective Security Advisor

Jason.salfen@cisa.dhs.gov

541-218-3111

<https://www.cisa.gov/about/regions/region-10> CISA Emergency Communications Coordination Program Branch Chief:

Steve Noel | Salem, OR | Steven.Noel@cisa.dhs.gov

DHS/CISA Remote Communications/Emergency Communications expert guy (Brandon Smith)

After meeting with 2 CISA folks at the OAWU conference last week, they recommended we connect with Brandon regarding the Radio Communication vulnerability we found at a Washington water system (and related topics).

Brandon Smith | Stanwood, WA | Brandon.Smith@cisa.dhs.gov REGION 10: AK, ID, OR, WA

Brandon Smith working on some very interesting EW (Electromagnetic Warfare), and Cyber RF (Radio Frequency), and "Spectrum Superiority" stuff with the Washington State National Guard that may involve AFRL.

Bob,/ Steve,

Sridhar Kowdley sridhar.kowdley@hq.dhs.gov at **DHS S&T** would be very interested to hear what your company is doing in the RF ICS space. Sridhar can be reached at:

Work: 202-254-8804

Cellular: 202-394-0822

Just let him know that we talked.

Respectfully,

Brandon H. Smith

Telecommunications Specialist

DHS Cybersecurity and Infrastructure Security Agency (CISA)

Emergency Communications Division, ICTAP/CIPD

Cell: (202) 308-1183 Office: (703) 705-6373

Email: Brandon.Smith@hq.dhs.gov

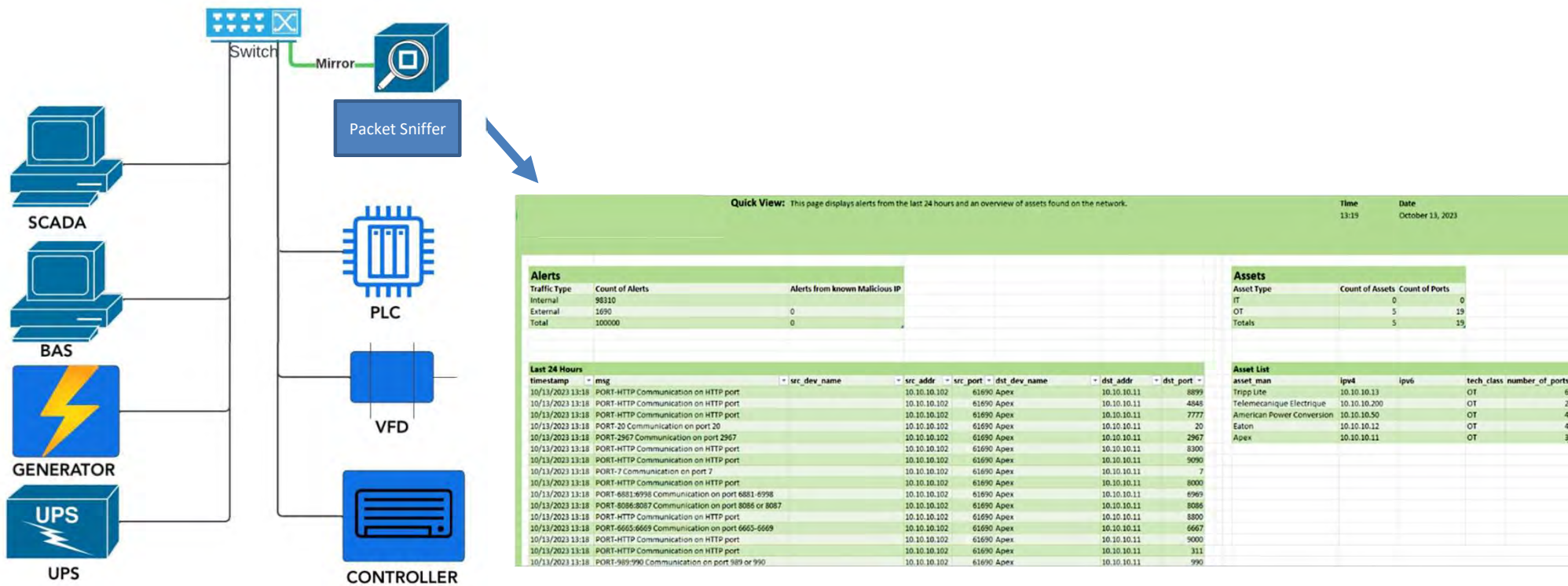
Good Threat Discovery Covers 1/3rd of Prioritized Requirements

These Requirements Can Be Affordably and Simply Managed to Protect OT Systems from Cyberattacks

- 1.1 Does the PWS detect and block repeated unsuccessful login attempts?
- 1.7 Does the PWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination or other factors?*
- 2.3 Does the PWS maintain an updated inventory of all OT and IT network assets?
- 3.1 Does the PWS collect security logs (e.g. system and network access, malware detection) to use in both incident detection and investigation?
- 3.2 Does the PWS protect security logs from unauthorized access and tampering?
- 3.3 Does the PWS use effective encryption to maintain the confidentiality of data in transit?
- 5.4 Does the PWS ensure that assets connected to the public internet expose no unnecessary exploitable services (e.g. remote desktop protocol)?
- 5.5 Does the PWS eliminate connections between its OT assets and the Internet?*
- 7.4 Does the PWS maintain updated documentation describing network topology (i.e. connections between all network components) across PWS OT and IT networks?
- 8.1 Does the PWS segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g. by IP address and port)?
- 8.2 Does the PWS keep a list of threats and adversary tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the PWS and have the capability to detect instances of key threats?

1st Solution: Powerful and Simple Threat Discovery & Response

A Packet Sniffer and Rule Set (e.g. SNORT*) Can Discover and Enable Response to Most Threats

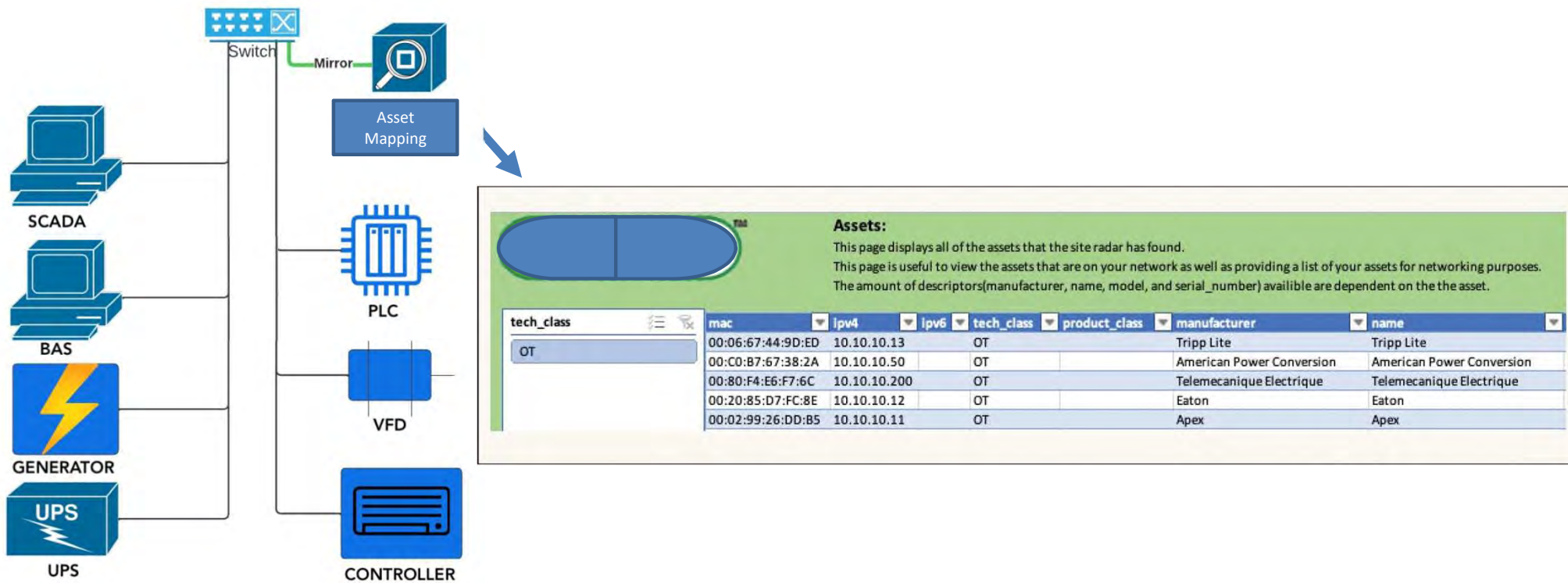


Example: This Tool Allows Smaller Utilities to Easily Understand Their Security Position with a simple Excel Dashboard

*SNORT is a free, open source rule set anyone can use in combination with a packet sniffer to analyze communication packets for threats and anomalies

...Which Can Generate (and Store) an OT Asset Inventory

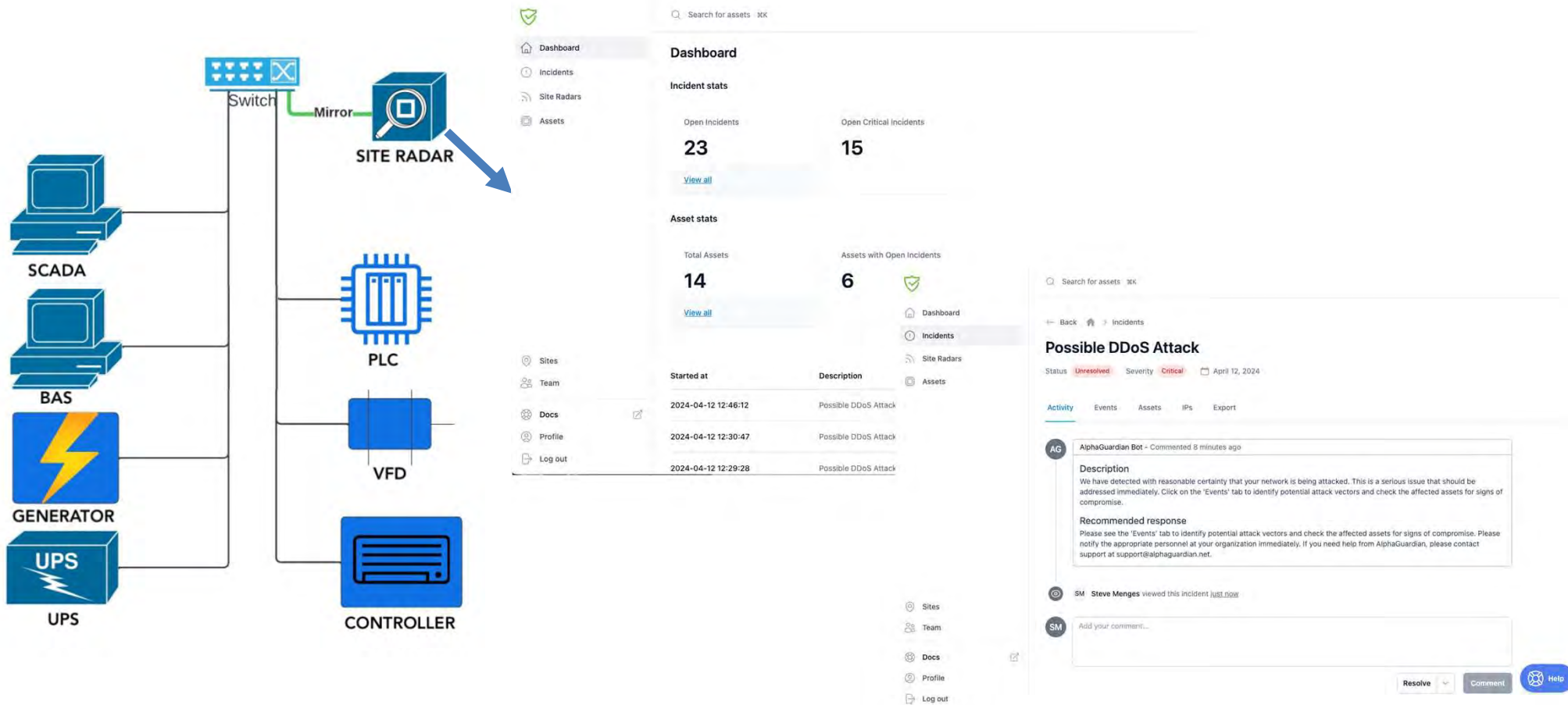
An OT Network Mapping Feature (like Nmap)



Example: This Tool Allows Smaller Utilities to Easily Understand Their Security Position with a simple Excel Dashboard

Powerful and Simple Threat Discovery & Response

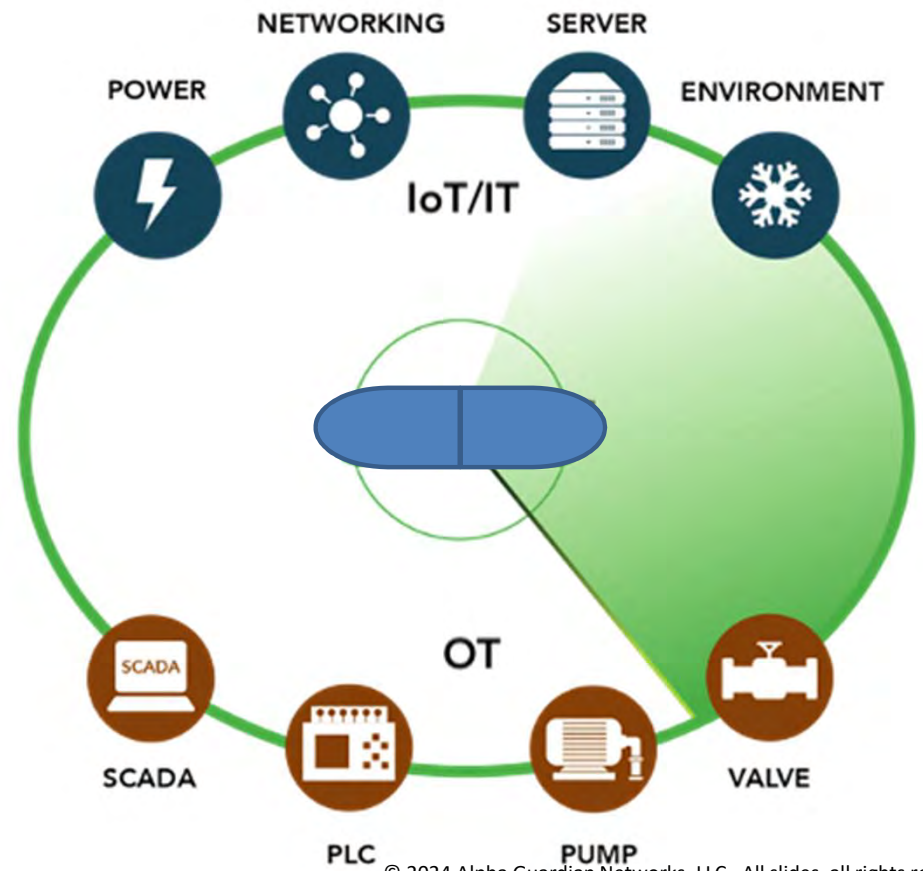
Web App Allows Smaller Utilities to Easily Understand Their Security Position



Map Your OT Network, Detect and Respond to Threats

Choose a Tool Which Provides Threat Detection and Response for OT and IoT Devices

- Create an inventory* of all OT and IT devices on your network and ensure that every OT device is completely separated from the IT device network.
- Get notified of unauthorized ports open on your devices
- Get notified of any impending IT and OT attack on the horizon and shows users how to respond.



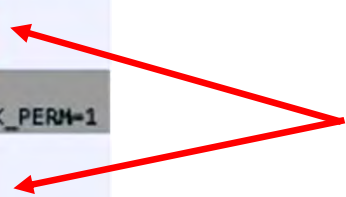
*Nmap is a popular free network mapping tool (<https://nmap.org>)

Russia Has Now Launched The Most Destructive OT Malware

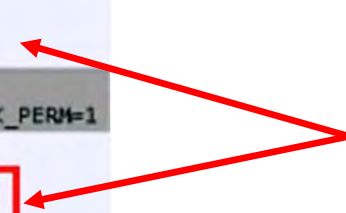
Russia's Frosty Goop Malware Specifically Targets Modbus Devices, The Heart of Water Systems

- [July 2024, Russians deploying Modbus specific malware to shut down critical utilities in Ukraine.](#)
- This malware can be used to target any Modbus system in any mission critical facility to shut it down instantly.
- Water systems rely on Modbus-based systems such as Programmable Logic Controllers (PLCs), Valves, etc.

```
TCP 66 49374 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49374 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49374 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 66 Query: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
Nodbus_ 73 Response: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
TCP 66 49375 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49375 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49375 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 66 Query: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
Nodbus_ 83 Response: Trans: 1; Unit: 254, Func: 3: Read Holding Registers
TCP 66 49376 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49376 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49376 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 66 Query: Trans: 1; Unit: 254, Func: 6: Write Single Register
Nodbus_ 66 Response: Trans: 1; Unit: 254, Func: 6: Write Single Register
TCP 66 49377 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 66 502 → 49377 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP 54 49377 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Nodbus_ 87 Query: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
Nodbus_ 66 Response: Trans: 1; Unit: 254, Func: 16: Write Multiple Registers
```



Malware reads monitoring data from Modbus Registers to surveil the system conditions



Malware then writes commands to Modbus Registers to shut-off systems

Firewalls Alone Are NOT Enough

Firewalls are Often Misconfigured and Actually Invite Cyberattacks While Giving False Sense of Security

66.211.16.100

host-66-211-16-100.cpws.net
Columbia Power and Water
Systems
United States, Columbia

Check Point **Firewall:**
Firewall Host: CPFirewall02
SmartCenter Host: CPManage.trh.com

209.152.146.84

Marshall Municipal Utilities
United States, St. Louis

Check Point **Firewall:**
Firewall Host: BPUS006NEF002
SmartCenter Host: UZNEF001-DMS-ITST01

 **SonicWall - Authentication** 

64.60.196.186
64-60-196-186.static-ip.telepacif
ic.net
Central Basin Municipal Water
United States, Fullerton

HTTP/1.0 200 OK
Server: **SonicWALL**
Expires: -1
Cache-Control: no-cache
Content-type: text/html; charset=UTF-8;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' 'unsafe-inli

 **DELL SonicWALL - Authentication** 

66.207.1.107
mpw-1-107.machlink.com
Muscatine Power and Water
United States, Muscatine

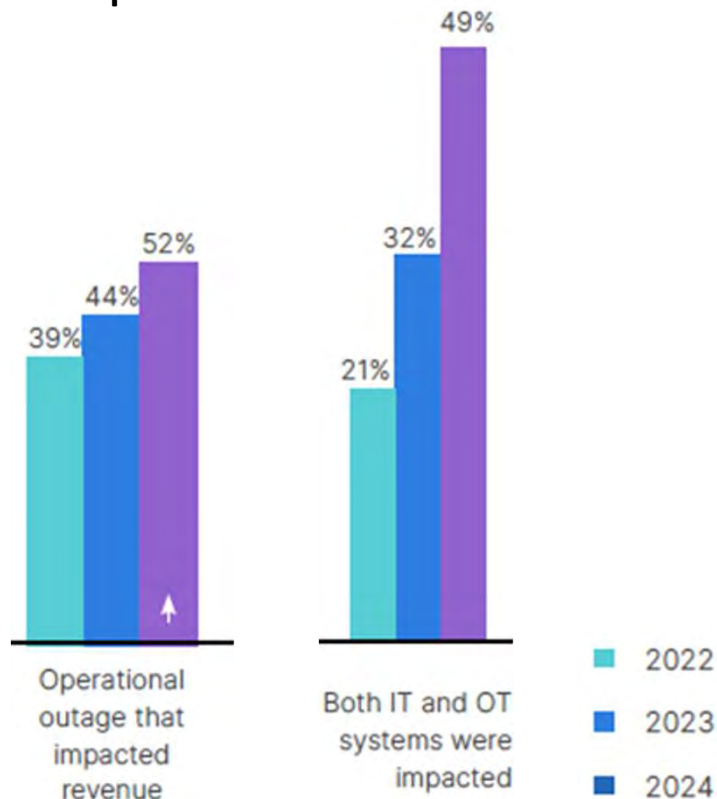
HTTP/1.0 200 OK
Server: **SonicWALL**
Expires: -1
Cache-Control: no-cache
Content-type: text/html; charset=UTF-8;

Dell **SonicWALL:**
SonicOS Version: 5.x
Serial Number: C0EAE4526740

Existing Firewalls Must Be Configured Correctly and Supplemented

Firewall Usage in OT Systems Is Now Universal but, Cyberattacks and Damage Keep Growing

Impact of OT Intrusions



[2024 – Fortinet](#)

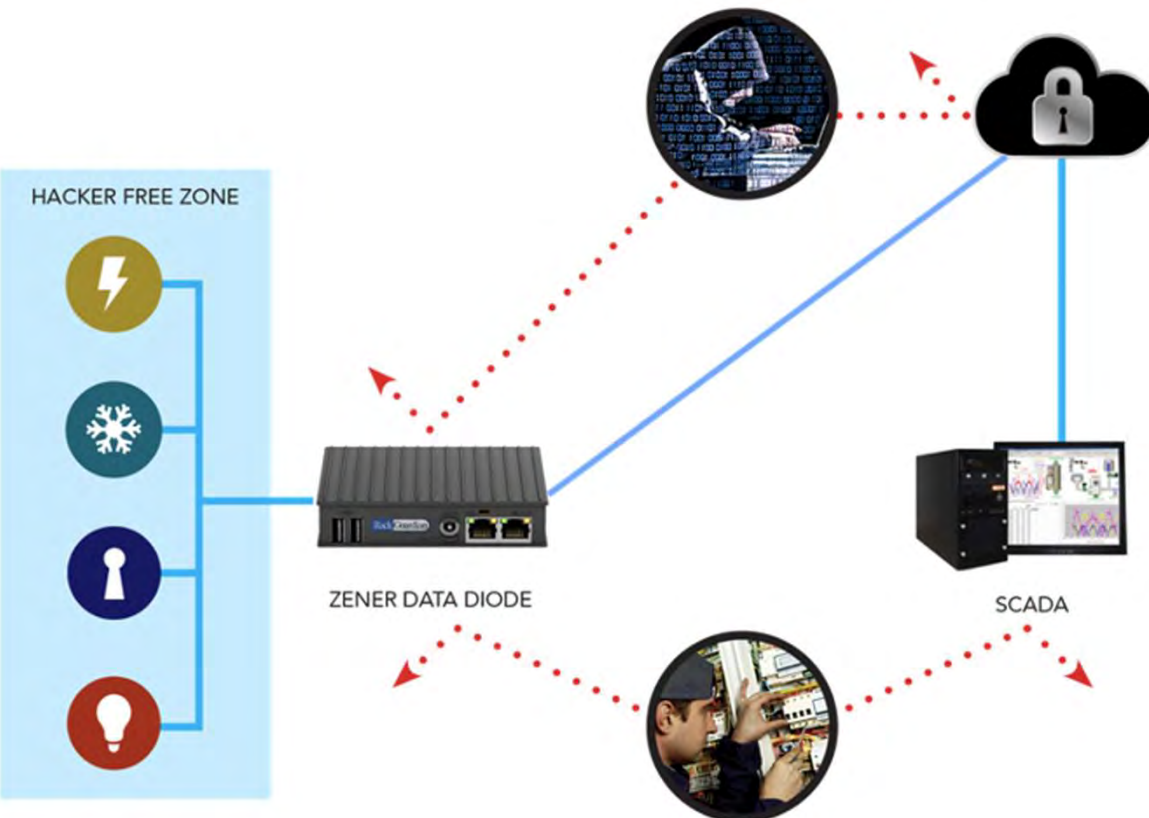
- Using firewalls alone is simply a cross your fingers and hope strategy, especially without knowledgeable configuration.
- Its necessary, at a minimum, to add a Threat Detection and Response System to see what is happening inside your OT network.:
 - It is likely that many sites already have latent Malware lurking in their OT Systems.
 - Without a Threat Detection System, you would never know the threat exists until its too late
 - A Threat Detection and Response System can also alert if an IT system has access to any OT system.
- Adding a SCADA Communications Firewall within the OT network to encrypt and manage packets between the SCADA and OT devices while protecting them from any other connection attempts is the final piece of OT security.

The Best Security Without Severing Your OT Network From the Internet

1. **Perimeter Firewall:** Shut down ALL network ports on the perimeter firewall except for either secure ports 443 and 22. These should be allowed ONLY when communicating with the SCADA vendor's upgrade cloud.
 2. **Add Threat Discovery and Response System:** The system must be updated with new threat information from a known global database and updated at least once per day. The system must have a defined response for customer action for any alerts that it generates.
 3. **Add SCADA Communications Firewall:** The system must encrypt all communications to and from each OT device AND it must provide diode-based protection for every OT device within the OT network.
-

Second Level Solution: Securing All SCADA to ICS Communications

Fully Secure SCADA Monitoring *and* Control of ICS Devices from ANY Location is the Next Objective



- Presently BMS and SCADA must communicate to any ICS device via insecure SNMP, Modbus or BACNet
- The future is replacing those communications with something more secure

Example: CyberGuardian® : Fully Secure SCADA Monitoring and Control of ICS Devices from ANY Location

© 2024 Alpha Guardian Networks, LLC. All slides, all rights reserved

Funding for PWS Cybersecurity

SLGCP

State Revolving Funds

Other (TA-Technical Assistance, etc.)

Cybersecurity Funding for Rural PWSs, Small Sites

There is following funding sources are available for a wide variety of cyber projects and the utilities will need to work directly with the funder for approval of each:

- [Clean Water State Revolving Fund \(CWSRF\)](#): Provides assistance to any public, private, or nonprofit entity for measures to increase the security of publicly owned treatment works, including cybersecurity.
- [Drinking Water State Revolving Fund \(DWSRF\)](#): Provides assistance with All-Hazard Risk and Resilience Assessment, Training, Equipment, and Infrastructure, including cybersecurity.
- [CISA State and Local Cybersecurity Grant Program \(SLCGP\)](#): Cybersecurity grant program for states, cities, counties, and towns from state administrative agency. Sub-award applications for cities, counties and towns must be submitted to the respective state administrative agency.
- **Drinking Water System Infrastructure Resilience and Sustainability Program**: This grant program can be used for planning, design, construction, implementation, operation, or maintenance of a program or project that increases resilience of public water systems, including cybersecurity.
- **Tribal Cybersecurity Grant Program: DHS grant program** for tribal governments to help address cybersecurity risks and threats to their information systems and improve their security.



Implementation of the Clean Water and Drinking Water State Revolving Fund Provisions of the Bipartisan Infrastructure Law



This document from the EPA clearly shows on the bottom of page 5 that this pool of funds provided by the EPA can be used to support water system resilience including against cyberattacks.




UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF WATER

March 8, 2022

MEMORANDUM

SUBJECT: Implementation of the Clean Water and Drinking Water State Revolving Fund Provisions of the Bipartisan Infrastructure Law

FROM: Radhika Fox
Assistant Administrator 

TO: EPA Regional Water Division Directors
State SRF Program Managers

Overview

President Biden signed the Bipartisan Infrastructure Law on November 15, 2021. The law's investment in the water sector is nothing short of transformational. It includes \$50 billion to the U.S. Environmental Protection Agency (EPA) to strengthen the nation's drinking water and wastewater systems – the single largest investment in clean water that the federal government has ever made.

EPA is committed to a productive partnership with states, tribes, and territories to maximize the impact of these funds in addressing urgent water challenges facing communities. The majority of water infrastructure dollars will flow through the Clean Water and Drinking Water State Revolving Funds (SRFs). For decades, the SRFs have been the foundation of water infrastructure investments, providing low-cost financing for local projects across America. EPA, states, tribes, and territories have successfully worked together to steward more than \$200 billion in SRF funds since 1988.

This memorandum provides information and guidelines on how EPA will award and administer SRF Capitalization Grants appropriated to the State and Tribal Assistance Grants (STAG) account in the Bipartisan Infrastructure Law (BIL) (P.L. 117-58), also known as the "Infrastructure Investment and Jobs Act of 2021" (IIJA). The information is organized in the following manner:

- **Implementation Memorandum.** This memorandum reviews key priorities for SRF BIL implementation. EPA Regional Water Divisions and Office of Water stand ready to work closely with states, tribes, and territories to collaboratively accomplish these goals.
- **Attachment 1: BIL Funding Implementation.** Attachment 1 provides detailed technical information pertaining to program requirements for the five SRF funds through the BIL: CWSRF General Supplemental Funding, CWSRF Emerging Contaminants Funding, DWSRF General

Support Resilience and One Water Innovation

One of the defining features of the SRFs is the broad range of eligible projects that states can fund to flexibly support priority needs. EPA encourages states to utilize the significant increase in SRF funding for infrastructure projects that make water systems more resilient to all threats – whether it is natural disasters, climate change, or threats such as bioterrorism and cyber-attacks.

States are strongly encouraged to fund projects that:

- **Foster resilience to all threats and hazards.** Consistent with Presidential Policy Directive (PPD) 21, critical infrastructure must be secure and resilient to all threats and hazards, both natural and manmade, in an increasingly electrified, digitized, and interconnected society. EPA urges states to use the historic increase in SRF funding to foster water, wastewater, and stormwater system resilience to all hazards, including new and emerging threats like cyber-attacks.
- **Support climate adaptation.** EPA strongly encourages states to support water, wastewater, and stormwater infrastructure projects that apply the best available and most geographically relevant

Page 5 of 56

State of Washington



[Water Quality Program](#)



<https://doh.wa.gov/community-and-environment/drinking-water/water-system-assistance/drinking-water-state-revolving-fund-dwsrf>

SLCGP

[State and Local Cybersecurity Grant Program \(SLCGP\)](#):



<https://watech.wa.gov/state-local-cybersecurity-grant-program>



Washington [IACC](#)

SLCGP - State of Washington

ELIGIBILITY - In terms of eligibility, any county, city, state agency, tribe, or special purpose district can apply.

- Are **Water Districts eligible** to receive SLCGP funds? YES, they are a special purpose district **agree**
- Are **Mutual PWSs** eligible to receive SLCGP funds? NO? **see note***
- Are **PUD (Public Utility District) PWSs eligible** to receive SLCGP funds? YES, they are a special purpose district **agree**

*RCW 26-96-010 [RCW 36.96.010: Definitions. \(wa.gov\)](#) includes the following under special purpose districts

(1) "Special purpose district" means every municipal and quasi-municipal corporation other than counties, cities, and towns. Such special purpose districts shall include, but are not limited to, water-sewer districts, fire protection districts, port districts, public utility districts, county park and recreation service areas, flood control zone districts, diking districts, drainage improvement districts, and solid waste collection districts, but shall not include industrial development districts created by port districts, and shall not include local improvement districts, utility local improvement districts, and road improvement districts;

-*"In terms of eligibility, I'd have to do more research to see what was considered special purpose district beyond this list."*

Which of these Cybersecurity products/services could be purchased with SLCGP funds:

- **Cyber Threat Monitoring Service** (i.e. 1 or 2-year subscription to an automated XDR (Extended Cyber Threat Discovery & Response) platform/service) YES, as it is a software subscription **yes as long as the timeframe is within the period of performance of the grant**
- **Cyber Event/Incident Triage & Response Service** (i.e. 1-year subscription or 1-year retainer for 100 hours of Response Expert services). NOT SURE, as it is a subscription to Cybersecurity staff augmentation **I'm not 100% sure and would need some more information before I made a determination either way.**
- **Purchase of IT Hardware/Appliance** to use to do packet sniffing and analysis to discover Cyber threats YES, as it is a Network hardware and a software subscription **yes as long as it follows all other requirements stated previously**
- **Hardware and Software Solution to secure Radio Communication** used for remote site pumps, etc. YES, as it is a Network hardware and a software subscription **yes as long as it follows all other requirements state previously**
- **Patching Service** (1 or 2-year subscription to a patching/update service for their systems) YES, as it is a software subscription **yes as long as it follows all other requirements**
- **Purchase of Public Water System Cyber Insurance policy.** NO? **Correct**

APPLYING FOR FUNDS

We are currently not accepting applications. We will open up a new solicitation at the end of March. We received 143 projects during the last solicitation and it takes a few months to review and then garner approval from FEMA/CISA. Once we receive that, we have to go through a contracting process which may take a few months depending on how many subrecipients we are working with and how responsive the subrecipient is. [\[We have funded 115 projects to date across all those types. Private and nonprofit organizations are not eligible. \]](#)

What is a realistic estimated timeline for an eligible Washington PWS who has submitted their National Cybersecurity Review (NCSR) self-assessment to actually receive SLCGP funds if they apply in April 2024? Is 90 days realistic (~July 2024)? **Realistic for finding out if they were selected for funding by the Planning Committee but not approval by FEMA. That is another month and then another month at least to get agreements out to subrecipients.**

Please have the local jurisdictions direct their questions to us in the future as we'll be able to answer specific questions more fully.

State of Washington

Examples of types of allowable costs include the following:

- Replacing or installing servers, communication, or network components onto existing racks and using existing cabling
- Installation of new equipment cabling through existing conduit and no new holes in walls, ceilings, or floors
- Tabletop equipment such as computers, monitors, and workstations
- Software
- Hiring cybersecurity or administration staff
- Creating cybersecurity plans or conducting cybersecurity testing

Training: Classroom only training, Computer or software training, Training at a designated training facility that does not involve ground disturbances or equipment installations

ELIGIBILITY

In terms of eligibility, any county, city, state agency, tribe, or special purpose district can apply. We have funded 115 projects to date across all those types. Private and nonprofit organizations are not eligible.

Please have the local jurisdictions direct their questions to us in the future as we'll be able to answer specific questions more fully.

Thanks so much. Sierra Wardell, Financial Operations Section Manager, Washington Emergency Management Division, Office: (253) 512-7121 | Mobile: (253) 921-8791 [note new number] sierra.wardell@mil.wa.gov | www.mil.wa.gov

SLCGP

State and Local Cybersecurity Grant Program
(SLCGP):



<https://watech.wa.gov/state-local-cybersecurity-grant-program>

Sierra Wardell
Financial Operations Section Manager
Washington Emergency Management Division
Office: (253) 512-7121 | Mobile: (253) 921-8791
sierra.wardell@mil.wa.gov | www.mil.wa.gov
Office hours: M-F, 8:00 am - 4:30 pm

Jeffrey Brink
Program Assistant
Preparedness Grants Section
Emergency Management Division
Washington Military Department
Work: 253-512-7136 | Cell: 253-888-2363
jeffrey.brink@mil.wa.gov |
www.mil.wa.gov/emergency-management-division

EMD core business hours: Mon-Fri, 8:00 am – 4:00 pm
My office hours: Mon-Fri, 7:00 am – 4:00 pm

Attachment A

https://www.epa.gov/dwsrf/annual-allotment-federal-funds-states-tribes-and-territories					
FY23 Summary					
Distribution of Drinking Water SRF Appropriation					
State	DWSRF Base	BIL DWSRF General Supplemental	BIL DWSRF Emerging Contaminants	BIL DWSRF LSLR	FY23 Total
Alabama	\$8,719,000	\$37,177,000	\$13,490,000	\$28,650,000	\$88,036,000
Alaska	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Arizona	\$8,638,000	\$36,833,000	\$13,365,000	\$28,650,000	\$87,486,000
Arkansas	\$5,912,000	\$25,209,000	\$9,147,000	\$45,299,000	\$85,567,000
California	\$53,272,000	\$227,150,000	\$82,428,000	\$28,650,000	\$391,500,000
Colorado	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Connecticut	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Delaware	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Florida	\$8,312,000	\$35,443,000	\$12,861,000	\$89,756,000	\$146,372,000
Georgia	\$6,172,000	\$26,316,000	\$9,549,000	\$31,809,000	\$73,846,000
Idaho	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Illinois	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Indiana	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Iowa	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Kansas	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Kentucky	\$8,312,000	\$35,443,000	\$12,861,000	\$89,756,000	\$146,372,000
Louisiana	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Maine	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Maryland	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Massachusetts	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Michigan	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Minnesota	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Mississippi	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Missouri	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Montana	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Nebraska	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Nevada	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
New Hampshire	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
New Jersey	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
New Mexico	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
New York	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
North Carolina	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
North Dakota	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Ohio	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Oklahoma	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Oregon	\$7,428,000	\$31,672,000	\$11,493,000	\$28,650,000	\$79,243,000
Pennsylvania	\$16,290,000	\$69,462,000	\$25,205,000	\$154,956,000	\$265,913,000
Puerto Rico	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Rhode Island	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
South Carolina	\$6,172,000	\$26,316,000	\$9,549,000	\$31,809,000	\$73,846,000
South Dakota	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Tennessee	\$8,312,000	\$35,443,000	\$12,861,000	\$89,756,000	\$146,372,000
Texas	\$39,369,000	\$167,867,000	\$60,914,000	\$146,246,000	\$414,396,000
Utah	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Vermont	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Virginia	\$6,973,000	\$29,732,000	\$10,789,000	\$48,717,000	\$96,211,000
Washington	\$11,307,000	\$48,214,000	\$17,495,000	\$28,650,000	\$105,666,000
West Virginia	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Wisconsin	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000
Wyoming	\$4,938,000	\$21,055,000	\$7,640,000	\$28,650,000	\$62,283,000

<https://www.epa.gov/cwsrf/clean-water-state-revolving-fund-cwsrf-allotments-federal-funds-states>

FY 2023 Distribution of Clean Water SRF Appropriation 2023 Consolidated Appropriations Base CWSRF Allotment of \$775,752,358*

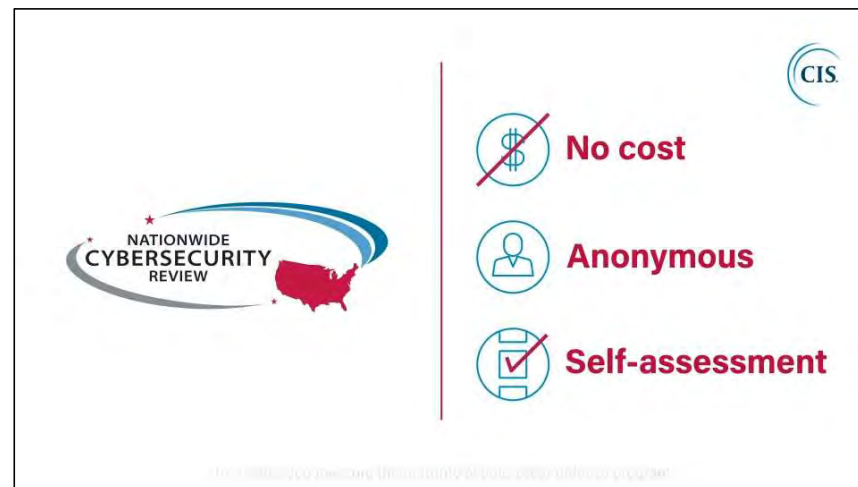
State	CWSRF Allotment			State	CWSRF Allotment		
	Total Allotment	604(b) Grant**	Capitalization Grant		Total Allotment	604(b) Grant**	Capitalization Grant
Alabama	\$8,473,000	\$85,000	\$8,388,000	New Jersey	\$30,963,000	\$310,000	\$30,653,000
Alaska	\$4,535,000	\$45,000	\$4,490,000	New Mexico	\$3,720,000	\$37,000	\$3,683,000
Arizona	\$5,118,000	\$51,000	\$5,067,000	New York	\$83,628,000	\$836,000	\$82,792,000
Arkansas	\$4,957,000	\$50,000	\$4,907,000	North Carolina	\$13,675,000	\$137,000	\$13,538,000
California	\$54,191,000	\$542,000	\$53,649,000	North Dakota	\$3,720,000	\$37,000	\$3,683,000
Colorado	\$6,061,000	\$61,000	\$6,000,000	Ohio	\$42,656,000	\$427,000	\$42,229,000
Connecticut	\$9,282,000	\$93,000	\$9,189,000	Oklahoma	\$6,122,000	\$61,000	\$6,061,000
Delaware	\$3,720,000	\$37,000	\$3,683,000	Oregon	\$8,559,000	\$86,000	\$8,473,000
Florida	\$25,576,000	\$256,000	\$25,320,000	Pennsylvania	\$30,014,000	\$300,000	\$29,714,000
Georgia	\$12,811,000	\$128,000	\$12,683,000	Puerto Rico	\$9,883,000	\$99,000	\$9,784,000
Hawaii	\$5,868,000	\$59,000	\$5,809,000	Rhode Island	\$5,088,000	\$51,000	\$5,037,000
Idaho	\$3,720,000	\$37,000	\$3,683,000	South Carolina	\$7,762,000	\$78,000	\$7,684,000
Illinois	\$34,269,000	\$343,000	\$33,926,000	South Dakota	\$3,720,000	\$37,000	\$3,683,000
Indiana	\$18,261,000	\$183,000	\$18,078,000	Tennessee	\$11,007,000	\$110,000	\$10,897,000
Iowa	\$10,255,000	\$103,000	\$10,152,000	Texas	\$34,632,000	\$346,000	\$34,286,000
Kansas	\$6,839,000	\$68,000	\$6,771,000	Utah	\$3,992,000	\$40,000	\$3,952,000
Kentucky	\$9,644,000	\$96,000	\$9,548,000	Vermont	\$3,720,000	\$37,000	\$3,683,000
Louisiana	\$8,329,000	\$83,000	\$8,246,000	Virginia	\$15,507,000	\$155,000	\$15,352,000
Maine	\$5,865,000	\$59,000	\$5,806,000	Washington	\$13,177,000	\$132,000	\$13,045,000


National Cybersecurity Review (NCSR)




(now a requirement for the SLCGP (State and Local Cybersecurity Grant Program))

Center for Internet Security (CIS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) about the National Cybersecurity Review (NCSR).

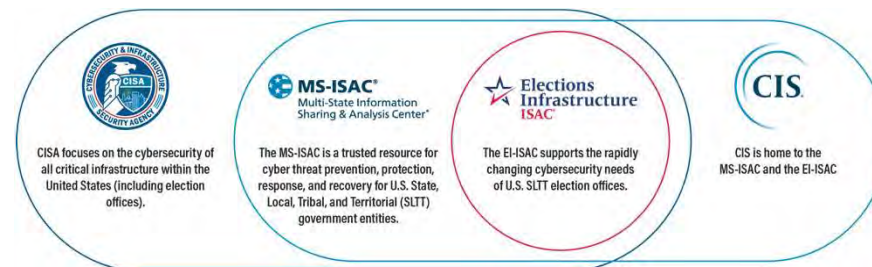
- NCSR:**
- 140 Question Self-Assessment (or Cyber-readiness/resiliency) by PWS (to then be done yearly), which will get aggregated and shared (purportedly anonymously) with DHS/Congress/others
 - Getting an account of the NCSR system, and completing the self-assessment is a requirement to even apply for SLCGP funds
 - NCSR System may only be “open” from October 1 – February 28








-  **No cost**
-  **Anonymous**
-  **Self-assessment**


Score	Maturity Level
<i>The recommended minimum maturity level is set at a score of 5 and higher</i>	
7	Optimized: Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified: Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process: Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	Risk Formally Accepted: Your organization has chosen not to implement based on a risk assessment.
4	Partially Documented Standards and/or Procedures: Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	Documented Policy: Your organization has a formal policy in place.
2	Informally Performed: Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	Not Performed: Activities, processes and technologies are not in place to achieve the referenced objective.




 CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).


 The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.


 The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.


 CIS is home to the MS-ISAC and the EI-ISAC

CIS is a nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, and is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®),

State of Washington



State of Washington Department of Ecology Water Quality Combined Funding Program

- “... *integrated funding program for projects that improve **and protect water quality** throughout the state.*”
- The program combines grants and loans from state and federal funding sources.
- One combined funding cycle, one application, one competitive rating process, and one list of funding offers.
- Funded projects can last 3-5 years (depending on type).

- **Cybersecurity, SCADA acquisition/refresh, etc. projects are eligible**

- Applicants **submit just one application** for all of the funding sources under the Water Quality Combined Funding Program.

- Also provides technical assistance to program applicants to help them navigate this process.
 - **Get started with the Department of Ecology team now and be ready for the start of the next application period next summer**

Eliza Keeley
Water Quality Combined Funding Planner
eliza.keeley@ecy.wa.gov
360-628-1976

Shelly McMurry
State Revolving Fund Coordinator
shelly.mcmurry@ecy.wa.gov
564-999-1649

Cyber Services Not Confirmed

Other Funding Possibilities

Funding Sources for Small and Rural Wastewater Systems

EPA and other organizations provide funding to improve water and wastewater systems in small and rural communities.

• Funding for All Communities

• Environmental Justice Grants and Cooperative Agreements

Provide financial assistance to eligible organizations to develop collaborative partnerships, identify environmental and public health issues, and develop projects.

• Nonpoint Source Grants Program (Section 319 of the Clean Water Act)

Provides grants for activities that prevent water pollution from nonpoint sources, including education, training, technical and financial assistance, technology transfer, demonstration projects, and monitoring nonpoint source implementation projects. Eligible projects include decentralized wastewater systems.

• Public Water System Supervision (PWSS) Grant Program

Assists states, territories, and tribes to develop and implement PWSS programs to enforce the requirements of the Safe Drinking Water Act.

• Water Pollution Control Grants Program (Section 106 of the Clean Water Act)

Provides federal assistance to states, territories, the District of Columbia, Indian tribes, and interstate agencies to establish and implement ongoing water pollution control programs.

Non-EPA Funding Sources

• Appalachian Regional Commission

A federal-state partnership that promotes sustainable communities and economic development in Appalachia.

• U.S. Department of Agriculture, Rural Development, Water and Environmental Programs

Provide loans, grants, and loan guarantees for drinking water, sanitary sewer, and storm drainage facilities in rural areas, cities, and towns with populations of 10,000 or less. Public bodies, non-profit organizations, and recognized Indian tribes may qualify for assistance.

• U.S. Department of Housing and Urban Development, Community Development Block Grants

Provide funds for long-term community needs, including rehabilitation, construction, or purchase of public facilities and infrastructure for water treatment and centralized and decentralized wastewater systems.

• Catalog of Federal Funding Sources for Watershed Protection

A searchable database of financial assistance sources (grants, loans, and cost-sharing) to fund a variety of watershed protection projects. To select funding programs for wastewater projects, select "wastewater" under "keywords."

• Catalog of Federal Domestic Assistance

Lists federal programs available to state and local governments (including the District of Columbia); federally-recognized Indian tribal governments; territories and possessions of the United States; domestic public, quasi- public, and private profit and nonprofit organizations and institutions; specialized groups; and individuals.

• Funding for Tribal Communities

• Funding for U.S.-Mexico Border Communities

Other Funding Possibilities Tribal

Cyber Services Not Confirmed

Funding for Tribal Communities

Alaska Native Villages and Rural Communities Grant Program

Assists Alaska Native Villages and Alaska's rural communities to construct new or improve existing drinking water and wastewater systems. Funds training and technical assistance to operate and maintain these systems. EPA provides grants to the Alaska Department of Environmental Conservation, which administers the funds through its Village Safe Water Program.

'Clean Water Indian Set-Aside (CWISA) Program

Provides funds for wastewater infrastructure to Indian tribes and Alaska Native Villages. The CWISA Program is administered in cooperation with the Indian Health Service (IHS). To be considered for CWISA funding, tribes must identify their wastewater needs through the IHS Sanitation Deficiency System.

Indian Environmental General Assistance Program

Provides grants to federally recognized tribes and tribal consortia to develop and implement wastewater and other programs on tribal lands. [Tribal Public Water System Supervision Support Grants](#)

Assist tribes implement water system supervision programs to ensure their water systems comply with Safe Drinking Water Act requirements and standards. [Tribal Water Pollution Control Program Grants \(Section 106 of the Clean Water Act\)](#) Assist Indian tribes implement effective water pollution control programs.

Non-EPA Tribal Funding Sources

• [Alaska Native Tribal Health Consortium \(ANTHC\)](#)

Plans, designs, and constructs drinking water and wastewater treatment facilities for Alaska Native communities.

• [U.S. Department of Agriculture, Rural Development, Native American Tribes](#)

Works with public and nonprofit organizations to provide funding options to communities in rural America including water and wastewater loans and grants.

• [U.S. Department of Health and Human Services, Administration for Native Americans, Environmental Regulatory Enhancement Grants](#)

Provide tribes with resources to develop legal, technical and organizational capacities, and protect their natural environments.

• [U.S. Department of Health and Human Services, Indian Health Service, Sanitation Facilities Construction Program](#)

Provides technical and financial assistance to Indian tribes and Alaska Native communities for the cooperative development and continuing operation of safe water, wastewater, and solid waste systems, and related support facilities.

• [U.S. Department of Housing and Urban Development, Indian Community Development Block Grant Program](#)

Provides direct grants to develop viable Indian and Alaska Native communities, including decent housing, a suitable living environment, economic opportunities, and water and sewer facilities, primarily for low and moderate income persons.

• [U.S. Department of Interior, Bureau of Indian Affairs](#)

Provides services through contracts, grants, and compacts to American Indians and Alaska Natives to enhance quality of life, promote economic opportunity, and protect and improve environmental assets.

• [U.S. Department of Interior, Bureau of Reclamation, Native American Affairs Technical Assistance Program](#)

Provides technical assistance to Indian Tribes to develop, manage, and protect water and related resources. Activities include water needs assessments, improved water management studies, water quality data collection and assessments, and water measurement studies.

Funding for U.S.-Mexico Border Communities

• [U.S.-Mexico Border Water Infrastructure Grant Program](#)

Provides grant assistance to communities along the U.S.-Mexico border for planning, designing, and constructing drinking water and wastewater infrastructure. The U.S.-Mexico border region is defined as 100 kilometers (62 miles) north and 100 kilometers south of the U.S.-Mexico border. EPA's grant program supports the Project Development Assistance Program, administered by the Border Environment Cooperation Commission, and the Border Environmental Infrastructure Fund, administered by the North American Development Bank.

• [U.S.-Mexico Border 2025 Program](#)

The latest environmental program implemented under the 1983 La Paz Agreement. The program emphasizes regional, bottom-up approaches for decision-making, priority setting, and project implementation to address environmental and public health problems in the border region. The program encourages participation from communities and local stakeholders.

CISA State and Local Cybersecurity Grant Program

(SLCGP): Grant program for states, cities, counties and towns from state administrative agency.

Sub-award applications for cities, counties and towns must be submitted to the respective state administrative agency. EPA's [SLCGP Fact Sheet](#) →

Department of Homeland Security (DHS) announced cybersecurity grant program specifically for state, local, and territorial (SLT) governments across the country.

In the Bipartisan **Infrastructure Law**, also known as the Infrastructure Investment and Jobs Act (IIJA), Congress established the [State and Local Cybersecurity Grant Program \(SLCGP\)](#) to “award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.” Within the **U.S. Department of Homeland Security (DHS)**, the **Cybersecurity and Infrastructure Security Agency (CISA)** and the **Federal Emergency Management Agency (FEMA)** are implementing this authority through two grant programs:

1. The SLCGP, which allows **state and territory State Administrative Agencies (SAAs)** to apply for grant funding. **Under SLCGP, states and territories are the only eligible entities. Local and tribal governments are eligible subrecipients under this program.**
2. The Tribal Cybersecurity Grant Program (TCGP), which allows **Tribal governments to apply for grant funding. Under TCGP, Tribal governments of federally-recognized Tribes are the only eligible entities** and do not apply for funding through SAAs.

An official website of the United States government [Here's how you know](#)

apply for grant awards under



State Administrative Agency (SAA) Contacts

The State Administrative Agency (SAA) is the only entity eligible to apply for and submit the application for the Homeland Security Grant Program (HSGP) and its component programs — State Homeland Security Program (SHSP), Urban Area Security Initiative (UASI), and Operation Stonegarden (OPSG) — as well as the Nonprofit Security Grant Program (NSGP).

Additionally, the SAA is one of two eligible entities allowed to apply for the Emergency Management Performance Grant **If you have a project you are interested in funding, please contact your applicable SAA POC.**

State/Territory	Website	Contact
Alabama	Alabama Law Enforcement Agency	Wendy Taylor

Contents Copyright 2024 – AlphaGuardian Networks LLC. All rights reserved



FEMA



INCREASING WATER SECTOR CYBER RESILIENCE WITH THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

PURPOSE

The United States Environmental Protection Agency (EPA) is promoting the \$1 billion State and Local Cybersecurity Grant Program (SLCGP) launched by the Department of Homeland Security (DHS) to address cybersecurity risks and threats to information systems owned or operated by state, local, and territorial governments. The grants will assist in addressing capability and capacity gaps that state primary agencies and local and territorial water systems may face when taking steps to improve cybersecurity measures.

Benefits to the Water Sector

State primary agencies can receive support from a portion of the funding provided to the State Administrative Agency (SAA). Water and wastewater systems can receive cyber support from locally sub-awards. Sub-award funding can be used to increase cyber resilience through qualifying activities designated by the grant.

STATE-LEVEL QUALIFYING ACTIVITIES

Funding will support the following activities:

- Establish a Cybersecurity Planning Committee
- Develop a state-wide Cybersecurity Plan
- Conduct cybersecurity assessments and evaluations
- Adopt key cybersecurity best practices

WHEN CAN WATER SYSTEMS BENEFIT?

Municipal water systems can expect to participate in the application process when their locality, county or city submits an application for a sub-award to the SAA. Each state process may vary; however, based on the current programmatic timeline, these announcements may not occur before **January 2023**.

How do water systems apply for sub-awards:

The application process for sub-awards may differ for each SAA. Please contact your SAA for further information. A listing of current SAAs is available at www.fema.gov/grants/preparedness/about/state-administrative-agency-contacts.

How is EPA helping?

The EPA is ensuring that the availability of funding is communicated broadly within the water sector. This fact sheet will be updated as additional information becomes available.

FOR MORE INFORMATION

Please visit: www.cisa.gov/cybergrants

Office of Water (4608T)
EPA-810-F-22-013
November 2022



The IIJA Cyber Funding Assessment and Plan is a NIST-based cybersecurity requirement of the Federal Government to apply for the funding set aside to strengthen the cybersecurity posture of state and local government agencies against cyber-attacks in the Infrastructure Investment and Jobs Act (IIJA).



**Grant Programs Directorate
Information Bulletin No. 489
August 7, 2023**

MEMORANDUM FOR: All State Administrative Agency Heads
All State Administrative Agency Points of Contact
All Urban Area Security Initiative Points of Contact
All State Homeland Security Directors
All State Emergency Management Agency Directors
All Tribal Nation Leaders
All Tribal Nation Points of Contact

FROM: Pamela S. Williams *P.S. Williams*
Assistant Administrator
Grant Programs Directorate

SUBJECT: Fiscal Year 2023 State and Local Cybersecurity Grant Program
Allocation Amounts

Today, the Federal Emergency Management Agency (FEMA) and Cybersecurity and Infrastructure Security Agency (CISA), both components of the Department of Homeland Security, announced the availability of the Fiscal Year (FY) 2023 Notice of Funding Opportunity (NOFO) for the State and Local Cybersecurity Grant Program (SLCGP). The FY 2023 SLCGP provides \$374,981,324 in federal assistance to State, Local, and Territorial governments to assist with managing and reducing systemic cyber risk. The FY 2023 SLCGP NOFO may be found online at <http://www.fema.gov/grants> and at <http://www.grants.gov>.

Eligible applicants (state or territory State Administrative Agencies) must apply for funding through the Grants.gov portal at <http://www.grants.gov>. When applicants apply through <http://www.grants.gov>, they must submit the Standard Form 424 in the initial Grants.gov application. The FEMA Non-Disaster (ND) Grants system will retrieve the Standard Form 424 directly from the Grants.gov system and will automatically populate the relevant data fields in the

State and territory allocations for the FY 2023 SLCGP are listed in the table below, as well as included in the FY 2023 SLCGP NOFO.

State/Territory	FY 2023 SLCGP Allocation	State/Territory	FY 2023 SLCGP Allocation
Alabama	\$7,840,285	Nevada	\$5,072,822
Alaska	\$4,567,677	New Hampshire	\$5,096,082
Arizona	\$6,776,692	New Jersey	\$6,858,348
Arkansas	\$6,402,359	New Mexico	\$5,178,907
California	\$15,879,497	New York	\$11,588,894
Colorado	\$6,553,216	North Carolina	\$10,813,417
Connecticut	\$5,465,875	North Dakota	\$4,666,397
Delaware	\$4,546,985	Ohio	\$10,042,553
District of Columbia	\$4,240,457	Oklahoma	\$6,665,123
Florida	\$11,997,340	Oregon	\$6,047,316
Georgia	\$9,873,903	Pennsylvania	\$10,463,799
Hawaii	\$4,567,336	Rhode Island	\$4,467,229
Idaho	\$5,210,589	South Carolina	\$7,428,446
Illinois	\$8,834,866	South Dakota	\$4,766,558
Indiana	\$7,977,398	Tennessee	\$8,606,142
Iowa	\$6,228,366	Texas	\$17,418,110
Kansas	\$5,707,130	Utah	\$5,348,368
Kentucky	\$7,413,939	Vermont	\$4,717,850
Louisiana	\$6,732,858	Virginia	\$8,712,723
Maine	\$5,439,273	Washington	\$7,403,503
Maryland	\$6,514,533	West Virginia	\$5,620,962
Massachusetts	\$6,419,112	Wisconsin	\$7,666,939
Michigan	\$9,609,530	Wyoming	\$4,477,270
Minnesota	\$7,270,657	Puerto Rico	\$5,068,610
Mississippi	\$6,639,551	U.S. Virgin Islands	\$1,046,957
Missouri	\$7,748,105	American Samoa	\$1,039,880
Montana	\$4,947,036	Guam	\$1,068,051
Nebraska	\$5,188,485	Northern Mariana Islands	\$1,037,018
Total			\$374,981,324

1. \$1,008,000 Total over 4 years:

\$185 million in August 2022 in the program's first year,

2. \$379 million being available as part of Year 2

3. TBD for Year 3

4. TBD for Year 4

INCREASING WATER SECTOR CYBER RESILIENCE WITH THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM



PURPOSE

The United States Environmental Protection Agency (EPA) is promoting the \$1 billion State and Local Cybersecurity Grant Program (SLCGP) launched by the Department of Homeland Security (DHS) to address cybersecurity risks and threats to information systems owned or operated by state, local, and territorial governments. The grants will assist in addressing capability and capacity gaps that state primacy agencies and local and territorial water systems may face when taking steps to improve cybersecurity measures.

Benefits to the Water Sector

State primacy agencies can receive support from a portion of the funding provided to the State Administrative Agency (SAA). Water and wastewater systems can receive cyber support from locality sub-awards. Sub-award funding can be used to increase cyber resilience through qualifying activities designated by the grant.

STATE-LEVEL QUALIFYING ACTIVITIES

Funding will support the following activities:

- Establish a Cybersecurity Planning Committee
- Develop a state-wide Cybersecurity Plan
- Conduct cybersecurity assessments and evaluations
- Adopt key cybersecurity best practices

WHEN CAN WATER SYSTEMS BENEFIT?

Municipal water systems can expect to participate in the application process when their locality, county or city submits an application for a sub-award to the SAA. Each state process may vary; however, based on the current programmatic timeline, these announcements may not occur before **January 2023**.

How do water systems apply for sub-awards:

The application process for sub-awards may differ for each SAA. Please contact your SAA for further information. A listing of current SAAs is available at www.fema.gov/grants/preparedness/about/state-administrative-agency-contacts.

Prevention & Compliance

PWS Cybersecurity Controls

New From CISA-EPA-FBI-USDA-DOE++++

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity **TLP:CLEAR**

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity **TLP:CLEAR**

- Immediately change all default and weak passwords. Ensure the factory default password is not in use. Open the device and change the password to a strong password as shown [\[CSG 2.A\]](#) [\[CSG 2.B\]](#).
- Keep VNC updated with the latest version available and apply patches and necessary security updates.
- Establish an allowlist that permits only authorized users to access the device at any time of the day to further obstruct malicious threat actors from alerting for monitoring access attempts.
 - Note: An allowlist is not a complete security measure. It is a threat actor to compromise a device.
- Log remote logins to HMIs, taking note of any failed login attempts.

Strengthen Security Posture

- Integrate cybersecurity considerations into the engineering and design process. For additional information, see the DOE Office of Cyber Security (DOE-CESER)'s publication on [Cyber-Informed Engineering](#).
- Practice and maintain the ability to operate systems in a safe manner. Create backups of the engineering logic, configure your organization with factory resets and backups, and ensure the integrity of PLC ladder logic or other I/O modules. Do not make unauthorized modifications to ensure correct operation of the device in an unsafe way by changing the logic.
- Update and safeguard network diagrams to reflect the current state of the network. Apply the principles of least privilege and need-to-know to restrict access to network diagrams and architectures and restrict mapping to trusted personnel. Use network segmentation and restrict mapping to trusted personnel.
- Be aware of cyber/physical-enabled threats. Adversaries may use physical means, including official visits, tradecraft, and social engineering, to gain access to systems and data.
- Take inventory and determine the end-of-life status of hardware. Implement software and hardware limits to the maximum extent possible to prevent a successful compromise. This can be completed through engineering, configuration, and cyber-informed engineering.

Limit Adversarial Use of Common Vulnerabilities

- Reduce risk exposure. U.S. organizations can use vulnerability assessment services to help provide additional review of their systems to mitigate vulnerabilities. Email [vulnerability@nsc.gov](#) to get started. UK organizations can use [UK Cyber Security Services](#).
- Assess your security posture. CISA's regional Cyber Security Centers can help U.S. organizations understand their current security posture.

OT Device Manufacturers

Although critical infrastructure device manufacturers are encouraged to build secure devices, they are also encouraged to take ownership of their devices. See [Balance of Cybersecurity Risk](#) for more information on this topic.

- Eliminate default and factory settings that allow threat actors to exploit to gain access to the device.
- Mandate multifactor authentication for all users.
- Include logging at no less than the critical level for all events.
- Publish Software Bills of Materials (SBOMs) for all devices. Measure and mitigate the risk of supply chain compromise.

Additionally, see CISA's [Secure by Design](#) guidance for more information on this topic. By securing "out of the box" without purchasing tiered security software, organizations can reduce their risk.

RESOURCES

Entities requiring additional support include:

- [CISA Cybersecurity Advisor](#) and [CISA Cybersecurity Support](#)
- [NSA, CISA, and DHS Recommendations](#)
- [CISA, EPA, Water and WWS](#)
- [CISA, EPA, FBI, Top Cyber](#)
- [Food and Agriculture in and Medium Enterprise](#)
- [DOE, National Association of Manufacturers, and Distribution Systems at Risk](#)

Additional resources include:

- [NCSO-UK: Operational Resilience](#)
- [EPA Cybersecurity for Industrial Facilities](#)
- [CISA: Cross-Sector Cyber Security](#)
- [CISA: More than a Password](#)
- [DOE: Cyber-Informed Engineering](#)
- [CISA: Cyber Hygiene Series](#)
- [CISA: Shifting the Balance](#)
- [CISA: Secure by Design](#)
- [CISA: Secure by Design](#)
- [CISA: Secure by Design: Malicious Cyber Activity](#)

REPORTING

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this fact sheet to:

- CISA via CISA's 24/7 Operations Center (report@cisa.gov) or 888-282-0870 or your [local FBI field office](#). 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.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- Water and Wastewater Systems Sector organizations should contact the EPA Water Infrastructure and Cyber Resilience Division at watersystems@epa.gov to voluntarily provide situational awareness.
- State, local, tribal, and territorial governments should report incidents to the MS-ISAC (ISOC@cisecurity.org or 866-787-4722).
- The Water Information Sharing & Analysis Center (WaterISAC) encourages members to share information by emailing analyst@waterisac.org, calling 866-H2O-ISAC, or using the [online incident reporting form](#).
- Entities required to report incidents to DOE-CESER should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergyCSIRMS@via.doe.gov. DOE also encourages energy entities to report information to their relevant energy ISACs:
 - Downstream Natural Gas (DNG-ISAC): analyst@dngisac.com
 - Electricity (E-ISAC): operations@eisac.com
 - Oil & Natural Gas (ONG-ISAC): soc@ongisac.org

International organizations:

- UK organizations are encouraged to report any suspected compromises to the NCSO via their [incident reporting website](#).
- Canadian organizations should report incidents by emailing COCS at contact@cyber.gc.ca.

ACKNOWLEDGEMENTS

The DNG-ISAC and WaterISAC contributed to this fact sheet.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.

VERSION HISTORY

May 1, 2024: Initial version.

TLP:CLEAR

“Old” from CISA

The IT/OT Disconnect

CYBER RISKS & RESOURCES FOR THE WATER AND WASTEWATER SYSTEMS SECTOR

The Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to highlight cyber risks and provide available resources to support the Water and Wastewater Systems Sector. The Federal Government released **Joint Cybersecurity Advisory AA21-287A** on October 14, 2021 in response to unauthorized access of Supervisory Control and Data Acquisition (SCADA) systems at U.S. drinking water treatment facilities. Cyber criminals have been observed targeting desktop sharing applications, which despite having legitimate uses, can also be exploited through malicious actors' use of social engineering tactics and other illicit measures. Computer networks running operating systems with end-of-life status also pose significant risks that malicious actors will gain unauthorized access to systems.

RISKS TO THE SUPPLY WATER NATIONAL CRITICAL FUNCTION

Operational Technology (OT)

1 NETWORK COMPLEXITY

Water OT networks may contain hundreds of diverse components that can be difficult to properly map and update. This complexity may lead to operators not having full visibility into their networks and may contribute to misconfigurations and continued usage of components that are not included in a utility's network mapping.

2 SYSTEM MAINTENANCE

Improperly maintained custom and Commercial off the Shelf (COTS) components, particularly those that have not been kept up to date on security patches or are operating beyond end-of-life, can leave OT systems vulnerable to attack. Managed Service Providers (MSP) may be used within critical infrastructure to support both IT and OT networks, and if compromised, could provide adversaries with remote access into customers' OT systems. A successful exploitation of an OT system can provide attackers with a direct means of manipulating systems that support the management of water systems.

IT/OT Convergence

3 NETWORK SEGMENTATION

Malicious actors may use IT networks as a vector to target non-segmented OT networks and systems. Proper network segmentation is the most effective way to prevent cyber-attacks against OT networks.

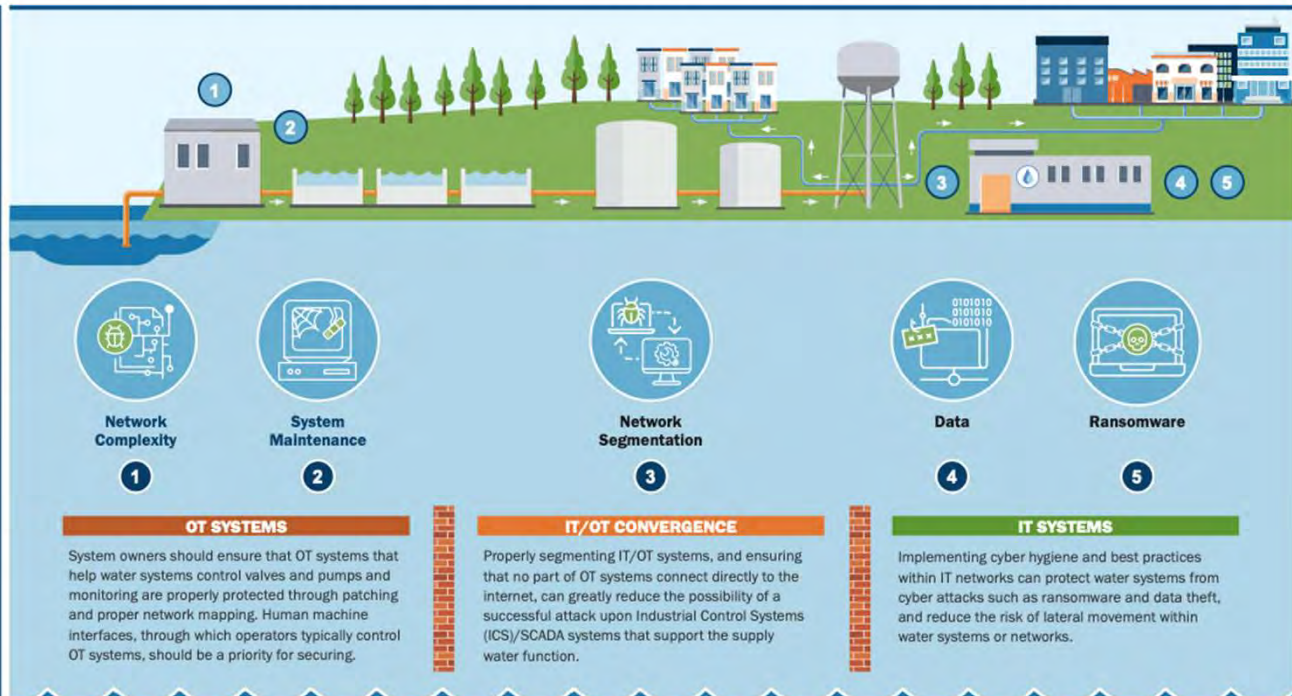
Information Technology (IT) Systems

4 DATA

Malicious actors may attempt to access IT systems to steal sensitive data, disable network components, and move laterally within the network to access other more sensitive systems. Malicious actors may also attempt to use stolen information to move laterally within the network and access other more sensitive areas.

5 RANSOMWARE

Ransomware attacks can disrupt operations within a facility until systems are restored. While disruptions in office-based systems are most common, it is possible for ransomware to also infect connected OT systems, particularly if there is not adequate segmentation between IT and OT systems.



Network Complexity

System Maintenance

Network Segmentation

Data

Ransomware

OT SYSTEMS

System owners should ensure that OT systems that help water systems control valves and pumps and monitoring are properly protected through patching and proper network mapping. Human machine interfaces, through which operators typically control OT systems, should be a priority for securing.

IT/OT CONVERGENCE

Properly segmenting IT/OT systems, and ensuring that no part of OT systems connect directly to the internet, can greatly reduce the possibility of a successful attack upon Industrial Control Systems (ICS)/SCADA systems that support the supply water function.

IT SYSTEMS

Implementing cyber hygiene and best practices within IT networks such as ransomware and data theft, and reduce the risk of lateral movement within water systems or networks.

RESOURCES

AVAILABLE RESOURCES INCLUDE: CISA's **Cyber Resource Hub** provides a range of free, immediately available cybersecurity resources. CISA's **Cyber Essentials Toolkit** for non technical leadership. **Securing Networking Devices** provides guidance on Segmenting and Segregating Networks. **Stopransomware.gov** contains best practices for preventing or responding to ransomware. The **Industrial Control Systems Joint Working Group (ICS JWG)** has links to trainings and resources related to the securing and safe operation of ICS systems. CISA also provides no cost **cybersecurity assessments**. The **WaterISAC** produces physical and cyber threat alerts and best practices specifically for the water and wastewater sector. The **AWWA's Security Guidance and Tool** supports the sector in implementing the NIST Cybersecurity Framework and use of Cybersecurity Guidance and Assessment Tool.

Biden-Harris Administration engages states on safeguarding water sector infrastructure against cyber threats [March 19, 2024]

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks, carried out by countries and criminals, have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities.

WASHINGTON – Today, March 19, U.S. Environmental Protection Agency Administrator Michael Regan and National Security Advisor Jake Sullivan sent a [letter](#) to all U.S. Governors inviting state environmental, health and homeland security Secretaries to a convening by their deputies to discuss the urgent need to safeguard water sector critical infrastructure against cyber threats. This meeting will highlight current federal and state efforts to promote cybersecurity practices in the water sector, discuss priority gaps in these efforts, and emphasize the need for states and water systems to take immediate action.

This virtual meeting will take place on Thursday, March 21, 2024, from 1:00pm – 2:30 pm EST. EPA will be sending meeting registration information to the states separately via email.

“Drinking water and wastewater systems are a lifeline for communities, but many systems have not adopted important cybersecurity practices to thwart potential cyberattacks,” said **EPA Administrator Michael S. Regan**. “EPA and NSC take these threats very seriously and will continue to partner with state environmental, health, and homeland security leaders to address the pervasive and challenging risk of cyberattacks on water systems.”

“The Biden Administration has built our national security approach on the foundational integration of foreign and domestic policy, which means elevating our focus on cross-cutting challenges like cybersecurity,” said **National Security Advisory Jake Sullivan**. “We’ve worked across government to implement significant cybersecurity standards in our nation’s critical infrastructure, including in the water sector, as we remain vigilant to the risks and costs of cyber threats. We look forward to continuing our partnership with the EPA to bolster the cybersecurity of America’s water and wastewater systems.”

The National Security Council (NSC) and EPA are encouraging all states to join this dialogue to drive rapid improvements to water cybersecurity and reinforce collaboration between state and federal entities and water systems.

Additionally, EPA will strive to collaborate with the Water Sector and Water Government Coordinating Councils in forming a Water Sector Cybersecurity Task Force to identify near-term actions and strategies to reduce the risk of water systems nationwide to cyberattacks. In addition to considering the prevalent vulnerabilities of water systems to cyberattacks and the challenges experienced by some systems in adopting best practices, this Task Force in its deliberations would seek to build upon existing collaborative products, such as the 2023 Roadmap to a Secure and Resilient Water and Wastewater Sector and recommendations stemming from the meeting with Environmental, Health and Homeland Security Secretaries.

These collaborative efforts will result in advances that will better protect the nation’s critical water infrastructure from cyberattacks. For information about EPA’s cybersecurity program or details about the upcoming meeting please visit [EPA’s Cybersecurity for the Water Sector website](#).

Background

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks, carried out by countries and criminals, have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. As the Sector Risk Management Agency identified in Presidential Policy Directive 21 for water and wastewater systems, EPA is the lead federal agency for ensuring the nation’s water sector is resilient to all threats and hazards.

EPA and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) offer guidance, tools, training, resources, and technical assistance to help water systems to execute these essential tasks. Further, cybersecurity support and technical assistance are available from state programs as well as private sector associations like the American Water Works Association, the National Rural Water Association, and the Water Information Sharing and Analysis Center. State leadership and messaging to connect water systems with these tools and resources is essential to ensure that utility leaders assess and mitigate critical cyber risks. Additionally, Homeland Security Advisors are also a resource to providing links to federal cybersecurity efforts and access to relevant information about these threats.

<https://www.epa.gov/newsreleases/biden-harris-administration-engages-states-safeguarding-water-sector-infrastructure#:~:text=Disabling%20cyberattacks%20are%20striking%20water,significant%20costs%20on%20affected%20communities>

Government Regulations and Recommendations to Cyber-secure Your ICS, SCADA and all OT



- [EPA Memorandum: Addressing Public Water System Cybersecurity in Sanitary Surveys \[March 3, 2023 EPA Memorandum\]](#)

[EPA Cybersecurity for the Water Sector](#)

- EPA: [Water Cybersecurity Assessment Tool and Risk Mitigation Plan Template \(xlsx\)](#) (100.48 KB, 03/31/2023)
- EPA: [Guidance on Evaluating Cybersecurity During Public Water System Sanitary Surveys \(pdf\)](#) (883.93 KB, 02/23, 817-B-23-001) (Checklist in Appendix) **NOTE: THIS MEMORANDUM HAS BEEN SWITCHED FROM MANDATORY AND PART OF THE REGULAR SANITARY SURVEY TO VOLUNTARY... FOR NOW**

THE WHITE HOUSE

- [Presidential Executive Order on Improving the Nation's Cybersecurity - May 12, 2021 \[Executive Order 14028\]](#)

"The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT))."

The Office of Management and Budget (OMB) issued [Memorandum 21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents](#), on August 27, 2021 [\[full Memorandum 21-31\]](#), in accordance with Executive Order 14028, Improving the Nation's Cybersecurity. The memorandum established federal agency requirements to increase the government's visibility "before, during, and after a cybersecurity incident." M-21-31 describes logs that agencies must capture as well as any required retention times. It also establishes a maturity model to track agency implementation. This document provides operational guidance to assist agencies with implementation of the M-21-31 requirements.

→ **US National Archives and Records Administration Updates Record Retention Rules - January 14, 2023 ...federal agencies must keep full capture packet data for at least 72 hours and cybersecurity event logs for 30 months.**



- [Internet of Things Cybersecurity Improvement Act of 2020 \[\(U.S Public Law 116-207; December 4, 2020\)\]](#)

[National Institute of Standards and Technology \(NIST\)](#) has set "guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices." *[Essentially, all IoT (including OT (Operational Technology) and ICS (Industrial Control System) devices like UPS (Uninterruptible Power Supplies), PDU (Power Distribution Units), etc. that support an IT device, that are purchased today, and in the future, must be cyber-secured and compliant]*



→ 8 → 33

4




Cybersecurity is For Everyone


- Recognize and Report Phishing
- Use Strong Passwords
- Turn on Multifactor Authentication (MFA)
- Update Software




MFA uses...



Something You Know
Like a PIN number or a password



Something You Have
Like an authentication application or a confirmation text on your phone



Something You Are
Like a fingerprint or face scan

Brian Wilson
Lauren Wisniewski
September 11, 2024

8



TLP: CLEAR

Top Cyber Actions for Securing Water Systems

4. Conduct an Inventory of OT/IT Assets

Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.

- **Free service:** [EPA's Cybersecurity Technical Assistance Program](#) supports you in conducting an inventory.
- **Free tool:** A first step in conducting an inventory is identifying the devices on the network. [CISA's Malcolm tool](#) enables network monitoring with custom parsers designed for industrial control system (ICS)/OT protocols.

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

Develop

Understand incident response actions, roles, responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.

- **Free resources:** EPA's [Cybersecurity Action Checklist](#) and CISA's [Incident Response Plan \(IRP\) Basics](#) help to develop cyber incident response plans. The [Joint CISA-FBI-EPA Water Incident Response Guide](#) provides valuable information on how to work with federal response partners before, during, and after a cyber incident. Note: See this guide for contact information for [CISA](#), [FBI](#), and the [EPA Water Infrastructure and Cyber Resilience Division](#).

Exercise

Test your incident response plan annually to ensure all operators are familiar with roles and responsibilities.

- **Free tools:** [CISA Tabletop Exercise Package \(CTEP\)](#) and [EPA tabletop exercise \(TTX\)](#) scenario tools assist critical infrastructure owners and operators in developing their own tabletop exercises to meet their specific needs.

6. Backup OT/IT Systems

Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule: 3) Keep three copies: one primary and two backups; 2) Keep the backups on two different media types; 1) Store one copy offsite.

- **Free resources:** [CISA's Cyber Essentials Toolkit Chapter 5: Your Data](#) and [NIST's Protecting Data From Ransomware and Other Data Loss Events](#) provide guidance on backing up your systems.

7. Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and keep all systems up to date with patches and security updates. Prioritize OT patches in accordance with [CISA's Known Exploited Vulnerabilities \(KEV\) catalog](#) during scheduled downtime of OT equipment; prioritize patches in IT, as applicable. [CISA's Secure our World Campaign](#) provides guidance on updating software.

8. Conduct Cybersecurity Awareness Training

Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.

- **Free resources:** See [EPA Cybersecurity Training](#) and CISA's free [Industrial Control Systems](#) cybersecurity virtual training to learn how to protect against cyberattacks to critical infrastructure. Also see [CISA's Secure our World Campaign: Employee Phishing Training](#) for practical steps to help your employees avoid phishing scams.

Support

If you require additional support for implementing any of these actions, contact [EPA](#) and/or your regional [CISA cybersecurity advisor](#) for assistance.

TLP: CLEAR

2

Topic	Topic Number	Checklist Number	Question	Response	Recommendation
Account Security	1.0	1.1	Does the PWS detect and block repeated unsuccessful login attempts?		When technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until remediated by an Administrator.
		1.2	**Does the PWS change default passwords?		When feasible, change of default manufacturer or vendor passwords before equipment or software is put into service.
		1.3	**Does the PWS require multi-factor authentication (MFA) whenever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?		Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.
		1.4	**Does the PWS require a minimum length for passwords?		When feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.
		1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?		Assign System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.
		1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?		Require a single user to have two different usernames and passwords, one set to be used to access the IT network, and the other set to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.
		1.7	**Does the PWS prevent disk-to-disk access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?		Use of alpha accounts to terminate access to accounts or networks upon retirement or termination of those making access unnecessary.
Device Security	2.0	2.1	Does the PWS require approval before new software is installed or deployed?		Only allow Administrators to install new software on a PWS-owned device.
		2.2	Does the PWS disable Microsoft Office macros, or similar embedded code, by default on all assets?		Disable embedded macros and similar executable code by default on all assets.
		2.3	**Does the PWS maintain an updated inventory of all OT and IT network assets?		Regularly review the list (manually) and maintain a list of all OT and IT assets with an IP address. This includes third party and legacy (i.e., vendor) equipment.
		2.4	Does the PWS prohibit the connection of untrusted hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?		When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports) on a laptop to prevent untrusted devices from connecting.
		2.5	**Does the PWS maintain current documentation detailing the setup and settings (i.e., configurations) of critical OT and IT assets?		Maintain accurate documentation of the operational current configuration of critical IT assets, including software and firmware, hardware.
Data Security	3.0	3.1	Does the PWS collect security logs (e.g., system and network access, malware detection) to assist both in incident detection and investigation?		Collect and store logs and/or network traffic data to assist in detecting cyberattacks and investigating suspicious activity.
		3.2	Does the PWS protect security logs from unauthorized access and tampering?		Protect security logs in a remote location or otherwise that cannot be accessed by a compromised or otherwise untrusted asset.
		3.3	Does the PWS use effective encryption to maintain the confidentiality of data in transit?		When sending information and data, use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) respective standards.
		3.4	Does the PWS use encryption to maintain the confidentiality of stored sensitive data?		Protect data on other disks, including external (i.e., removable and removable) drives that.
Policy and Training	4.0	4.1	**Does the PWS have a named role/responsible that is responsible and accountable for planning, executing, and execution of cybersecurity activities within the PWS?		Identify user roles/responsible/responsible for cybersecurity within the PWS. Whoever (the role) is responsible, this is then a range of all PWS cybersecurity activities.
		4.2	Does the PWS have a named role/responsible that is responsible and accountable for planning, executing, and execution of OT-specific cybersecurity activities?		Identify user PWS responsible/responsible for ensuring planning, executing, and execution of OT-specific cybersecurity activities.
		4.3	**Does the PWS provide at least annual training for all PWS personnel that covers basic cybersecurity concepts?		Conduct annual basic cybersecurity training for all PWS personnel.

Topic	Topic Number	Checklist Number	Question	Response	Recommendation
Governance		4.4	Does the PWS offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties?		Provide specialized OT-focused cybersecurity training to all personnel who use OT assets.
		4.5	Does the PWS offer regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?		Facilitate meetings between OT and IT personnel to provide opportunities for all parties to better understand organizational security needs and to strengthen working relationships.
Vulnerability Management	5.0	5.1	**Does the PWS patch or otherwise mitigate known vulnerabilities within the recommended timeframe?		Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.
		5.2			N/A
		5.3			N/A
		5.4	Does the PWS ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol)?		Eliminate unnecessary exposed ports and services on public-facing assets and regularly review.
		5.5	**Does the PWS eliminate connections between its OT assets and the Internet?		Eliminate OT asset connections to the public Internet unless explicitly required for operations.
		5.6			N/A
Supply Chain / Third Party	6.0	6.1	**Does the PWS include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services?		Include cybersecurity as an evaluation criterion when procuring assets and services.
		6.2 / 6.3	**Does the PWS require that all OT and IT vendors and service providers notify the PWS of any security incidents or vulnerabilities in a risk-informed timeframe?		Require vendors and service providers to notify the PWS of potential security incidents and vulnerabilities within a stipulated timeframe described in procurement documents and contracts.
Response and Recovery	7.0	7.1	Does the PWS have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterSAC, cyber insurance provider)?		Document the procedure for reporting cybersecurity incidents promptly to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats.
		7.2	**Does the PWS have written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly practiced and updated?		Develop, practice, and update an IR plan for cybersecurity incidents that could impact PWS operations. Participate in tabletop exercises to improve responses to any potential cyber incidents.
		7.3	**Does the PWS backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?		Maintain, store securely and separately, and test backups of critical PWS OT and IT systems.
		7.4	**Does the PWS maintain updated documentation describing network topology (i.e., connections between all network components) across PWS OT and IT networks?		Maintain complete and accurate documentation of all PWS OT and IT network topologies to facilitate incident response and recovery.
Other	8.0	8.1	Does the PWS segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g., by IP address and port)?		Require connections between the OT and IT networks to pass through an intermediary, such as a firewall, bastion host, jump box, or demilitarized zone, which is monitored and logged.
		8.2	Does the PWS keep a list of threats and adversary tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the PWS and have the capability to detect instances of key threats?		Receive CISA alerts and maintain documentation of TTPs relevant to the PWS.
		8.3	Does the PWS use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?		Ensure that email security controls are enabled on all corporate email infrastructure.



[EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation’s Drinking Water - May 20, 2024](#)

WASHINGTON – Today, May 20, the U.S. Environmental Protection Agency issued an [enforcement alert](#) outlining the urgent cybersecurity threats and vulnerabilities to community drinking water systems...

... Today's alert emphasizes the importance of EPA’s ongoing inspection and enforcement activities under [Safe Drinking Water Act section 1433](#). The agency will increase the number of planned inspections and, where appropriate, will take civil and criminal enforcement actions, including in response to a situation that may present an imminent and substantial endangerment. Inspections will ensure that water systems are meeting their requirements to regularly assess resilience vulnerabilities, including cybersecurity, and to develop emergency response plans...

America's Water Infrastructure Act Section 2013: Risk and Resilience Assessments and Emergency Response Plans

On **October 23, 2018**, **America’s Water Infrastructure Act (AWIA)** was signed into law. AWIA Section 2013, which amended Section 1433 of the Safe Drinking Water Act (SDWA), requires community (drinking) water systems (CWSs) **servicing more than 3,300 people** to develop or update **risk and resilience assessments (RRAs)** and **emergency response plans (ERPs)**. The law specifies the components that the RRAs and ERPs must address, and establishes deadlines by which water systems must certify to EPA completion of the RRA and ERP. The [Federal Register Notice for New Risk Assessments and Emergency Response Plans for Community Water Systems](#) is available.

AWIA Section 2013 also states that EPA should provide guidance and technical assistance to water systems that serve less than 3,301 people on how to conduct RRAs and ERPs, though these systems are not required to certify completion to EPA.

Certification Deadlines

*ERP certifications are due six months from the date of the RRA certification. The dates shown above are certification dates based on a utility submitting a RRA on the final due date.

Population Served	Previous RRA Deadline	Next 5-Year Submission Cycle RRA Deadline
≥100,000	March 31, 2020	March 31, 2025
50,000-99,999	December 31, 2020	December 31, 2025
3,301-49,999	June 30, 2021	June 30, 2026

Population Served	Previous ERP Deadline*	Next 5-Year Submission Cycle ERP Deadline*
≥100,000	September 30, 2020	September 30, 2025
50,000-99,999	June 30, 2021	June 30, 2026
3,301-49,999	December 31, 2021	December 31, 2026



Incident Response Plan (IRP) Basics

OVERVIEW

An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization *before, during, and after* a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a cybersecurity [list](#) of key people who may be needed during a crisis.

BEFORE A CYBERSECURITY INCIDENT

- **Train the staff.** All staff need to understand their role in maintaining and improving the security of the organization. That includes knowing how to report suspicious events. Be gracious when people report false alarms. Reward people who come forward to report suspicious events as part of your commitment to a culture of security.
- **Review your plan with an attorney.** Your attorney may instruct you to use a completely different IRP template. Attorneys often have preferences on how to engage with outside incident response vendors, law enforcement, and other stakeholders.
- **Meet your CISA regional team.** You can find your [regional office information here](#). Within each CISA Region are your local and regional Protective Security Advisors (PSAs), Cybersecurity Advisors (CSAs), Emergency Communications Division Coordinators, and other CISA personnel to handle a wide array of needs.
- **Meet your local law enforcement agency (LEA) team.** In coordination with your attorney, get to know your local police or FBI representatives. The time to figure out how to notify LEA representatives isn't in the heat of battle.
- **Print these documents** and the associated contact list and give a copy to everyone you expect to play a role in an incident. During an incident, your internal email, chat, and document storage services may be down or inaccessible.
- **Develop an incident staffing and stakeholder plan.** What roles will everyone play? Which people and groups will need to be notified that won't be top of mind during the incident? Examples include the board of directors, key investors, and critical partners.
- **Review this plan quarterly.** The best IRPs are living documents that evolve with business changes.
- **Prepare press responses in advance.** If a reporter calls you, claiming to have data stolen from your file servers, what will you say? Having a good "holding statement" will help.
- **Select an outside technical resource/firm** that will investigate potential compromises.
- **Conduct an attack simulation exercise**, sometimes called a tabletop exercise, or TTX. A TTX is a role-playing game where a facilitator presents a scenario to the team. The exercise might start with the head of communications receiving an email from a reporter about rumors of a hack. The facilitator will provide other updates during the game to see how everyone plays their role. Every sports team rehearses, and you should too!

DURING A CYBERSECURITY INCIDENT

- **Assign an Incident Manager (IM).** This person leads the response. They manage communication flows, update stakeholders, and delegate tasks. However, the IM does not perform any technical duties. During a time of crisis, time dilation affects people's perception of time passing. The IM will monitor the clock to avoid that common problem. The IM may also lead the retrospective meeting (outlined below) to gather

DEFEND TODAY.
SECURE TOMORROW

Incident Response Plan (IRP) Basics

lessons learned.

- **Assign Tech Manager (TM).** The TM will serve as the subject matter expert. They will bring in other internal and possibly external technical experts (with the consent of the IM and possibly your attorney!)
- **Assign Communications Manager (CM).** The CM will interact with reporters, post updates on social media, and may interact with external stakeholders (like shareholders).

AFTER A CYBERSECURITY INCIDENT

- **Hold a formal retrospective meeting** (sometimes called a "postmortem"). In the retrospective, the IM will report out the known incident timeline and ask for additions and edits. They will then ask for analysis from the incident response team and suggest areas for improvement.
 - **Note: Retrospectives must be blameless.** For retrospectives to have any value, all participants need to feel free to openly discuss the incident in a safe and supportive environment. Security incidents are rarely the result of one person's action. They are almost always the result of a failure of the overall system. The retrospective will examine *people, processes, and technologies*. The focus should be on the *processes* and ways to improve them.
- **Update policies and procedures** based on the retrospective meeting.
- **Communicate** the findings to your staff. Transparency builds trust and many staff will appreciate hearing how seriously the executives consider security. That's how you build a culture of security.

SEE ALSO

- NIST guidance: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- CISA guidance: <https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability>

EPA Resources

- [EPA: Cybersecurity Technical Assistance Program for the Water Sector](#): The Cybersecurity Technical Assistance Program will support primacy agencies and water systems in implementing cybersecurity measures. Users may submit questions or request to consult with a subject matter expert regarding cybersecurity in PWS sanitary surveys or other cybersecurity matters.
 - [EPA: Water Sector Cybersecurity Evaluation Program](#): EPA's Cybersecurity Evaluation Program will conduct a cybersecurity assessment for PWSs. The assessment will follow the checklist in the guidance on Evaluating Cybersecurity in PWS Sanitary Surveys which will then generate a report that will highlight gaps in cybersecurity, including potential significant deficiencies.
 - [Small Public Water System Operator Resources Knowledge Retention Tool](#): The [Knowledge Retention Tool Spreadsheet for Small Water Systems](#) is an Excel spreadsheet that helps operators consolidate system information into one location, enabling increased organization and coordination among operators. Designed to assist in personnel transition, the tool encompasses a wide variety of information that a new or contract operator would need to effectively manage and operate a small water system.
-

EPA Resources - Training

[EPA Cybersecurity Training Page](#)

Recorded Training

- [EPA Cybersecurity IOI Training Video/Webinar](#)
 - Cybersecurity IOI Webinar: This webinar is an introduction to the basic principles of cybersecurity.
 - The presentation slides can be downloaded: [Cybersecurity IOI Webinar Slides \(pdf\)](#) (1.81 MB, 03/03/23).
 - NOTE: The following states have approved this training for CEUs: AZ – 0.5 PDH (DW/WW), CN – 0.5 TCH (WW), MN – 1.0 CH (DW), NV – 1.0 CH (WW), NH – 1.0 CH (DW), NM – 0.5 TCH (Both), VT – 1.0 CH (WW), WY – 0.5 CH (Both)
 - To receive a certificate of completion for the training, please fill out and complete the following post-training quiz here: [Cyber 101 Quiz \(pdf\)](#) (250.11 KB) and submit the completed quiz to the following email address: WaterCyberTA@epa.gov. You should receive your certificate of completion within 3-5 business days. If you have any questions, please feel free to reach out to WaterCyberTA@epa.gov.

EPA WCAT Cybersecurity Assessment Training for Water and Wastewater Systems

- This webinar demonstrates how to use the Water Cybersecurity Assessment Tool (WCAT) to conduct cybersecurity assessments at water and wastewater systems.

Additional Training Resources

- Develop and Conduct a Cybersecurity Tabletop Exercise (TTX): Tool used to plan, conduct, and evaluate a cybersecurity tabletop exercise.
 - CISA's Tabletop Exercise Packages (CTEPs): Cybersecurity-based threat vector topics including ransomware, insider threats, phishing, and Industrial Control System compromise, featuring a Water and Wastewater Systems Situation Manual.
 - CISA FedVTE: Free virtual training to gain a better understanding of cybersecurity. Classes provide a certificate of completion which could grant CEUs.
 - CISA Incident Response Training: Free training that provides information on cybersecurity awareness and organizational best practices.
 - CISA Industrial Control System Cybersecurity Training: Free training that provides information on cybersecurity for industrial control systems. Trainings are either self-virtual or instructor led virtual.
-

Cybersecurity & Ransomware Insurance for PWSs

Considerations for 2024...

Eligibility for new policies may require:

- Multi-factor Authentication
- Automated Patching Solution (for IT software and firmware)
- Proof/Attestation:
 - OT Devices and SCADA not Connected/Visible on the Internet
 - The OT Network has no IT devices, and the IT Network has no OT Devices
 - Scanning/Threat Hunting

Considerations:

Coverages that make robust additions to the benefit of policy holding PWSs:

- Built-in Voluntary Notification (coverage for expenses incurred to notify affected parties of a privacy breach)
- Duty-to-defend (insurer's obligation to provide legal defense for a lawsuit)
- No/minimal Exclusion for State-sponsored Cyberattack or “Moonlighting” activities of Cyber-soldiers
- Full Ransomware coverage
- No Phishing/Social Engineering Sublimits

Also, look for a cybersecurity “program” which also includes bundled and/or discounted...

- OT Threat Hunting/Discovery & Response Tool
- Annual Employee Cybersecurity Training
- The 33 EPA Cybersecurity Controls for PWSs

Review: OT Compliance and Best Practices

- OT (Operational Technology) Asset Inventory
- OT Cyber Threat Monitoring/Hunting/Discovery (and Response)
- Isolate OT Network and Devices from IT Network and Devices
- PCAP Files stored for CISA/other Forensics
- Develop and Implement Security Policies for Staff
- Staff Training on OT Cybersecurity, IT Cybersecurity, Phishing

Recommendations

- Do the “4” of 4→8→33
- Do the “8” of 4→8→33
- 33 Cybersecurity Controls for PWSs:
 - Add Visibility and Threat Hunting/Discovery for OT & IT Networks/Devices
 - Add/Configure Your OT Firewall Appropriately for OT Traffic
 - Implement Policies & Training to Address “Human” Weak Spots, Enable ERP
- Dig into the Cybersecurity Sections of these Required Documents:
 - Risk & Resilience Assessment
 - ERP Emergency Response Plan
- Secure the Communications Between Your SCADA and ICSs
- Implement a Data Diode-based OT Firewall

Recap & Q&A



AlphaGuardian™

OPERATIONAL TECHNOLOGY SECURITY MADE SIMPLE

AlphaGuardian Networks, LLC

Main Office:

111 Deerwood Road, suite 200

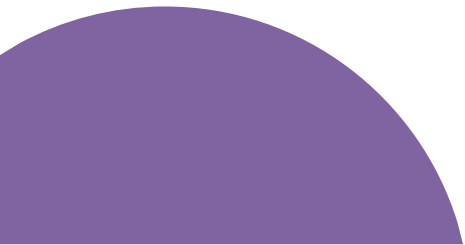
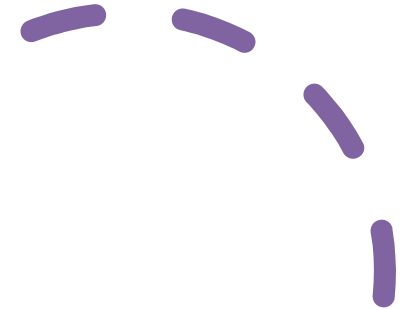
San Ramon, CA. 94583

(925) 421-0050

(888) 990-ALPHA

Principal Contact: Bob Hunter

bhunter@alphaguardian.net



Proud Member



California
Rural Water Association



Evergreen
Rural Water of Washington



Oregon Association of Water Utilities



We make it easy.



CYBER THREAT DISCOVERY & RESPONSE



SECURE ICS/SCADA COMMUNICATIONS



AlphaGuardian™

OPERATIONAL TECHNOLOGY SECURITY MADE SIMPLE

ALPHAGUARDIAN.NET



Main Office:
111 Deerwood Road, suite 200
San Ramon, CA 94583
(925) 421-0050
(888) 990-ALPHA

Contact:
Principal Contact: Bob Hunter
bhunter@alphaguardian.net
or
GM: Steven Menges
smenges@alphaguardian.net
mobile: 646-391-3364

Compliance Tool Example

EPA Cybersecurity Checklist for Sanitary Surveys

Utility ID: _____
 PWS Staff (Initials Only): _____
 Assessment Date: _____
 Assessor: _____



Topic	Topic Number	Checklist Number	Question	Response	Recommendation	Explanation of Response
Account Security	1.0	1.1	Does the PWS detect and block repeated unsuccessful login attempts?		Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.	
		1.2	**Does the PWS change default passwords?		When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.	
		1.3	**Does the PWS require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?		Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.	
		1.4	**Does the PWS require a minimum length for passwords?		Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.	
		1.5	Does the PWS separate user and privileged (e.g., System Administrator) accounts?		Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.	
		1.6	Does the PWS require unique and separate credentials for users to access OT and IT networks?		Require a single user to have two different usernames and passwords: one set is to be used to access the IT network, and the other set is to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.	
Device Security	2.0	1.7	**Does the PWS immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?		Take all steps necessary to terminate access to accounts or networks upon a change in an individual's status making access unnecessary.	
		2.1	Does the PWS require approval before new software is installed or deployed?		Only allow Administrators to install new software on a PWS-issued asset.	
		2.2	Does the PWS disable Microsoft Office macros, or similar embedded code, by default on all assets?		Disable embedded macros and similar executable code by default on all assets.	
		2.3	**Does the PWS maintain an updated inventory of all OT and IT network assets?		Regularly review (no less than monthly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.	
		2.4	Does the PWS prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?		When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.	
		2.5	**Does the PWS maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?		Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version.	
Data Security	3.0	3.1	Does the PWS collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?		Collect and store logs and/or network traffic data to aid in detecting cyberattacks and investigating suspicious activity.	
		3.2	Does the PWS protect security logs from unauthorized access and tampering?		Store security logs in a central system or database that can only be accessed by authorized and authenticated users.	
		3.3	Does the PWS use effective encryption to maintain the confidentiality of data in transit?		When sending information and data, use Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption standards.	
		3.4	Does the PWS use encryption to maintain the confidentiality of stored sensitive data?		Do not store sensitive data, including credentials (i.e., usernames and passwords) in plain text.	
Personnel and Training	4.0	4.1	**Does the PWS have a named role/position/title that is responsible and accountable for planning, resourcing, and execution of cybersecurity activities within the PWS?		Identify one role/position/title responsible for cybersecurity within the PWS. Whoever fills this role/position/title is then in charge of all PWS cybersecurity activities.	
		4.2	Does the PWS have a named role/position/title that is responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities?		Identify one PWS role/position/title responsible for ensuring planning, resourcing, and execution of OT-specific cybersecurity activities.	
		4.3	**Does the PWS provide at least annual training for all PWS personnel that covers basic cybersecurity concepts?		Conduct annual basic cybersecurity training for all PWS personnel.	
			Does the PWS offer OT-specific cybersecurity training at least an annual basis?		Provide specialized OT-focused cybersecurity training to all personnel.	

Governor	4.4	Does the PWS offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties?		Provide specialized OT-focused cybersecurity training to all personnel who use OT assets.		
	4.5	Does the PWS offer regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?		Facilitate meetings between OT and IT personnel to provide opportunities for all parties to better understand organizational security needs and to strengthen working relationships.		
Vulnerability Management	5.0	5.1	**Does the PWS patch or otherwise mitigate known vulnerabilities within the recommended timeframe?	Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.		
		5.2		N/A		
		5.3		N/A		
		5.4	Does the PWS ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol)?		Eliminate unnecessary exposed ports and services on public-facing assets and regularly review.	
		5.5	**Does the PWS eliminate connections between its OT assets and the Internet?		Eliminate OT asset connections to the public Internet unless explicitly required for operations.	
		5.6		N/A		
Supply Chain / Third Party	6.0	6.1	**Does the PWS include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services?	Include cybersecurity as an evaluation criterion when procuring assets and services.		
		6.2 / 6.3	**Does the PWS require that all OT and IT vendors and service providers notify the PWS of any security incidents or vulnerabilities in a risk-informed timeframe?	Require vendors and service providers to notify the PWS of potential security incidents and vulnerabilities within a stipulated timeframe described in procurement documents and contracts.		
Response and Recovery	7.0	7.1	Does the PWS have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterISAC, cyber insurance provider)?	Document the procedure for reporting cybersecurity incidents promptly to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats. Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022, CISA will establish procedures that may apply to public water systems. This recommendation will be revised as necessary when those procedures are issued.		
		7.2	**Does the PWS have written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly practiced and updated?	Develop, practice, and update an IR plan for cybersecurity incidents that could impact PWS operations. Participate in tabletop exercises to improve responses to any potential cyber incidents.		
		7.3	**Does the PWS backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?	Maintain, store securely and separately, and test backups of critical PWS OT and IT systems.		
		7.4	**Does the PWS maintain updated documentation describing network topology (i.e., connections between all network components) across PWS OT and IT networks?	Maintain complete and accurate documentation of all PWS OT and IT network topologies to facilitate incident response and recovery.		
Other	8.0	8.1	Does the PWS segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g., by IP address and port)?	Require connections between the OT and IT networks to pass through an intermediary, such as a firewall, bastion host, jump box, or demilitarized zone, which is monitored and logged.		
		8.2	Does the PWS keep a list of threats and adversary tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the PWS and have the capability to detect instances of key threats?	Receive CISA alerts and maintain documentation of TTPs relevant to the PWS.		
		8.3	Does the PWS use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?	Ensure that email security controls are enabled on all corporate email infrastructure.		

SAMPLE ONLY



Cyber Event and Incident Collection Form

-----This section to be completed by PWS (Public Water System) Security officer-----

- PWS Event and Incident Control #:
(e.g. 12252022_01, 12262022_02, etc.)
- PWS site name and identifying information (if applicable)
- PWS point of contact information (name, position, telephone, email)
- Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)
- FOR US MILITARY BASE PWS:
 - U.S. Government Program Manager point of contact (name, position, telephone, email)
 - Contract number(s) or other type of agreement affected or potentially affected
 - Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
 - Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)

Cyber Event/Incident Exercise: CISA Submission

This section to be completed by PWS staffer who discovered (or was first notified about) the event/incident. Note: An Event is an exception to the normal operation of our Public Water System (PWS) IT infrastructure, systems, or services. Not all events become incidents, but all events must be documented as if they are incidents.

INSTRUCTIONS: Please fill out as many fields as possible and immediately communicate the information per the PWS Incident Response Policy.

- PWS point of contact information (name, position, telephone, email):
- Date and time incident discovered:
- Date and time incident started/began:
- How incident was discovered:
- Impact of incident (to date):
- Incident location:
- Platforms or systems involved:
- Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
- Description of technique or method used in cyber incident:
- Incident outcome (successful compromise, failed attempt, unknown)
- Incident/Compromise narrative (Ex: Chronological explanation of event/incident, threat actor TTPs, indicators of compromise, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred):
- What response actions have already been taken:
- Who has been notified (to date):
- Any additional information you deem relevant:

version 1.0