

Defending U.S. Water Systems: What a Real National Plan Requires, and Where a Preemptive Layer Delivers It Today

The CyberScoop five-part plan for water-sector cybersecurity, read against PacketViper's preemptive, agentless architecture.

CRITICAL INFRASTRUCTURE PERSPECTIVE

What's inside

The October 2026 CyberScoop op-ed's plan to defend U.S. water systems, from zero trust to an AI-capable defense cohort, and how PacketViper's deployed architecture (agentless inline enforcement, AMTD, command-level Modbus protection, autonomous Remote Security Units, and on-premises AI advisory) delivers each element for utilities of every size, affordably.

Prepared October 6, 2026

Why This Matters

On October 5, 2026, CyberScoop published an op-ed by Franklin D. Kramer, Robert J. Butler and Melanie J. Teplinsky arguing that the United States needs a real plan to defend its water systems. The trigger was this summer's campaign by Iranian actors against water systems in 12 states. CISA has since reported that more than 100 internet-exposed water systems were targeted in July alone, most often through programmable logic controllers (PLCs) connected directly to cellular modems. The authors warn that a broad attack on water infrastructure could have consequences comparable to a public health crisis affecting the entire country.

Their diagnosis is technical, legal and practical. About 80% of U.S. water systems lack even basic cyber hygiene. The EPA lacks clear statutory authority to impose broad cybersecurity requirements, and its 2023 attempt was withdrawn after legal challenges. Roughly 45,000 systems serve 3,300 people or fewer, and most sit below the "cyber poverty line," without the funding, staff or expertise for effective security. Meanwhile, AI systems can now plan, test and execute attacks in cycles measured in minutes, down to seconds.

The authors also name the reason policymakers have struggled to respond: "the cost and complexity of adopting stronger technical defenses," combined with a highly fragmented sector. Their answer is a five-part federal program. Below, each element of that program is summarized on its own, followed by a look at how PacketViper's architecture, already deployed in water and wastewater environments, is positioned to deliver it: affordably, ready for AI-speed threats, and at every scale from a single unmanned lift station to a utility with hundreds of sites.

A note on how to read this

This is commentary and analysis of a published op-ed, read against PacketViper's stated architecture and field experience. Customer references are anonymized. Where PacketViper complements a recommendation rather than fulfilling it, that is noted rather than implied.

The Plan, Element by Element

The op-ed's first element, stronger technical capabilities, rests on two distinct pillars: zero trust architecture and secure code. They are treated separately here, for six items in all.

1. Stronger Technical Capabilities: Zero Trust Architecture

The authors call for water systems to adopt zero trust architecture, which permits only authenticated, minimum-necessary access to resources and segments networks so that a breach in one area does not compromise the entire system. They argue that such an architecture could have blocked the unauthorized intrusions used in the summer attacks and note that zero trust is already widely used across other sectors and supported by commercial providers.

Source: [The US needs a real plan to defend its water systems | CyberScoop](#)

HOW PACKETVIPER ADDRESSES THIS

The obstacle in water is that most zero trust frameworks are built around identity on the endpoint, and the endpoints in a treatment plant are PLCs, RTUs and HMIs that cannot run an agent and speak protocols such as Modbus and DNP3 that have no authentication at all. PacketViper enforces zero trust at the network layer instead. It sits inline as a transparent Layer 2 bridge, with no readdressing and no agents, and uses context groups, custom rules and sensors to define exactly which devices may talk to which, over which ports, and during which hours. Anything outside that pattern is stopped and alerted on, not just logged. Enforcement is scoped to the device, never the subnet, so one violating source is contained while production keeps running. Deployment follows a "start open, narrow in" sequence: observe and profile legitimate traffic first, then enforce. That is what makes a phased adoption realistic for operators who cannot risk a disruption to treatment.

2. Stronger Technical Capabilities: Formal Methods and Code Mending

The authors also call for formal methods (memory-safe languages, mathematically verified code and secure microkernels) and AI-assisted "code mending" to reduce vulnerabilities in software that cannot safely fail. They note that while the summer attackers did not appear to exploit code flaws, a high-level adversary such as China would be likely to, and that much of the control software in U.S. water utilities comes from a small group of industrial automation vendors.

Source: [The US needs a real plan to defend its water systems | CyberScoop](#)

HOW PACKETVIPER ADDRESSES THIS

PacketViper does not rewrite vendor code, and nothing here argues against the authors' push for safer software. What it addresses is the long gap between today and the day a utility's installed base actually runs verified code. A large share of water-sector OT is decades old and cannot be patched at all. PacketViper's command-level Modbus protection parses each packet for unit ID, function code, register or coil address and the specific value being written. A utility can let a historian read tank levels while blocking any write to a chemical-dosing register from an untrusted source, or any diagnostic command that could force a controller into listen-only mode. An exploit that depends on a malicious command reaching the controller is stopped at the wire, whether or not the underlying flaw has been discovered. This is a compensating control that works on the code utilities run today, while the longer-term work on formal methods proceeds.

3. Support Large Water Systems

The authors propose that Congress require large water systems to adopt zero trust, code-mending tools and formal methods on a phased schedule, with tax credits to offset the cost of developing, implementing and maintaining those protections. A relatively small number of large systems serve about half of the U.S. population, and they have long been targets of sophisticated adversaries, including China's Volt Typhoon campaign.

Source: [The US needs a real plan to defend its water systems | CyberScoop](#)

HOW PACKETVIPER ADDRESSES THIS

Large systems need enforcement that scales without multiplying headcount or hardware. The platform is rated at 501,496 connections per second, and its embedded analytics engine returns sub-second queries across billions of events. Federation and centralized management let a policy authored once be enforced on every unit in the deployment. The Hive capability means that when any unit detects malicious behavior, it blocks locally

and propagates that block to every other unit in milliseconds, without waiting on a human to push a policy. Against a Volt Typhoon-style adversary, whose method is quiet, long-dwell reconnaissance, Automated Moving Target Defense (AMTD) is the relevant control: it continuously rotates the visible attack surface so that a map built over months is stale by the time it is used. On the mandate side, compliance reporting maps to 21 frameworks and 258 controls, with audit evidence generated as a byproduct of normal enforcement. In one large critical infrastructure deployment spanning more than 800 unattended remote OT sites, the client cut firewall utilization by roughly 60% and avoided an estimated \$7 million in planned WAN and satellite upgrades.

4. Assist Midsize Water Systems

For the roughly 4,500 midsize systems, including many municipal utilities, the authors propose a federal program providing technical expertise and financial support, delivered by a federally funded cohort of government and private-sector experts organized into regional teams by geography or technical specialty, with a longer phase-in than for large utilities.

Source: [The US needs a real plan to defend its water systems | CyberScoop](#)

HOW PACKETVIPER ADDRESSES THIS

Midsize utilities typically have an IT team but no 24/7 security operations center, and they cannot absorb a tool that needs constant tuning. PacketViper is designed to be light-touch: most installations complete in hours, not weeks, and after an initial tuning period the system operates autonomously with periodic review. Deceptive responders that mimic PLCs, HMIs and SCADA services alert only when something touches what it never should, so a lean team receives signal rather than noise. One platform covers boundary defense, OT enforcement, deception, passive asset discovery and analytics, consolidating functions that would otherwise take five to seven separate tools. That matters to a regional expert team as much as to the utility: a team supporting dozens of utilities can work from one console rather than a different stack at every site.

Two water-sector examples illustrate the fit. A long-standing municipal customer, now in its third multi-year contract term, extended PacketViper from City Hall IT to a 28-location water and wastewater OT environment, reducing firewall traffic, SIEM volume and false positives along the way. A large metropolitan wastewater utility evaluating the platform at its primary pump station and remote facilities surfaced unauthorized east-west traffic between devices that should never communicate, along with an operational fault that had been saturating the link to unmanned sites. No existing tool had revealed either one.

5. Create a Safe Operations Posture for Small Water Systems

Systems serving 3,300 people or fewer rarely have cybersecurity resources and often depend on remote monitoring because on-site service is beyond their budgets. The summer attacks primarily exploited industrial devices exposed directly to the internet. EPA, FBI and CISA guidance recommended locking devices in "run" mode to prevent remote reprogramming, which reduces risk but forces in-person operation. The authors conclude that small utilities need either the staff for manual operations or secure remote access operated by trained personnel, possibly through a state-led volunteer cybersecurity corps modeled on the National Guard.

Source: [The US needs a real plan to defend its water systems | CyberScoop](#)

HOW PACKETVIPER ADDRESSES THIS

This is the scenario PacketViper's Remote Security Unit (RSU) was built for. The RSU is a ruggedized, industrial-grade, DIN-rail appliance that installs inline in an existing cabinet at a pump station, lift station or well site, on AC

or DC power, with no changes to the PLC. It puts a directly exposed controller behind a managed enforcement point: reads for remote monitoring stay open, while writes from untrusted sources, logins from unapproved geographies and sessions outside approved windows are blocked. In effect, it delivers "run mode" for everyone except the utility's own authorized staff, without taking remote operation away from the utility. The RSU keeps enforcing autonomously if the link to the central office drops, and hardware bypass means physical operations continue if the unit itself loses power. Alerts can be polled over Modbus and shown on the SCADA HMI operators already watch, so the person answering the alarm does not need a security console. For a state-led corps, the same units can be managed centrally across many small systems, so a small number of trained personnel can cover an entire region.

6. Build an AI-Capable Cybersecurity Cohort

The authors propose that the expert cohort include AI specialists, including experts from leading AI companies, who would use AI tools to develop and deploy zero trust and code-mending programs for utilities of every size, working with major industrial-technology vendors and directly with water systems. They stress that AI systems can now "plan, test, and execute attacks in rapid cycles," and that applying AI to protect water systems should be a national priority.

Source: [The US needs a real plan to defend its water systems | CyberScoop](#)

HOW PACKETVIPER ADDRESSES THIS

AI readiness cuts two ways. **Defending against AI-driven attacks:** in a controlled March 2026 study, PacketViper tested an autonomous AI agent framework instructed to be stealthy, mimic legitimate traffic, spawn sub-agents and change its network identity if blocked. Across four configurations, the agent was stopped at the first PacketViper sensor every time. It reached zero internal hosts and exfiltrated no data; and when it provisioned new virtual machines to obtain fresh IP and MAC addresses, each new identity was stopped on its first probe. No AI-specific rules were configured; the sensors ran standard production AMTD settings.

Putting AI to work for defenders: the platform's AI advisory runs on-premises, contextualizing patterns across the full dataset and recommending enforcement actions, with no operational data leaving the utility's environment. That suits a sector understandably wary of sending control-system data to the cloud. And as utilities adopt AI tools of their own, PacketViper's Secure Control Layer for AI enforces what those tools and agents can reach and do on the network. For an AI-capable cohort, this is a ready platform: AI-assisted analysis for the experts, and deterministic, wire-speed enforcement at every site they support.

The Common Thread

Every element of the plan runs into the constraint the authors identified: cost and complexity, multiplied across nearly 50,000 systems of very different sizes. Most approaches to OT security assume capabilities water systems do not have: agents on endpoints, a staffed SOC, a maintenance window and a multi-year integration budget. A defense that will actually reach the sector has to remove those assumptions, and it has to work the same way at the smallest site and the largest.

System tier	What the op-ed calls for	PacketViper deployment
Small (3,300 people or fewer; roughly 45,000 systems)	A safe operations posture; secure remote access run by trained personnel, possibly a state-led cyber corps	One RSU per site, inline in the existing cabinet; autonomous enforcement; alerts into the existing SCADA HMI; central management by a regional team
Midsize (roughly 4,500 systems)	Federal technical expertise and funding; zero trust and code mending on a longer phase-in	Boundary and OT units installed in hours; deception for high-fidelity alerts; one console in place of five to seven tools
Large (roughly 450 systems; about half the population)	Mandated zero trust, code mending and formal methods, phased in with tax credits	Federated enterprise deployment; Hive propagation in milliseconds; 501,496 connections per second; compliance evidence across 21 frameworks

Table 1: One architecture, every tier. System counts are from the CyberScoop op-ed.

PacketViper's positioning, as stated on packetviper.com and in its field deployments, is built around exactly that requirement:

- **Agentless, inline enforcement:** no software on PLCs, RTUs or HMIs, and no network changes. The platform sits in the traffic path as a transparent bridge.
- **Protocol-native control:** Modbus, DNP3, BACnet, S7 and more, enforced down to individual commands and values rather than allow-all or block-all.
- **AMTD and deception:** the visible attack surface keeps moving, so reconnaissance returns stale or misleading results, and any interaction with a deceptive responder is unauthorized by definition.
- **Autonomous edge:** RSUs keep enforcing without a live connection, and Hive propagation pushes a block detected at one site to every other site in milliseconds.
- **AI-ready:** tested against an autonomous AI agent, with on-premises AI advisory and enforcement for the AI tools utilities adopt themselves.
- **Affordable by design:** deployments measured in hours, tool consolidation, and fixed multi-year pricing with no annual escalation. Deployments have typically reduced firewall traffic by 30 to 70% within 90 days and lowered SIEM and SOC costs, which helps offset the investment from year one.

A compensating control that can deploy now

None of this argues against the author's plan. Federal funding, tiered standards, safer code from industrial vendors and a trained cyber corps are all needed, and the \$600 million a year proposed in the Water Safety Shield Act would help. The argument is about timing. The phase-ins described will take years, and adversaries using AI are shortening their timelines, not extending them. A preemptive, agentless layer that protects the control equipment utilities already run, at a cost a small utility can justify and a scale a large one requires, can close much of that window today. That is the fit worth testing directly: PacketViper offers a proof-of-concept against a real environment as a standard option that demonstrates value on day #1 (packetviper.com/proof-of-concept).

Sources

- [The US needs a real plan to defend its water systems \(Kramer, Butler, Teplinsky\) | CyberScoop](#)
- [Over 100 US water utilities had cyberattacks in July, says CISA | SC Media](#)
- [PacketViper | Water and Wastewater](#)
- [PacketViper | Secure Control Layer for AI](#)
- [PacketViper | Cyber Physical Compute Edge](#)
- [PacketViper | Preemptive Network Security for IT and OT \(homepage, capabilities, FAQ\)](#)

About PacketViper

PacketViper delivers Preemptive cybersecurity and Automated Moving Target Defense solutions for OT/ICS and IT practitioners in critical infrastructure industries seeking real-time visibility into their environment's expanding attack surface. Our patented technology allows users to proactively defend OT/ICS assets, remote OT endpoints, and IT infrastructures. PacketViper's agentless detection, prevention, containment, deception, and response technology automates attack detection and prevention from both external and internal threats. Our solutions provide operators with the contextual security data required to act quickly while potential threats are still in motion, and before critical OT/ICS and IT assets are compromised.