KALEN

VALIDATING TRUST ACROSS THE GRID

POWERED BY GRID FRAMEWORK

Issue 03

Monthly Member Publication

KALEN INTELLIGENCE BRIEF

ISSUE No. 3 · AUGUST 2026

Validating Trust Across the Grid. Informing What Comes Next.

CYBERSECURITY | CRITICAL INFRASTRUCTURE | WATER SECURITY | ARTIFICIAL INTELLIGENCE | NERC CIP | FEDERAL POLICY

utc.org/KALEN
Utilities Technology Council

Utilities Technology Council

A Message from UTC

Office of the Vice President, Cybersecurity & Advocacy

Cordell Briggs

Vice President,
Cybersecurity & Advocacy

Utilities Technology Council

For months, this brief has tracked warnings about cybersecurity risks to critical infrastructure. This month, several of those warnings became reality.

Since late July, water utilities in at least a dozen states have been targeted by coordinated attacks on their operational technology. Around the same time, a UK power plant was taken offline for four days by a similar campaign. Days later, five federal agencies confirmed that attackers are now using AI to generate exploit code targeting exposed industrial controllers. On Capitol Hill, lawmakers introduced multiple bills that would, for the first time, make cybersecurity mandatory for critical infrastructure operators rather than a voluntary best practice. On August 26, President Trump signed an Executive Order declaring a national emergency over foreign-sourced bulk-power system equipment, the most direct federal action yet tying supply chain cybersecurity to procurement and equipment restrictions.

The purpose of the KALEN™ Intelligence Brief is to help UTC members understand developments like these before they become operational, procurement, compliance, or business challenges.

This month, we examine NERC's recently closed comment period on proposed cloud services standards; the coordinated cyberattacks on U.S. water utilities and a UK energy generator; the President's new national emergency declaration regarding foreign-sourced bulk-power system equipment; other congressional efforts to mandate critical-infrastructure cybersecurity; and DOE's expanding program to test AI in operational technology environments.

Regulatory & Standards Watch

NERC's Cloud Services Standards Reach a Critical Point

NERC's informal comment period on Project 2023-09, Risk Management for Third-Party Cloud Services, closed on August 21, 2026, marking the end of the industry's first opportunity to weigh in on draft standard language: CIP-002-9, CIP-102-1, CIP-103-1, CIP-105-1, and CIP-113-1, along with an accompanying Implementation Plan.

The proposed approach is notable for what it doesn't do: rather than rewriting the existing CIP standards, NERC created a parallel "100-series" that entities can opt into on a system-by-system basis when using cloud-based systems, with the new System Security Plan approach at its core.

The comment period also drew significant industry scrutiny. Drafting team members have acknowledged in industry discussions that even entities that don't intend to use cloud services for high- or medium-impact BES Cyber Systems may still be affected by the new standards in ways that are not yet fully clarified, signaling that further refinement is likely before the standards move to ballot.

Why It Matters

- Utilities should monitor the drafting team's response to comments and prepare for these standards to move toward a formal ballot in the coming months.
- Suppliers, particularly cloud, telecom, and managed service providers, should track how the "opt-in" scope is clarified, as early signals suggest it may be broader than initially described.
- This is the clearest sign yet that mandatory, cloud-specific CIP requirements are on the horizon. Entities should not wait for a final rule before preparing.

Critical Infrastructure Cyber Alert

Coordinated Cyberattacks Disrupt U.S. Water Utilities and Take a UK Energy Generator Offline

Active, ongoing threat activity. Federal agencies have issued joint advisories with specific mitigations. See Recommended Actions below.

U.S. Water Utilities Hit by Coordinated OT Attacks Across a Dozen States

Since July 27, 2026, water and wastewater utilities in at least a dozen states, including Minnesota, Michigan, Georgia, South Dakota, and New Jersey, have reported cyberattacks on their operational technology as part of a campaign multiple sources have linked to Iran-affiliated actors. The FBI, CISA, and EPA say attackers exploited internet-exposed programmable logic controllers, particularly Rockwell Automation/Allen-Bradley PLCs, by changing passwords and disabling alarms to lock operators out of their own systems. In Minnesota alone, more than 30 water systems were affected. Some incidents degraded water operations, including loss of pressure and flooding, though no drinking water contamination has been reported.

Suspected Iran-Linked Attack Takes UK Power Plant Offline for Four Days

Around the same time, a cyberattack attributed to Iran-linked hackers forced a small-scale UK energy generator offline for four days, which UK officials describe as the first successful cyberattack of its kind against British energy infrastructure. The UK's Department for Energy Security and Net Zero said the wider national grid was never at risk, but the incident prompted the government to brief energy-sector CEOs and issue new security guidance.

Why This Matters to Utilities & Suppliers

- Utilities should treat the water sector attacks as a directly applicable case study: attackers are actively scanning for and exploiting internet-exposed PLCs from multiple manufacturers, not just one.
- The UK incident shows that this activity isn't confined to the U.S. or to any single critical infrastructure sector. It is expanding geographically and across sectors.
- Suppliers of industrial control systems and PLCs should expect heightened customer scrutiny of default configurations, remote access, and internet exposure.

Operational Considerations

- ✓ Identify and remove any PLCs or OT devices that are directly exposed to the internet.
- ✓ Change default passwords and enforce strong authentication across all OT devices and remote access paths.
- ✓ Confirm that the organization can revert to manual operations if automated control systems are compromised.
- ✓ Review the joint FBI/CISA/EPA advisories AA26-097A and AA26-231A for specific indicators of compromise and mitigations.

Legislative & Policy Watch

President Declares National Emergency to Secure the Bulk-Power System

On August 26, 2026, President Trump signed Executive Order 14420, declaring a national emergency under the International Emergency Economic Powers Act regarding foreign-sourced bulk-power system electric equipment. The order generally prohibits the acquisition, importation, transfer, or installation of foreign-produced bulk-power system equipment associated with a "Covered Foreign Entity" when the Secretary of Energy determines that the transaction poses an undue risk of sabotage, unauthorized access, or supply disruption.government and industry.

The order broadly defines bulk-power system electric equipment. It covers transformers, generators, battery energy storage systems, grid-connected inverters, protective relaying, high-voltage circuit breakers, and industrial control systems, including PLCs, RTUs, and intelligent electronic devices, along with associated software, firmware, and remote-access capabilities. Facilities used for local electricity distribution are excluded.

The order isn't limited to future purchases. It also authorizes the Secretary of Energy to impose conditions on equipment installed before the order, including requirements to identify, isolate, monitor, secure, disconnect, replace, or remove it. The Secretary must first consider the effects on reliability, safety, and continuity of service and may phase in compliance.

DOE has 120 days to publish implementing rules and 180 days to recommend changes to federal procurement rules to prioritize U.S.-manufactured energy infrastructure. DOE may also publish a list of pre-qualified equipment and vendors exempt from the new restrictions.

Why It Matters

- Utilities using foreign-sourced transformers, generators, protective relays, or industrial control systems, especially those from adversarial nations, should begin reviewing equipment inventories now, ahead of DOE's implementing rules.
- This order extends beyond new purchases. Existing installed equipment may be subject to removal or replacement requirements, so a full asset inventory is the practical first step.
- Suppliers of bulk-power system equipment should closely monitor DOE's pre-qualified vendor list. Being on it, or not, is likely to become a significant competitive factor.
- This is the most direct federal action yet linking supply chain cybersecurity to actual procurement and equipment restrictions rather than to voluntary guidance.

Recommended Actions

- ✓ Inventory bulk-power system equipment of foreign origin, particularly transformers, generators, ICS/PLCs, and associated software or remote access tools.
- ✓ Identify any equipment associated with vendors that may be classified as a Covered Foreign Entity.
- ✓ Watch for DOE's implementing rules, due within 120 days (by late December 2026), and for the pre-qualified vendor list once published.
- ✓ Engage suppliers now on the country of origin and ownership structure for bulk-power system equipment already in the procurement pipeline.

Legislative & Policy Watch CONTINUED

Congress Advances Mandatory Water Sector Cybersecurity Requirements

In direct response to the water sector attacks, Senators Amy Klobuchar and Adam Schiff introduced the Water Cyber Shield Act of 2026, which would, for the first time, establish mandatory cybersecurity requirements for drinking water and wastewater treatment systems and introduce new cyber incident reporting obligations.

The Senate Environment and Public Works Committee advanced the Water Resources Development Act of 2026 with bipartisan support. The bill includes provisions to strengthen water-sector cybersecurity funding and training. Separately, Senator Mark Warner introduced the Combat Emerging Threats to Critical Infrastructure Act of 2026, which would require CISA to update cybersecurity plans across all 16 critical infrastructure sectors to address AI-enabled threats.

These efforts come as final implementing regulations for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) are expected in September 2026. The regulations will require covered entities, including water and wastewater systems, to report substantial cyber incidents to CISA within 72 hours and ransomware payments within 24 hours.

Why It Matters

- Utilities across sectors, not just water utilities, should expect this momentum toward mandatory cybersecurity requirements and reporting obligations to continue expanding, following the same trajectory NERC has already set for the electric sector.
- Suppliers should anticipate that utility customers will soon face binding compliance deadlines, leading to faster, more specific procurement and vendor-security requirements.
- Organizations should review their incident reporting obligations now, ahead of the final rule under CIRCIA taking effect in September.

Artificial Intelligence Watch

AI Meets OT: DOE Expands Testing of Agentic AI in Critical Infrastructure

DOE's CESER has expanded its AI security work under a new framework, AI-FORTS (Artificial Intelligence for Operationally Resilient Technologies and Systems), organized around pillars that include securing infrastructure against AI-enabled attacks and securing infrastructure with AI-enhanced defenses. Stormbreaker, the LLM and agentic AI testbed CESER launched with Lawrence Livermore National Laboratory in July, is a core part of that work, evaluating how AI models behave under realistic, adversarial OT conditions.

This work has taken on new urgency. On August 19, 2026, NSA, CISA, FBI, DOE, and EPA jointly warned that threat actors are using AI-generated exploit scripts, disguised as legitimate monitoring tools, to target Siemens S7 Series PLCs across the energy, water, chemical, and manufacturing sectors. This is the first advisory from the federal government confirming AI-generated exploitation activity against critical infrastructure OT devices.

Why It Matters

- Utilities should recognize that AI is now a factor on both sides of critical infrastructure security, accelerating attacker capabilities and the tools available to test and defend systems.
- Suppliers offering AI-enabled OT products should expect DOE and utility customers to ask whether their systems have been tested under adversarial conditions, not only standard benchmarks.
- Organizations using Siemens S7 PLCs or similar internet-exposed OT devices should treat CISA Advisory AA26-231A as an immediate action item, not as background reading.

KALEN™ Perspective

What This Means for Utilities and Suppliers

For months, this brief has tracked warnings about cybersecurity risks to critical infrastructure. This month, several of those warnings became reality.

The threat is no longer theoretical. It's operational, and Washington's response has shifted from guidance to a mandate.

Coordinated attacks disrupted water utilities across a dozen states and took a UK power plant offline. Federal agencies confirmed that attackers are using AI to generate exploit code targeting exposed industrial controllers. DOE responded by expanding its AI testing infrastructure to evaluate how AI performs, and fails, in OT environments. NERC closed its first public comment period on cloud security standards. Congress introduced multiple bills that would make cybersecurity mandatory across sectors that have long relied on voluntary guidance. The President declared a national emergency that, for the first time, gives the federal government direct authority to restrict or remove foreign-sourced equipment already installed in the bulk-power system.

Taken together, these developments raise sharper questions than they did just a month ago:

- Can this organization prove, not just claim, that its OT devices aren't exposed as this month's victims were?
- Does this organization know, with confidence, the country of origin and ownership for every piece of bulk-power system equipment it operates?
- Is AI being evaluated as a new attack surface or only as a new capability?
- Will mandatory requirements arrive as a surprise or as the natural next step in a trend this brief has tracked for months?

For utilities, this means closer scrutiny of internet-facing OT devices, vendor remote access, incident response readiness, and now the country of origin of bulk-power system equipment already in the ground. That work needs to start now, not next year.

For suppliers, it means utility customers will start asking tougher, more specific questions about how AI-enabled products have been tested under adversarial conditions, whether OT devices ship with secure defaults rather than insecure ones, and where equipment and components actually come from.

KALEN™ was built for exactly this shift. It helps utilities identify suppliers with independently validated cybersecurity credentials and helps suppliers demonstrate maturity through recognized certification frameworks rather than self-attestation alone.

KALEN™ Takeaways

For Utilities

- ✓ Immediately identify and remove internet-exposed PLCs and OT devices; review CISA advisories AA26-097A and AA26-231A for specific mitigations.
- ✓ Inventory bulk-power system equipment of foreign origin under Executive Order 14420, and monitor DOE's implementing rules and pre-qualified vendor list.
- ✓ Confirm manual-operation fallback capability in case automated systems are compromised.
- ✓ Track NERC Project 2023-09 as it moves toward ballot, and monitor emerging mandatory requirements under the Water Cyber Shield Act, WRDA 2026, and CIRCIA.
- ✓ Ask AI-enabled OT suppliers whether their products have been tested under adversarial, realistic conditions.

For Suppliers

- ✓ Review product exposure to the PLC-targeting techniques described in CISA AA26-231A, particularly default configurations and remote access.
- ✓ Confirm and document the country of origin and ownership structure of bulk-power system equipment ahead of DOE's pre-qualified vendor list under Executive Order 14420.
- ✓ Prepare for utility customers to ask about AI-specific testing and validation, not only traditional certifications.
- ✓ Anticipate mandatory cybersecurity and reporting requirements will expand beyond the electric sector into water and other critical infrastructure sectors.
- ✓ Consider pursuing independent certification pathways to demonstrate cybersecurity maturity ahead of upcoming compliance deadlines.

Bottom Line

TThis month proved that the risks this brief has been tracking are not hypothetical. Attacks are occurring, Washington is responding with mandatory requirements and a national emergency declaration backed by real enforcement teeth, and AI is reshaping both sides of the fight. Utilities and suppliers who can demonstrate tested, validated cybersecurity practices, not merely claim them, will be the ones ready for what comes next.

KALEN

VALIDATING TRUST ACROSS THE GRID

POWERED BY GRID FRAMEWORK

ABOUT KALEN™

KALEN™ helps utilities and suppliers validate trust across the grid through recognized cybersecurity certifications, industry collaboration, and the GRID Framework.

By connecting utilities with suppliers that have demonstrated cybersecurity maturity through recognized validation mechanisms, KALEN™ supports more informed risk-management decisions and strengthens the resilience of critical infrastructure ecosystems.

FOR MORE INFORMATION

Visit **utc.org/KALEN** or contact Cordell Briggs.

VALIDATING TRUST ACROSS THE GRID. INFORMING WHAT COMES NEXT.

Utilities Technology Council™