EINPRESSWIRE

InfraShield at NEI: Navigating Nuclear Cyber Complexity Requires Regulatory Precision and Secure-by-Design Innovation

InfraShield to address evolving NRC compliance requirements while showcasing next-gen portable media security tool at NEI Cyber Security Implementation Workshop

CHARLOTTE, NC, UNITED STATES, March 19, 2026 /EINPresswire.com/ -- InfraShield, a global operational technology (OT) cybersecurity leader that specializes in protecting nuclear power facilities, will present new guidance at the Nuclear Energy Institute (NEI) Cyber Security Implementation Workshop in Charlotte, North Carolina, beginning March 23. The company will address how nuclear operators and advanced reactor developers can navigate increasingly complex regulatory requirements while implementing secure, resilient, and operationally viable cybersecurity architectures.

As the nuclear industry undergoes a historic transformation, driven by advanced reactor deployment, digital modernization, AI innovation, and evolving threat landscapes, cybersecurity regulations are becoming more expansive, nuanced, and difficult to operationalize. InfraShield's Director of Nuclear Security and Compliance Mario Fernandez, who previously served as the Cybersecurity Branch Chief at the NRC, will lead a featured session titled "Bridging the Gap: From Regulation to Implementation," focused on helping industry leaders translate regulatory intent into executable security programs.

"Today's regulatory environment is not just changing. It's expanding in ways that offer greater flexibility and the potential for operational agility, but also introduce new layers of complexity," Fernandez said. "Frameworks like 10 CFR Part 73 for current operators and Part 53 for advanced reactors and evolving guidance such as NEI 08-09 and NRC Regulatory Guide 5.71 are moving the industry in the right direction, but the residual complexity creates a steep learning curve for operators," said Fernandez.

> “Today’s regulatory environment is not just changing. It’s expanding in ways that offer greater flexibility and the potential for operational agility, but also introduce new layers of complexity.”
>
> *Mario Fernandez*

“Many are still working to translate these performance-based expectations into their plant cybersecurity programs, so that they can function more cost-effectively within live operational environments, without compromising safety. That’s where having a trusted cyber compliance partner becomes critical,” he added.

Recent regulatory developments are introducing new operational challenges across the nuclear fleet and next-generation designs. As part of their presence at NEI, InfraShield’s experts will provide unique insights to support industry leaders as they navigate these challenges, which include:

- The shift toward risk-informed, performance-based regulatory frameworks, particularly for SMRs and microreactors, which introduces flexibility for companies in how they reduce licensing hurdles and incentivizing cost-efficient, next-generation technologies
- Emerging technologies adopted without clear security models, which increases regulatory compliance complexity
- AI shifting the threat landscape faster than guidance evolves, creating gaps in cybersecurity program

With the adoption of novel digital technologies and a rapidly evolving threat environment widening the gap between regulatory expectations and operational reality, InfraShield’s experts will emphasize that closing this gap requires more than compliance; it requires a shift toward secure-by-design cybersecurity architectures, particularly for SMRs and advanced reactor concepts. Rather than retrofitting legacy controls, secure-by-design approaches integrate cybersecurity into system architecture from the outset.

“When cybersecurity is treated as an afterthought, it becomes a constraint,” Fernandez added. “When it is engineered into the design, it becomes an enabler of safe, reliable, and scalable nuclear operations.”

As part of its presence at the NEI workshop, InfraShield will also showcase its next-generation Portable Electronic Equipment Protection System (PEEPS®). This is a purpose-built solution designed to address one of the industry’s most persistent and high-risk compliance challenges: securing portable media and mobile devices used in nuclear environments.

“PEEPS allows our clients to enforce strict control over their data transfer, prevent unauthorized device introduction, and eliminate risks associated with the ‘air-gap myth’ in maintenance and testing activities by optimizing automation and mitigating the risk of human error. We are excited to share this technology with our NEI colleagues,” Fernandez said.

Attendees are invited to visit InfraShield at Booth #3 to learn more about PEEPS® and how InfraShield helps nuclear organizations translate complex regulatory requirements into practical, defensible, and future-ready cybersecurity solutions.

ABOUT INFRASHIELD

InfraShield protects the vital sectors that make society function, specializing in cybersecurity for critical infrastructure across operational technology (OT) and information technology (IT) environments. The company is a recognized leader in nuclear cybersecurity, designing and implementing solutions, architectures, and strategies that defend high-value assets against evolving cyber threats across nuclear power, advanced reactors, energy, transportation, water, and government sectors.

Rob Legare
Blue Highway Advisory
+1 703-957-8428
email us here
