RELI Group

White Paper

Transforming Cybersecurity: Enabling Tribal, Territorial and State Governments with the Empowering RELI Approach

Written by:
Will Smith, CGEIT, CISM, CDPSE, Sec+ CE
Julie G. Tu

Published November 27, 2023

Transforming Cybersecurity: Enabling Tribal, Territorial, and State Governments with the Empowering RELI Approach

State, local, tribal, and territorial (SLTT) communities consistently battle crises, some of which are deep-rooted inequities that the COVID-19 pandemic accentuated. This backdrop paints a landscape with fragile economic conditions and an ever-increasing dependency on digital platforms. As these entities become more digitally interconnected, they expose themselves to many cybersecurity threats, demanding a robust defense strategy.

The Infrastructure Investment and Jobs Act and the State and Local Cybersecurity Improvement Act, both monumental in shaping cyber resilience, brought to light the pressing concerns of SLTT communities. They are facing an increasing number of cyber threats that are evolving quickly. These threats are made worse by the limited resources to combat them. Two grant programs, the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program, have been established with a budget of $1 billion over four years. However, there are still challenges with outreach and implementation.

Key Challenges Identified

1. Pervasive and growing cyber threats.
2. The need for more resources and expertise in the SLTT communities.
3. Inefficient outreach and communication channels.

RELI addresses unique cybersecurity concerns by developing tailored solutions with federal agencies. Within these collaborations, we design a roadmap and model to scale to our customer's mission, as illustrated below:

Enterprise Risk Management and Cybersecurity Change Control: RELI advocates for large federal agencies, providing technical and operational support in vulnerability management and configuration security changes. With a focus on automation, RELI is leading the future of cybersecurity compliance by implementing automation tools like ServiceNow for governance, risk, and compliance (GRC) tracking and awareness.

Secure Systems Engineering Life Cycle by Design: RELI ensures that security is a core principle in its methodical system design approach. Reviewing system architecture designs and establishing protocols for data management are just a few facets of this exhaustive process.

Security Control Assessments and Vulnerability Management: RELI's continuous engagement with federal entities allows for ongoing assessment, ensuring that cybersecurity measures remain updated and effective. We provide technical supervision and support for vulnerability management and Continuous Diagnostics and Monitoring (CDM) tools and assist CDM efforts by managing applications. We connect the current state with our GRC view to provide the best picture of our customer's environment, allowing each team a risk-aware action model.

In today's digital age, the threat of cyber-attacks is constant. That's where RELI comes in, providing robust and reliable protection. With a successful track record, advanced solutions, and unwavering dedication, RELI is the top choice to assist SLTT communities with their cybersecurity efforts. RELI understands the pressing need for cybersecurity in SLTT communities. By drawing on our extensive experience, commitment to innovation, and proven solutions, RELI goes beyond just being a service provider - they become a partner in achieving national cyber resilience. As cyber threats evolve, RELI will adapt its strategies to ensure that digital infrastructure remains secure, efficient, and resilient for years.