

Developing Secure Information Sharing in Defence Networks

By [Kristian McCann](#) (Technology Magazine)
May 08, 2025

SMX executive explains how with design, integration and zero trust, they're able to keep mission critical information sharing in defence networks secure

As digital ecosystems expand and intertwine at an unprecedented rate, the task of securing networks has become increasingly Herculean. Yet one company has emerged as a trusted partner of governments and military clients for its ability to provide the utmost security.

Next-generation cloud, C5ISR, and advanced engineering and IT solutions provider SMX develops innovative solutions for complex multi-national defence networks. As a technology integrator and service provider, SMX specialises in designing, implementing and managing secure information sharing environments for government and military clients. With a focus on Mission Partner Environments (MPEs) and zero trust architectures, SMX is revolutionising how nations collaborate in the digital space.

The company's expertise spans across project management, systems integration and cutting-edge cybersecurity implementations. SMX's work is particularly crucial in the Indo-Pacific region, where they support the US Indo-Pacific Command (INDOPACOM) in establishing robust, secure communication networks among partner nations.

Revolutionising partner environments

At the heart of SMX's innovations is its work on the Indo-Pacific Mission Network (IMN). This initiative represents a significant leap forward in secure, multi-national information sharing.

"Through IMN, we are actively designing, testing, fielding and validating a zero trust, data-centric security enabled Mission Partner Environment, which has as its core purpose sharing information amongst partner nations," explains Dana Dewey, Mission Solutions Group President at SMX.

The complexity of these environments is staggering, involving intricate webs of technology and governance requirements.

Dewey explains that it is a combination of factors at play that make building such military and governmental clients so complex.



SMX: Developing Secure Information Sharing in Defence

"Mission Partner Environments are some of the most complex environments in terms of both technology and data governance, where there are a lot of requirements for information sharing driven not only by governance and technology but also by partner relationships," he says.

However, SMX's unique position as an integrator allows it to navigate these complexities effectively. It sources solutions, builds and executes assessment methodologies and validates the viability of IMN as a partner information sharing solution.

Zero trust architecture as an integrator

One of the key innovations SMX is spearheading is the implementation of zero trust architecture in MPEs. This paradigm shift, however, presents unique challenges.

"IMN is crucial to protecting the US and the information from our partner networks," says Dewey.

SMX's approach therefore involves a risk-informed assessment methodology driven by real-world threats and traditional sources of vulnerability information.

This methodology is tailored across various governance requirements, including the traditional Risk Management Framework (RMF) and rapidly developing standards associated with zero trust and data-centric security.

Securing a future for multi-cloud strategies

Looking to the future, SMX is heavily invested in multi-cloud strategies. It is working directly with clients to design roadmaps for building and deploying multi-cloud solutions.

"We are unique in that we have strong partnerships across multiple cloud providers and are using our on-ground perspective driven by a mission-centric strategy to leverage those partnerships," explains Dewey.

This focus on cloud integration aligns with the broader industry trend towards flexible, scalable solutions, with Dewey highlighting the flexibility potential key to expanding its services.

"Cloud is a wonderful opportunity to take advantage of both SaaS and its flexibility to deliver agile services based on the dynamic mission requirements, which often change at a rapid pace," he says.

SMX will therefore work to implement agile methodologies to rapidly evolve with increasing demands and complexities. It is also expanding its reputation as mission-oriented solutioning experts, working closely with government partners to adapt quickly to changing geopolitical climates.

All these applications, plus understanding of the dynamic new needs of its security-critical clients, mean that SMX is not just keeping pace with the cybersecurity needs of complex Mission Partner Environments – it's setting the pace.

By focusing on zero trust architectures, multi-cloud strategies, and agile methodologies, SMX is ensuring that future information sharing in multi-national defence networks remains secure.

To read the full U.S. Indo-Pacific Command Digital Report, click [HERE](#).