Wednesday, June 3

10:50 am – 11:10 am

Zero Trust at the Tactical Edge: Enforcing Policy in Contested and Disconnected Battlespace

David Herbst

Director of Solutions - Federal

Mattermost

Abstract:

Joint and coalition forces are increasingly forced to fight through denied, degraded, intermittent, and limited (DDIL) environments where traditional, centralized trust models cannot keep pace with peer adversaries. Zero Trust principles offer a path forward, but only if identity, access control, and policy enforcement can operate at the edge—across classified and unclassified networks—without assuming reliable cloud reachback or pristine transport. In this context, the question is not whether to adopt Zero Trust, but how to implement it in a way that survives jamming, disruption, and isolation while still protecting critical data and mission systems.

This session will explore how industry can support DISA and the broader DoD in advancing distributed identity, edge-based policy enforcement, and continuous authentication in contested environments. From a Mattermost perspective, the discussion will focus on what it takes to push decision-making and enforcement closer to the tactical user, synchronize policy across echelons and domains, and maintain resilient C2 and Joint All-Domain Operations even when links are unstable or partially severed. The objective is to outline practical design and governance principles that help commanders and cyber defenders treat Zero Trust not as a centralized service, but as a distributed warfighting capability that can endure in the realities of modern conflict.