Senator Joni Ernst, Chair
Senator Elissa Slotkin, Ranking Member
U.S. Senate Committee on Armed Services
Subcommittee on Emerging Threats and Capabilities

Statement by:

Michael Stokes, Vice President of Strategy, Ridgeline International
Tuesday, Oct. 7, 2025 | 2:30 p.m.

Introduction:

Chair Ernst, Ranking Member Slotkin, and Members of the Subcommittee, thank you for the opportunity to testify.

My name is Michael Stokes, Vice President of Strategy at Ridgeline International. We have followed this problem closely since 2016. In our work across government and industry, we use the term Ubiquitous Technical Surveillance (UTS) to describe this threat.

I will offer two things today: a concise definition of the problem and a path forward.

The Definition. UTS is not a single sensor you can switch off. It is a fused fabric of phones and apps, connected cars, building cameras, electronic payments, cell and Wi-Fi metadata – plus a vast commercial data market. That fusion exposes patterns, and deviations from those patterns are triggers for an adversary. An unusual no-phone day. Synchronized travel by people who should be unconnected. A route, flight, or driving pattern that does not match the desired cohort. These anomalies trigger an automated investigation, followed by human scrutiny. Near-peer adversaries – and sophisticated non-state actors, such as cartels – already leverage UTS to anticipate, frustrate, and compromise U.S. missions worldwide.

The Path Out. Admiring the problem is one thing; this hearing is bringing the right attention to the problem. But awareness without doctrine, policy, standards, and resourcing will not move the needle. At Ridgeline, we enable Digital Signature Warfare – a proactive approach to managing digital signatures so behavior and emissions align with a cohesive cover narrative before, during, and after operations. The aim is simple: protect the operational act, avoid investigative triggers, and mitigate forensic reconstruction.

Here are **Four** recommendations to make that real.

One. Name a single accountable lead for UTS and publish an enterprise baseline for signature management.

Today, UTS is everyone's problem and no one's priority, so dollars for digital force protection fall below the line. An ad-hoc approach to this issue is not sufficient. Task a single office in OSD with owning the problem. They should issue a Digital Signature Management plan for any device that connects to the public internet. This includes a serious conversation about personal devices. This policy should consider commercial data, covering device posture, routing diversity, cohort fit, and normalized absence.

Two. Protect our people by shrinking the commercial attack surface.

The data-broker ecosystem still trades in sensitive datasets, including precise geolocation. Consumer opt-outs will not safeguard a sergeant's commute to base housing. Congress can direct a Department "Do-Not-Collect/Do-Not-Sell" policy for service members and dependents – enforceable on app stores and brokers with penalties – and require annual Inspector General and GAO audits of compliance.

Three. Close two infrastructure gaps: telecom and connected vehicles.

As the impact of the recent Salt Typhoon and related attacks comes into focus, the vulnerabilities of our commercial communications infrastructure are now clearer than ever. This infrastructure compromise illustrates the need for end-to-end encrypted enterprise-grade commercial messaging applications. Connected vehicles are essentially smartphones on wheels equipped with sensors and uplinks. These vehicles feed data into unregulated commercial data economies.

Support the Commerce Department’s work to restrict untrusted connected vehicles and fully implement provisions that ban Chinese connected vehicles on Military installations. Leverage enterprise-grade secure messaging applications such as Element to communicate unclassified content on phones.

Four. Units should deploy a Digital Mirror, a survey policy, and posture for UTS vulnerabilities, and then adjust routes, timing, and device use until they blend into the desired cohort. The objective is not to vanish; it is to look normal – in pattern – all the time.

Conclusion:

Effective UTS mitigation is not theoretical. Technology, training, and tradecraft already exist and are being effectively applied at the very peak of our sensitive defense and intelligence operations. It is time to adapt and scale these solutions for the broader force.

Let me close with a family-level point. This is not only for SOF or intel operators. Spouses, kids, contractors, and base workers all generate the patterns adversaries use. If a hostile actor can determine where a soldier sleeps or which gate a unit uses, we have ceded initiative. With the steps above – governance, guardrails for commercial data, and infrastructure risk reduction – we can lower trigger rates, make it harder for the enemy to reconstruct an operation, and reduce the cost of secrecy across the force. That is how we turn UTS from a persistent disadvantage into an operational edge.

Thank you for the opportunity to testify. I look forward to your questions.