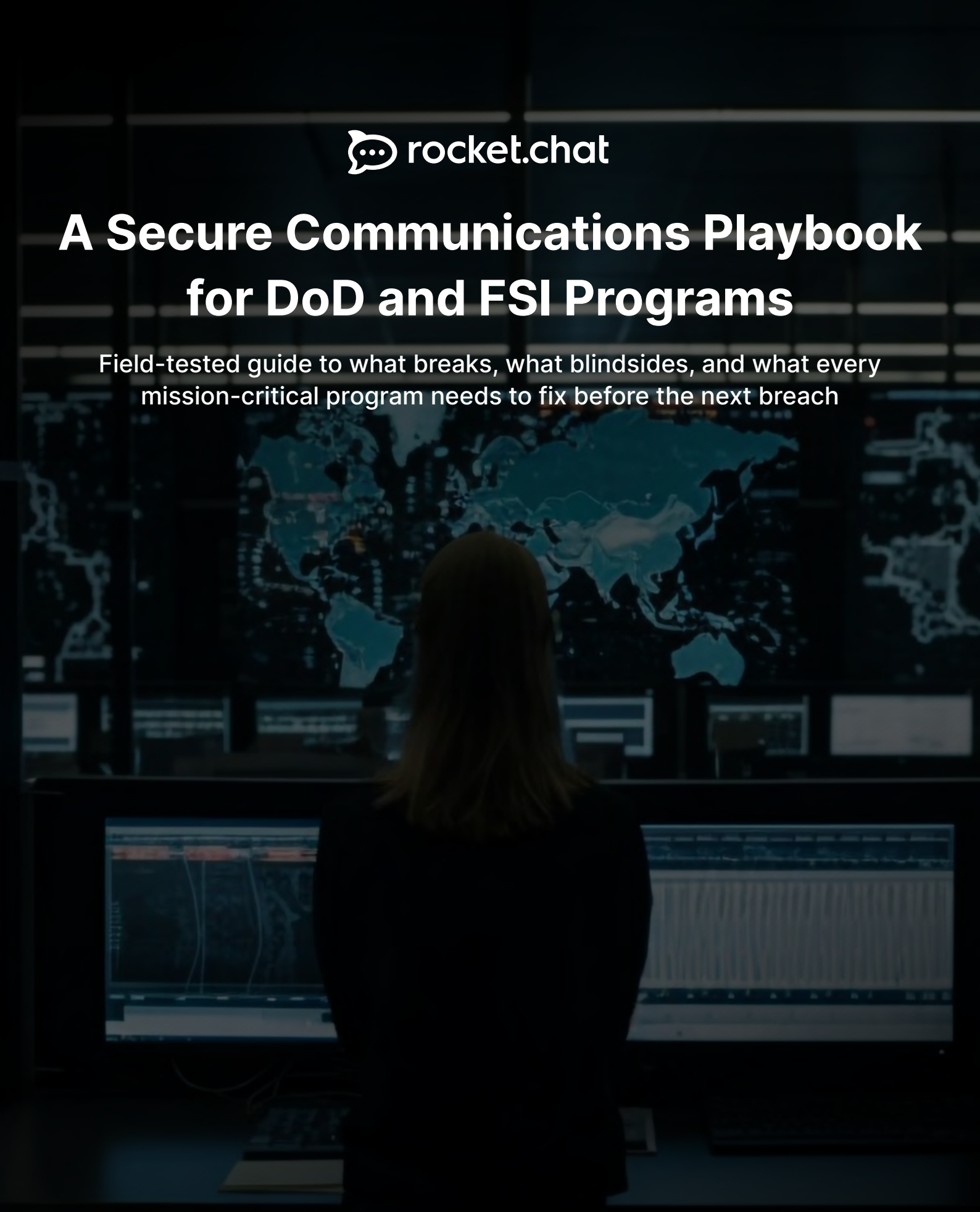
rocket.chat

A Secure Communications Playbook for DoD and FSI Programs

Field-tested guide to what breaks, what blindsides, and what every mission-critical program needs to fix before the next breach



Executive Summary

The next breach won't start with malware. It will start with a message.

It won't come through a firewall. Instead it will come through a familiar app or a platform they've used a hundred times before, in meetings, in motion, under pressure.

That's what happened at the **Treasury, at the Pentagon, and inside a Signal group chat** where the U.S. Defense Secretary unknowingly briefed an unauthenticated participant on planned airstrikes.

Read the full analysis

These weren't some sophisticated hacks. They were as predictable and preventable as it could have been.

The pattern is clear. The problem was policy blind spots, authentication gaps and the disconnect between secure infrastructure and how people actually communicate during operations.

And this pattern isn't hypothetical. It's replicating itself across defense, intelligence, and federal systems at speed.

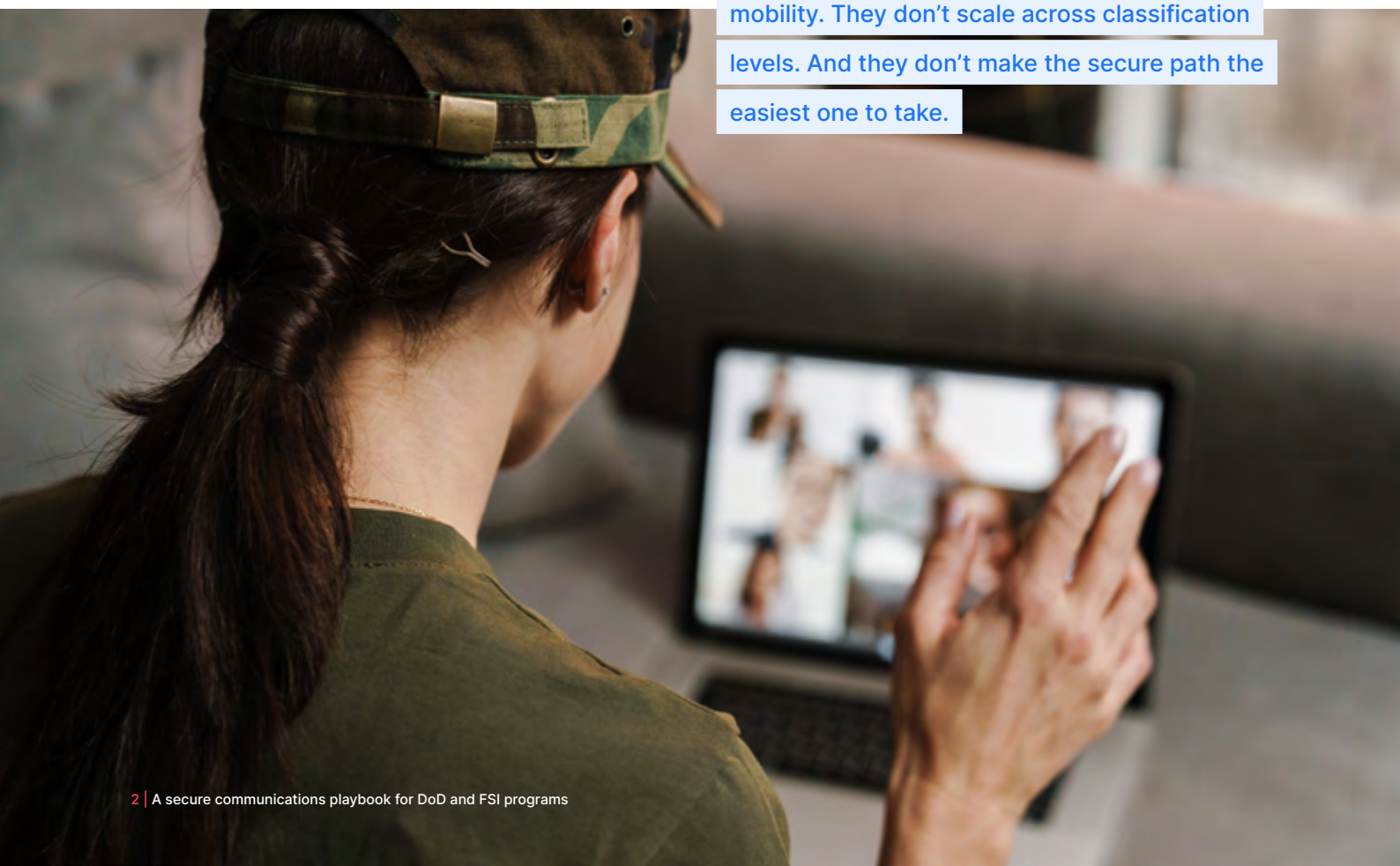
This report is a wake-up call. Based on high-profile breaches and candid insights from senior military leaders, it reveals:

- Why secure messaging is breaking down at the edge
- What FSIs and DoD programs keep missing about user behavio
- Where the next compromise is most likely to hit and how to prevent it

We close with **five tested, actionable recommendations and lessons from Special Operations and Air Force leaders** who've seen these breaches unfold.

Because in mission comms, there's no margin for error. You get one message. Make sure it goes to the right place.

The truth is: most mission communications today aren't secure. Not because they lack encryption, but because they lack resilience. They don't flex with mobility. They don't scale across classification levels. And they don't make the secure path the easiest one to take.



The defense communications threat landscape

In 2025, breaches don't break down doors anymore, they just piggyback on convenience.

From Special Operations to federal agencies, **frontline teams are defaulting to what is convenient.**

Every unsanctioned download, every shadow login, every cross-boundary share chips away at mission integrity and becomes a risk vector, unfortunately invisible until it's too late.

This is the new threat landscape:

- Consumer apps in classified environments
- Authentication failures hidden in routine coordination
- Shadow IT masquerading as speed and flexibility
- Operational gaps between secure infrastructure and reality

2025 is a tipping point.

Either secure communications become a force multiplier or they become the next source of failure.

This report exists to make sure it's the former.

Did you know?

1000+ government officials use Signal or similar consumer messaging apps for official work, despite policies against unapproved platforms.

Takeaway: If secure tools aren't usable, users will default to what is.

Source: AP news

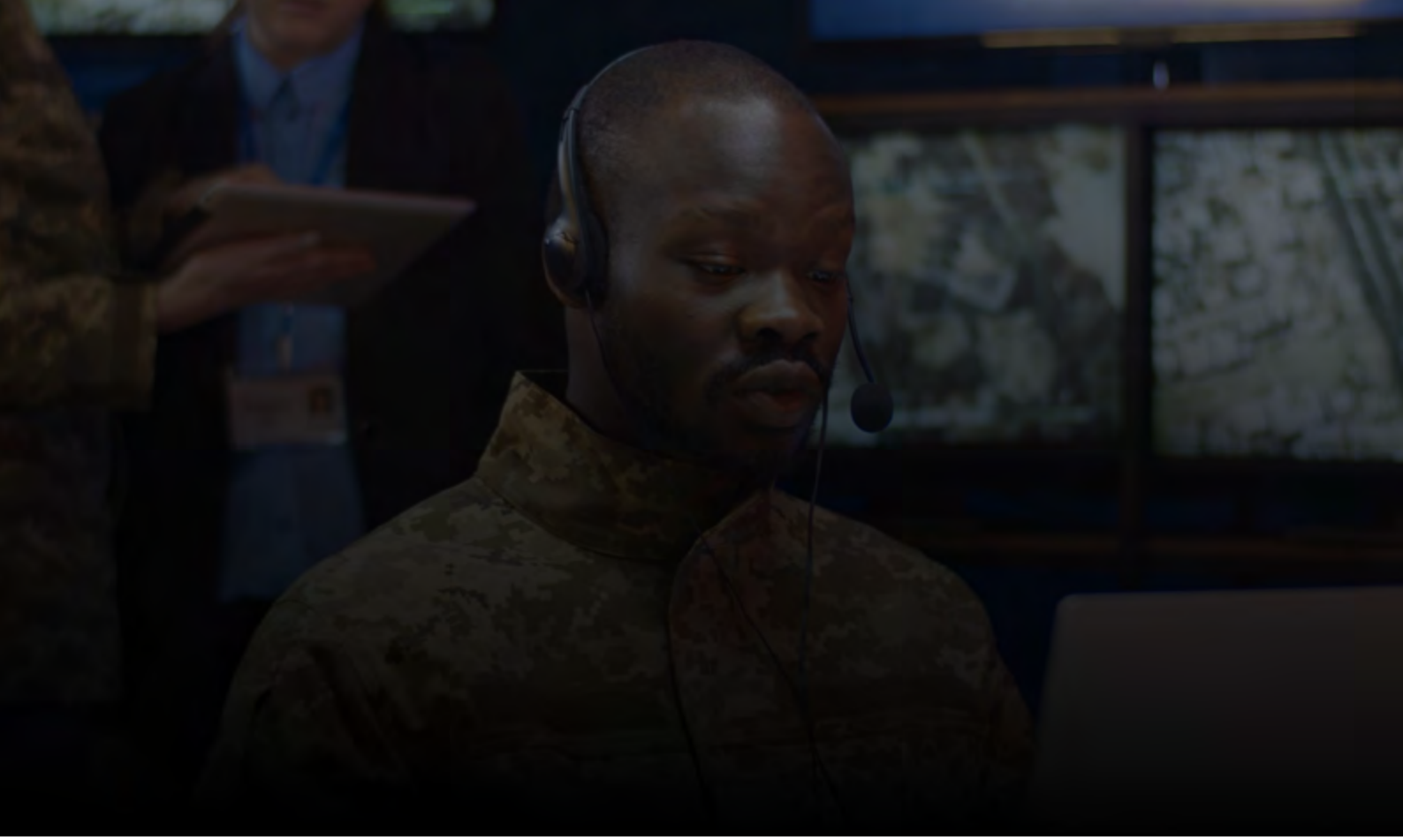
The 2025 DHS OIG report discovered identity and access weaknesses, missing ATOs, incomplete configurations, and delayed revocations across DHS systems.

Takeaway: Encryption is moot if you don't control who gets in or has access.

67% of federal employees use personal devices for work-related communications.

Takeaway: Your comms stack must secure the message, not just the device.

Source: CISA Security Report



What this means for your program

No breach starts out looking like one.

It looks like a workaround or a temporary fix.

It's mostly a team under pressure doing what it takes to get work done and stay coordinated.

That's why most compromises aren't caught in real time.

They live in the seams, between secure systems and real-world operations, between what's approved and what's actually used.

If you lead a program that handles mission communication, these patterns aren't edge cases. **You'll know that they're the norm.**

This is what's at stake inside your own stack:

If your secure tools are painful to use, people will bypass them.

If you lack visibility across chat, logs, and integrations, you'll catch the breach late.

If your vendors aren't held to the same operational rigor as your internal teams, you've already extended your risk perimeter.

If you think this won't happen in your environment, you're who it's most likely to happen to.

Don't treat your comms stack as a side concern. It's the next breach vector. That's why the smartest programs aren't asking "What tools do we have?". Instead they're asking:

How are those tools actually being used during operations?

Who's really in the loop, and who's unverified?

What are we missing because it looks like everything's working?

To put these questions to the test, we brought in national security leaders and mission insiders to challenge the assumptions and see what the audience believes about secure comms.

The patterns surfaced from the webinar polls reveal what many still get wrong, even at the highest levels.

If you've seen the following dynamics play out in your own environment, what follows will hit close to home.

FACT or FICTION

Here's your reality check.

Policy, not technology, caused the Discord, Signal, and Treasury leaks.

Verdict: **Fact**

People rarely breach on purpose.
They breach under pressure.

In fast-moving and high-stakes missions, the line between urgency and protocol gets blurry.

What this poll really probed: Are breaches the result of flawed technology, or of policies that weren't enforced when it mattered?

What came through loud and clear

"Technology can't prevent stupidity. The Signal breach? Preventable. If they'd verified phone numbers and followed procedures, it wouldn't have happened. The Airman in Discord? He knew the rules. He ignored them. That's a policy enforcement failure."
Rich Gibaldi, Ret. USAF Colonel

"In special warfare, you're trained to communicate the full story. But the narrative doesn't follow classification markings. That's where people leak proprietary data; not on purpose, but because the context demands it. And when the boundaries aren't clear, risk creeps in."
Alan Oshirak, 30-Year Navy SEAL

7 in 10 attendees

agreed that most breaches weren't technical failures, they were policy failures in plain sight.

Takeaway
Your next breach won't be a technical failure.

It'll be a policy gap no one enforced, a procedure someone skipped, or a tool someone repurposed under pressure.

- ✓ Treat comms policy as operational doctrine.
- ✓ Validate participants.
- ✓ Enforce verification.
- ✓ Audit usage.
- ✓ And make policy training as routine as platform onboarding.

You can't secure the stack if you don't control how it's used.

FACT or FICTION

Here's your reality check.

End-to-End Encryption (E2EE) alone keeps adversaries out of mission chats.

Verdict: **Fiction**

End-to-end encryption looks airtight on paper. But real-world missions aren't paper-based.

This poll posed a critical question: Can encryption alone keep adversaries out, or is it just one part of a deeper, more layered security strategy?

How our experts challenged that assumption

"End-to-end encryption protects the pipe but not what happens before or after. The tech might be solid, but situational awareness is often nonexistent. People leave screens open, forward messages without thinking, walk away mid-chat. The connection might be secure, but the behavior isn't. That's the gap we keep underestimating."
Alan Oshirak, 30-Year Navy SEAL

"End-to-end encryption is helpful, but it's not a complete answer. Chat doesn't exist in a vacuum. It's intertwined with voice, video, radio. If one link in that chain isn't secure, the whole mission's at risk. Especially when you're coordinating with partners who don't share your tools, your classification levels, or your protocols."
Rich Gibaldi, Ret. USAF Colonel

Majority of the attendees

assumed encryption alone was enough to keep adversaries out but we proved otherwise.

Takeaway
Encryption is essential, but it's just one layer.

Mission comms need security built into the full lifecycle: identity, access, audit, and intent.

Choose platforms that go beyond encryption, the ones that verify identity, enforce policy at the point of use, log activity by default, and flex across classification boundaries.

Always remember that encryption protects the message, not the behavior.

FACT or FICTION

Here's your reality check.

Mobility and SCIF-grade security are mutually exclusive.

Verdict: **Fiction**

SCIF (Sensitive Compartmented Information Facility) is a secure, access-controlled room or building used to process classified intelligence. Historically, it's been the gold standard for secure communications.

But today's mission tempo doesn't wait for a room. Coordination happens on the move across domains, partners, and platforms. Still, many assume that SCIF-level protection only exists behind concrete and lead.

This poll tested a core belief: can mobility and SCIF-grade security truly coexist?

According to the experts, here's what most people miss

"We used to think SCIF-level security meant you had to be standing inside a hardened facility. Not anymore. Air Combat Command funded mobile command centers that operate at SCI levels, even in support of Special Ops. We're now fighting on arrival and that means secure comms on the move, by design."
Rich Gibaldi, Ret. USAF Colonel

"We live in a connected world. Everyone has smart devices, real-time alerts, continuous access to news, weather, operations. You take that away, you're disconnected, and it shows.

What we need now is a pocket-sized SCIF. Something built on zero trust, able to operate at the speed of the mission. Because real-world decision-making happens in motion and often in seconds."
Alan Oshirak, 30-Year Navy SEAL

Over 50% of attendees

still assumed mobility meant sacrificing security. The speakers set the record straight.

Takeaway
Mobility isn't the enemy of security. Instead, it's the new requirement.

Your comms stack must support SCIF-level protection without anchoring teams to fixed infrastructure.

It's important for mission programs to adopt platforms that carry classification-aware protections wherever operations go: on base, in the field, or mid-air.

Look for solutions that bring zero trust, multi-domain access, and identity verification into the field because modern operations don't stand still.

FACT or FICTION

Here's your reality check.

End-user training beats technical controls in stopping the next breach.

Verdict: **Fact**

It's a question of where to place your bets. On hardened systems that enforce security by design? Or on people who must operate those systems under pressure, distraction, and risk?

This poll tested a core tension: Can technical controls alone prevent breaches or does everything fall apart without trained, ready operators?

The reality from the field

"Training isn't just learning, it's rehearsal. I've seen people who could talk through a skill but couldn't execute under pressure. Why? They hadn't trained for the environment. In special ops, we rehearse in the cold, the heat, the dark, tired, one-handed, injured because in real missions, that's exactly when you need to perform. If you haven't been tested that way, you won't hold up when it matters."
Alan Oshirak, 30-Year Navy SEAL

"As a commander in Korea, I had gear sitting inside a SCIF that nobody knew how to use because the training contract ran out. A 3-star general looked at a system and asked, 'Do we use that?' And the answer was no, and not because it didn't work, but because we hadn't trained on it. That's how readiness erodes. Technology without training is just expensive shelfware."
Rich Gibaldi, Ret. USAF Colonel

Two-thirds agreed

that training isn't just important, it's decisive and beats technical controls any day.

Takeaway
Your most advanced platform is worthless if no one knows how to use it under duress.

Training can't be an afterthought or a checkbox.

The most effective programs build it into the entire lifecycle of operational readiness.

And they pick tools that work for the average Joe, not just tech-savvy people.

Because in the field, there's no time to fumble.

Platforms must guide the mission, not get in the way.

If your team can't use it when it matters most, it isn't mission-ready.

FACT or FICTION

Here's your reality check.

Legacy systems can't be made mission-secure

Verdict: **Fact**

Legacy platforms were built for a different threat environment which was before zero trust or insider leaks. They weren't designed for modern missions that require real-time visibility, user verification, and secure collaboration across domains.

Yet too often, legacy is romanticized as "proven."

This poll tested a critical assumption: can outdated platforms still be trusted to protect today's operations?

The reality from the field

"Real readiness means integrating legacy tools with new capabilities and making sure they're secure and usable together. Bottom line: You fight with what you have. And legacy systems, if hardened and well-integrated can absolutely be mission-secure."
Rich Gibaldi, Ret. USAF Colonel

"Some of these legacy systems are tough to integrate. You can't build a wartime Twister game and expect the average Joe to operate it. The solution has to be intuitive, interoperable, and mission-proof or people will default to what's familiar, even if it's less secure."
Alan Oshirak, 30-Year Navy SEAL

63% of attendees

still believe legacy systems can be secured for today's missions but that doesn't hold true in the modern threat landscape.

Takeaway
Legacy systems might be tested, but they weren't built for today's threat surface.

If a system lacks identity-aware access, real-time logging, and zero trust enforcement, it's mission-risk.

And that makes it harder to monitor, harder to secure, and easier to exploit.

Shift to future-proof solutions that are designed to evolve with your needs and accelerate modernization.

Stop retrofitting yesterday's tech for today's battlefield.

If you're not building for this, you're not building for real-world operations.

The bar for "secure" has changed.

If your stack only encrypts data in transit, you're behind. Real-world mission environments demand more, especially when comms are mission-critical.

This checklist isn't theoretical. It reflects what operationally resilient programs already expect by default and what your next ATO or red team assessment will look for.

So, ask yourself:

Identity and access Who's in the room, and should they be?	**Governance and oversight** Can you see what happened, when and why?
Role-based access that adapts per mission	Fully searchable audit trails that are tamper-resistant
Built-in identity verification (not optional, not bolted on)	Automated redaction or hashing of sensitive content
Granular permissions by user, channel, and classification levels	Enforceable data retention and deletion policies
Verified presence with real-time visibility into identity, status, and role	Real-time content moderation based on policy triggers
Mission partner controls Can your teams share intel without switching tools or leaking it?	**Flexibility and field readiness** Will this hold under pressure?
Cross-platform / cross-domain messaging that doesn't break flow	Operates in low bandwidth, disconnected, or air-gapped environments
Clearance-aware file sharing with automatic tagging	Scales from 10 to 10,000 users without re-architecting
AI capabilities gated by role and classification level	Customizable and extensible to support unique operational needs
Native interoperability with mission tools and partner platforms	Available across desktop, laptop, and mobile with an intuitive UI

The tools that earn trust are the ones that prove control, verify intent, and adapt to how operations actually run. Start holding your systems to that standard.

PS: The best programs are already building against this list.

What secure-by-design really looks like in practice.

Security isn't a setting. It's a series of choices made under pressure such as who gets access, how fast you respond, what tools you trust, and what risks you ignore until it's too late.

These aren't best practices. They're non-negotiables.

The difference between "we were prepared" and "we didn't think it would happen to us."

1 Policy beats tools. But only if it's enforced.

"Technology alone isn't the be-all and end-all. It's a value-added tool, not the first or last line of defense."
Rich Gibaldi

No tool can compensate for what policy fails to enforce. If users aren't verified, if access isn't logged, and if rules rely on memory, you're already exposed.

Strong policy isn't just about rules, it's about real enforcement.

Build systems that verify who's in the room, track every action, and make oversight automatic. **Because when policy depends on people remembering what to do, it won't hold under pressure.**

2 Treat usability as a security requirement.

"We've made secure comms so painful that people default to what's easy. That should scare us."
Alan Oshirak

If your secure channel is hard to use, your team won't use it. They'll pivot to phones, side chats, or commercial apps. That's not defiance, it's operational pressure to get things done.

Pick tools that work in motion, support the tempo of the mission, and don't need an instruction manual. **Secure systems should make the secure path the easiest one.**

3 Build for the full communication lifecycle.

"Chat doesn't exist in a vacuum. It's always intertwined with voice, video, and radio."
Rich Gibaldi

Mission communication doesn't start and stop with chat. It flows across voice, video, file sharing, and radio, often in the same operation.

Encryption protects messages in transit, but it can't control what happens after.

That's why your comms stack needs to cover the full lifecycle: verify identity, enforce access, log every action, and stay consistent across modes. **If even one channel is left unmanaged, that's where the breach gets in.**

4 Train like you fight. Then test like it's live.

"Training isn't just learning, it's rehearsal. You need to do it tired, one-handed, injured."
Alan Oshirak

You don't rise to the occasion. You fall to the level of your training. Real readiness means your team knows how to use the comms stack under pressure, in the cold, under jamming, with limited support. Not just in theory, but in practice.

Build training into the lifecycle and avoid treating it as a one-off exercise.

And if a tool can't be mastered by an average Joe under duress, it doesn't belong in your mission kit.

5 Stop retrofitting what wasn't built for today.

"Legacy systems might be tested, but they weren't built for today's threat surface."
Rich Gibaldi

You can't outpace modern threats with outdated tools. Systems without identity-aware access, audit logs, or zero trust principles don't just slow you down, they create blind spots that adversaries exploit.

If your platform can't evolve with the mission, it becomes a liability. Don't patch your way to security. **Build on systems that are secure by design and made for today's missions.**

Why secure programs start with Rocket.Chat.

The most secure programs aren't perfect. They're prepared. They know the breach won't come through the front door. It'll show up in a group chat, a forwarded file, or an unverified participant.

That's why they start with Rocket.Chat to take control of every layer and to ensure that their comms platform is as agile and resilient as their operations.

Rocket.Chat Secure CommsOS™ unifies messaging, voice, video, AI, and mission-critical applications into a single platform, ensuring full **data privacy, compliance, and operational efficiency** for defense operations, government agencies, and critical infrastructure sectors.

Whether you need to:

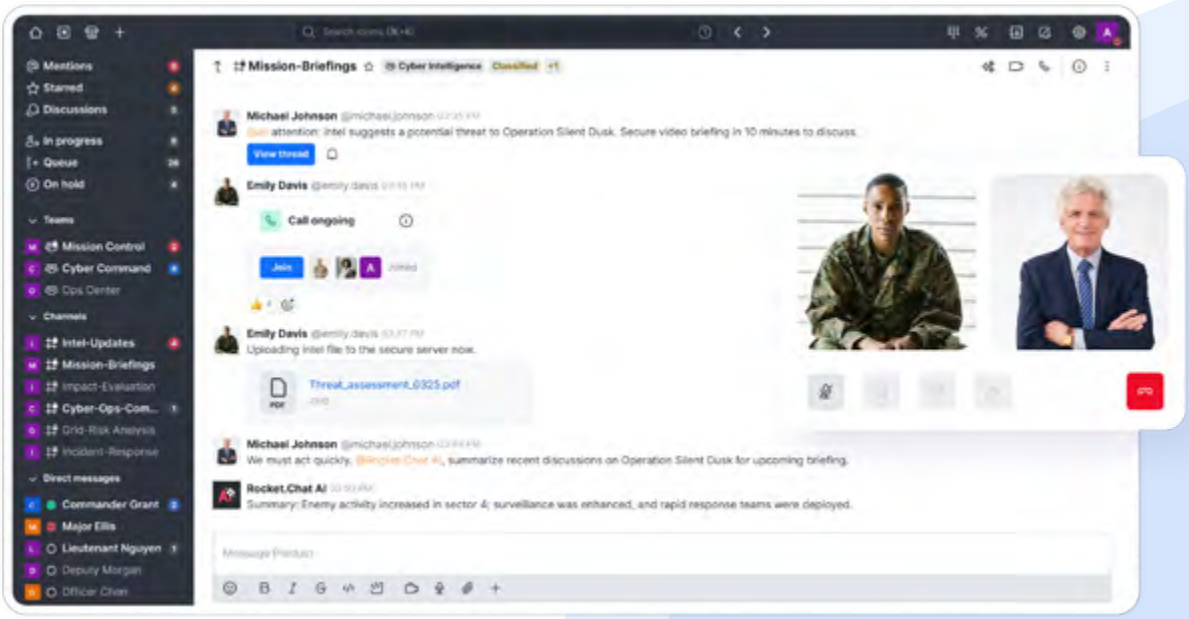
- Operate in air-gapped or low-connectivity environments
- Enforce fine-grained access and classification-based permissions
- Securely share files, logs, and media across coalition networks
- Or run full-stack audit, traceability, and lifecycle governance

Rocket.Chat gives you full operational control and real-time visibility across every message, user, and mission context.

The next compromise won't happen because you had the wrong tool. Rather, it'll happen because you made the wrong tradeoff. Don't wait to find out which one it was.

Ready to Get Started?

Request a Guided Evaluation



Learn more at rocket.chat/industry/federal-system-integrators


rocket.chat