

# How to achieve secure, mobile-first collaboration in the zero trust era

Thank you for downloading this Mattermost eBook. Carahsoft is the distributor for Mattermost solutions available via GSA 2GIT, NASA SEWP V, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Mattermost's solutions, please check out the following resources and information:



For additional resources:  
[carah.io/Mattermost-Resources](https://carah.io/Mattermost-Resources)



For upcoming events:  
[carah.io/Mattermost-Events](https://carah.io/Mattermost-Events)



For additional Mattermost solutions:  
[carah.io/Mattermost-Solutions](https://carah.io/Mattermost-Solutions)



For additional Cybersecurity solutions:  
[carah.io/Cybersecurity-Mattermost](https://carah.io/Cybersecurity-Mattermost)



To set up a meeting:  
[Mattermost@carahsoft.com](mailto:Mattermost@carahsoft.com)  
571-662-4800



To purchase, check out the contract vehicles  
available for procurement:  
[carah.io/Mattermost-Contracts](https://carah.io/Mattermost-Contracts)

# EXPERT EDITION

How to achieve secure,  
mobile-first collaboration in  
the zero trust era



## Insights from

- Air Force
- National Guard
- Navy





# Mission-Critical Collaboration for Modern Defense

Learn how Mattermost puts your mission in motion with secure collaboration built for complex environments.





# TABLE OF CONTENTS

Is secure collaboration at scale within reach? .....	4
Navy expects agentic AI will bolster authentication in a zero trust environment .....	5
How Air Force, Space Force secure 'ubiquitous communications' .....	7
BYOD helps National Guard make collaboration continuous .....	10
Evolving secure communications: Mobile and BYOD's olutions in government and military contexts .....	12

# Is secure collaboration at scale within reach?

As federal agencies continue to modernize and streamline operations, secure collaboration is a mission critical element.

We talked with technology leaders across the Air Force, Navy and National Guard Bureau about how they are reimagining the ways their teams communicate, share data and stay agile — especially in mobile environments — without compromising security.

## **First, all three leaders agree that zero trust must be the foundation.**

No surprise: Agencies are moving away from perimeter-based security toward granular, role-based access and microsegmentation.

David Voelker, zero trust lead for the Navy, recommends starting with the essentials. “Identify those things that you need to protect, implement microsegmentation right away and implement attribute-based access control,” he said.

Aaron Bishop, chief information security officer for the Air Force, added that tagging and managing data is “a key component of how you put together a zero trust infrastructure.”

## **Second, mobile collaboration is no longer optional, it’s operational.**

With most National Guard personnel lacking government-issued devices, secure bring your

own device programs have become essential. Kenneth McNeill, CIO of the National Guard Bureau, noted that “93% of the National Guard do not have government-furnished devices. This has made a tremendous impact for the National Guard mission space.”

The Air Force is similarly focused on delivering secure capabilities to endpoints, then connecting them into hardened backbones.

## **Third, artificial intelligence is emerging as a force multiplier for security.**

The Navy is exploring agentic AI to enhance authentication and threat detection. By using neural networks to analyze behavioral patterns, teams can identify adversarial activity faster and more accurately. While still evolving, these tools promise to reduce manual workload and improve response times.

Across all three themes, one constant remains: Security must be embedded into the mission, not bolted on. Can AI help push that desire, no essential requirement for mission success, forward?

Check out the articles in the pages ahead to see how technology and vision can combine to give agencies the best chance at managing risk and scaling collaboration without sacrificing trust.



*Vanessa Roberts*

Editor, Custom Content  
Federal News Network

# Navy expects agentic AI will bolster authentication in a zero trust environment

BY DAISY THORNTON

It's perhaps no surprise that two of the biggest buzzwords in cybersecurity — zero trust and artificial intelligence — are coming together.

David Voelker, zero trust lead at the Department of the Navy, said he's been pushing for an agentic threat detection framework as the next stage of the Navy's zero trust transformation. He said AI has the potential to enhance user and entity behavioral analytics for better authentication.

"The [Mitre ATT&CK framework](#) will provide recommended detections, recommended mitigations," Voelker said on [Federal Monthly Insights — Securing mobile collaboration](#). "And those detections and mitigations can be reduced into an artificial neural network to provide a probability of whether or not we've detected some adversarial threats specific to the technologies that they're implementing in their environment. Being able to optimize that data point on a probability that we can report back to a security operations center member to give them a definitive yes or no, based on a probability that we have something that we need to pay attention to."

## Aligning authentication of device and user

That's part of an effort to put more emphasis on the ability to bind the authentication of the user to the authentication of the device.

Voelker said it's difficult to determine whether the person who was issued the authentication token and is bound to the device is the actual person who is moving in a cyber environment. And it's especially

Detections and mitigations can be reduced into an artificial neural network to provide a probability of whether or not we've detected some adversarial threats.



**David Voelker**  
Zero Trust Lead, Navy

important when a user may be swapping between devices, such as starting out on a mobile device in the field and then moving to a laptop or desktop in the office.

Monitoring that user's behavior over time can create behavioral patterns, both for an individual and for a business unit, making that authentication more difficult to spoof. But an AI agent can flag deviations.

For example, is a person from finance trying to access the engineering environment or vice versa? That's something the SOC team needs to know about and investigate further.

At that point, the organization can deploy countermeasures, both automated and human initiated. On the automated side, the system may force the individual to re-authenticate. At the same time, the SOC team can contact an individual's supervisor to ask for more context. It could be something as simple as an employee working on a new project with data they never had access to before. Or it could be a bad actor attempting to move laterally within a network.

## Prioritizing microsegmentation

"As people come into the network, having that level of control of your data pathway and those things you need to protect is paramount," Voelker said on the [Federal Drive with Terry Gerton](#). "The first thing I would recommend for anyone implementing zero trust: Identify those things that you need to protect, implement microsegmentation right away and implement attribute-based access control."

When implementing attribute-based access control, he suggested that agencies start by asking themselves: What are the most critical things to protect?

The first thing I would recommend for anyone implementing zero trust: Identify those things that you need to protect, implement microsegmentation right away and implement attribute-based access control.

— Navy's David Voelker

Every agency likely has a database filled with sensitive data that it needs to protect, for instance. But a federal office building also likely has operational technology, like water, electricity and fire suppression systems controlled by IT systems. Those systems are often overlooked and therefore present an easier opportunity for an adversary to breach and move laterally, Voelker pointed out. 🛡️



***Listen to the full conversation with the [Navy's David Voelker on the potential for agentic AI to improve zero trust capabilities](#)***



# How Air Force, Space Force secure 'ubiquitous communications'

BY DAISY THORNTON

Air Force planes have to be able to communicate and share data with one another and back to their bases from environments worldwide, including degraded or denied spaces.

But that's just one of the many challenges Aaron Bishop, chief information security officer of the Department of the Air Force, faces when providing secure communications to both the Air Force and the Space Force. He also has to ensure safe and secure communications to and from satellites in space, as well as across hardened IT at more than 180 bases — essentially small cities

with housing, hospitals and other critical infrastructure.

Bishop said there's always tension between using the newest, most cutting-edge technology and the ability to use it securely, or even ensure networks are secured against threats using the newest technology.

"I do have responsibilities to the federal government on requirements on how I protect it, but I also have responsibilities for the mission commanders to deliver on capability," Bishop said on [Federal Monthly Insights — Securing mobile collaboration](#). "That friction is healthy so we can have the conversation: What is it you're trying to accomplish? What's the best way to do it?"

Bishop doesn't take a compliance-based approach to those conversations. Instead, he works with the mission commanders to give them the best possible way to accomplish the job they need to.

## Consistent communication across any channel

The Air Force is making a push toward ubiquitous communication, he said. What does that look like? Having the same protections across every medium that planes, satellites and other endpoints might use to communicate in any environment, be it

We're trying to get to, here's the capability you need at the end. Let's harden it and make it secure from that perspective — and then connect it into an already secure backbone.



**Aaron Bishop**  
Chief Information Security  
Officer, Air Force





terrestrial link, satellite link, radio frequency or any other channel for transporting data.

If a plane has to go to the other side of the planet, Bishop said, he has to ensure that data is still able to reach that plane, and it's able to transmit back as well as communicate with any potential international allies.

That need results in a larger focus on the supply chain and ensuring endpoint devices have a standard set of protections, which can then be linked via that ubiquitous connection.

"When you do that, then it's a much easier way to change technology in and out rather than trying to research and accredit the entire thing all at once. That becomes a very problematic, time-consuming and very slow process when we're trying to do the whole system end to end rather than, 'This part is trusted. This part is trusted. Bring them together to do this function that we need them to do,'" Bishop said on the [\*Federal Drive with Terry Gerton\*](#).

"From a mobile end user perspective, that's what we're trying to do. We're trying to get to, here's the capability you need at the end. Let's harden it and make it secure from that perspective — and then connect it into an already secure backbone that is providing the transport rather than trying to create an end-to-end solution."

## Defaulting to zero trust

The key to securing all the different types of data across these various communication channels is anticipating changes through zero trust principles, he said. That way in an instance of human error, whether an operator mistake or a misconfigured system, the Air Force can contain the damage and protect the rest of the system.

That's important because every new technology, solution or link in the supply chain introduces new vulnerabilities, but also new opportunities to apply zero trust

principles, Bishop said. IT personnel then know, as data travels from one part of the architecture to another, what they have, how to protect it and what that looks like under normal conditions.

Tags provide one way to let the IT team know who should have access to specific data and the systems that data is allowed on.

"The way we identify, tag and manage that data is hard, and it is a key component of how you put together a zero trust infrastructure," Bishop said.

Plus, that has to happen with a variety of new endpoints in mind, beyond laptops and desktops.

"Form factors are so ubiquitous beyond that today. Tablets, iPads, you might have a watch, you may have a small screen display in your Humvee vehicle, any of these kinds of component displays within an aircraft, or you may have it as a huge display for command and control of satellites," Bishop said.

"You may have all these different form factors that you now have to incorporate into your endpoint devices that are no longer just a Windows laptop. And all the configuration, protections and the things we want to do for that endpoint now have to apply to all these different kinds of devices before you allow it into our ecosystem. And that becomes the other end of the challenge that is pretty monumental." 🧩

You may have all these different form factors that you now have to incorporate into your endpoint devices that are no longer just a Windows laptop. And all the configuration, protections and the things we want to do for that endpoint now have to apply to all these different kinds of devices before you allow it into our ecosystem.

— Air Force's Aaron Bishop



***Listen to the full conversation with the [Air Force's Aaron Bishop on achieving secure ubiquitous communications](#)***

# BYOD helps National Guard make collaboration continuous

BY DAISY THORNTON

When it comes to technology initiatives, Kenneth McNeill leads from the front — his own phone in hand.

"I gave up my government-furnished device, now about almost five years. And I've been using bring your own device ever since," said the National Guard Bureau's chief information officer on [Federal Monthly Insights — Securing mobile collaboration](#). "I wanted to lead by example and say, 'Hey, as a CIO, I'm comfortable with this capability.' Because anything that's new, there's going to be questions about the privacy piece. And it's working: 93% of the National Guard do not have government-furnished devices. This has made a tremendous impact for the National Guard mission space."

The National Guard BYOD initiative wrapped up its pilot phase two years ago and is now a fully implemented capability. Soldiers and flight crew members are able to use their personal mobile devices for work purposes. Currently, more than 100,000 National Guard members are part of the program.

## Continuous collaboration

BYOD provides the National Guard with the capability to access collaboration tools outside of drill weekends. Soldiers and flight crew members can access Microsoft Teams and other virtual capabilities from their own

93% of the National Guard do not have government-furnished devices. This has made a tremendous impact for the National Guard mission space.



**Kenneth McNeill**  
Chief Information Officer,  
National Guard Bureau

devices, meaning they spend less time on drill weekends getting caught up. McNeill said one of the biggest improvements is that everyone can virtually sign documents now.

Previously, soldiers and flight crew members had no way to collaborate before deploying in response to hurricanes, other natural disasters and the COVID-19 pandemic.

"Now, you're on the network," McNeill said. "Now, you can plan. You can coordinate. Long before ... you show at the armory, you're ready to deploy and go support whatever mission you're supporting."

## Education and incorporating feedback

He noted the biggest hurdle has been education, ensuring everyone knows how to use the BYOD program. Besides getting fact sheets out as quickly as possible, McNeill also spends a lot of time going state to state and interacting with National Guard members in person.

Privacy and security concerns were often the most challenging hesitations to overcome, he said. Those were program priorities from day one and are built in through the cloud. He said zero trust is a major focus, and the National Guard is trying to ensure that it keeps up with future technology and cyber requirements. Education efforts require continually spreading the word and reassuring soldiers and flight crew members across the states.

Feedback has also been integral in making the program as useful as possible to the National Guard as a whole.

"I like to joke about this: Every time I visit a state, I get to hear feedback. But we communicate constantly with the states and the G6 community — and IT community — on how we can improve this," McNeill said.

Early feedback has already led to changes in the program and providing requested capabilities.

"Initially, as we were going through to pilot, the capability was you did not get alerts that

Initially, as we were going through to pilot, the capability was you did not get alerts that popped up on your phone. ... We've worked very closely with our partners as we move forward to improve the capability. We're building the airplane while in flight.

— National Guard's Kenneth McNeill

popped up on your phone. You had to log in, and you had to look at, 'Hey, do I have emails? Do I have this?' So, we've worked very closely with our partners as we move forward to improve the capability," McNeill said. "We're building the airplane while in flight." 🛩️



**Listen to the full conversation with the [National Guard's Kenneth McNeill on how BYOD helps improve collaboration and mission readiness](#)**



# Evolving secure communications: Mobile and BYOD solutions in government and military contexts

BY TERRY GERTON

The conventional wisdom of highly restricted, in-person information sharing is being challenged in an era where digital threats loom large and the need for immediate, secure communication is paramount.

Bill Anderson, principal product manager at [Mattermost](#), recently discussed the evolving landscape of secure communications, particularly within government and military contexts, emphasizing the shift towards mobile, flexible and resilient networks.

## The need for speed in secure communications

Recent global events have underscored the critical need for secure communication that can keep pace with rapidly unfolding situations. While traditional secure compartmented information facilities (SCIFs) remain essential for the most sensitive information, not all critical data falls into this category. "There are some things that are just too sensitive to be accessed outside of a SCIF. But not everything's top secret. So when you're doing your job and you're performing the mission that requires you to handle classified information, often, failure to move quickly and failure to have the maximum context is actually a benefit to our adversaries," Anderson said on [Federal Monthly Insights — Securing mobile collaboration](#).

What government needs is a system that also enables control over that government specific information when it goes down to the user on their iPhone or their Android device. It still needs to be secure.



**Bill Anderson**  
Principal Product  
Manager, Mattermost

This highlights the dilemma faced by military leaders and government executives who need to act swiftly with comprehensive information, even when physically reaching a secure location is impractical. The focus, then, shifts to enabling secure collaboration wherever the user is, ensuring data remains safe from adversaries actively seeking to intercept communications.

## Securing mobile and BYOD environments

Anderson discussed the increasing role of mobile devices, including bring your own device (BYOD) solutions, in handling sensitive but unclassified information (CUI), a significant paradigm shift. While government-issued and managed phones exist, the sheer number of personnel requiring secure mobile access makes providing a custom device for everyone economically unfeasible.

The challenge lies in extending stringent security controls to personal devices. This requires robust backend solutions that can enforce policies like biometric authentication, detect compromised devices (jailbroken or rooted), prevent screen sharing and video recording, and ensure files are never downloaded to the device itself.

“What government needs is a system that also enables control over that government specific information when it goes down to the user on their iPhone or their Android device. It still needs to be secure,” Anderson said. The goal is to connect policy with reality, putting “really, really stringent controls around that information before it goes down to the device.”

## Zero trust and granular access control

Preparation is key to enabling secure mobile operations. Organizations must deploy systems, train users, and establish workflows in advance. For BYOD scenarios, mobile device management (MDM) software can provide containerized control, allowing administrators to manage or even remotely wipe government data on personal devices.

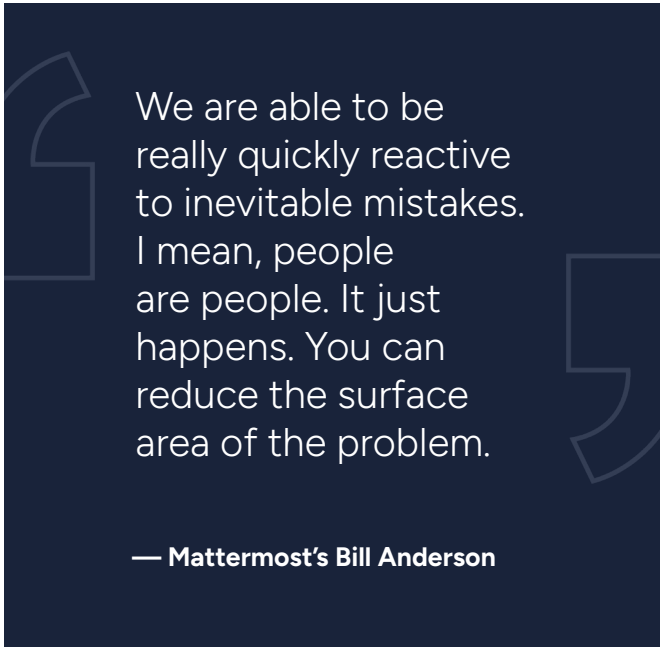
However, in situations where MDM isn't feasible, a system with extensive access control rules and boundaries around information becomes crucial. This is where

zero trust access control comes into play. This approach involves highly granular, dynamic controls that verify user identity, clearance levels, physical location (e.g., on base), and even device operating system updates before granting access to information.

The objective is to allow users to view necessary information without creating persistent artifacts on their devices that could be exploited by adversaries. This system requires careful planning and definition of policies, aligning with initiatives like the mandate by the Defense Department chief information officer to enforce zero trust on all DoD systems.

## Mitigating human error

Even with advanced technological safeguards, human error remains a factor. A common scenario involves sensitive documents being inadvertently shared in a collaboration channel. Traditionally, such incidents could lead to catastrophic and expensive remediation, sometimes requiring servers to be taken offline and every user's device to be wiped.



We are able to be really quickly reactive to inevitable mistakes. I mean, people are people. It just happens. You can reduce the surface area of the problem.

— Mattermost's Bill Anderson

Mattermost's approach addresses this by allowing immediate flagging and removal of inappropriate content from a channel, followed by a security review.

"We are able to be really quickly reactive to inevitable mistakes. I mean, people are people. It just happens. You can reduce the surface area of the problem," Anderson said.

This localized response significantly reduces the cost and time associated with incident resolution, focusing on the few individuals who may have seen the unauthorized information rather than a widespread system purge.

## International collaboration and data sovereignty

Collaborating with international partners or even different domestic agencies introduces further complexity due to varying security standards, classification rules and data sovereignty concerns.

"Especially across countries, it's an issue because they don't call these things the same thing, and so the rules are different," said Anderson.

The solution involves establishing clear policies and enforcing them through granular, zero-trust access controls applied to files, people and communication channels. For international intelligence sharing, established mechanisms exist, but enforcement across both sides is critical.

Data sovereignty — who owns and controls the data — is a key consideration, especially when information originates from different countries or when new artifacts are created collaboratively. Independent servers with federated connections allow each organization to maintain control over its data and adhere to its internal record-keeping and archiving standards.

Even private sector entities collaborating with government agencies can be integrated using similar technical approaches, often employing cross-domain filters to prevent accidental sharing of classified information with unclassified systems.

## Resilient infrastructure and future-proofing

System resilience is paramount, as network outages are inevitable during emergencies. Governments, drawing on lessons from projects like ARPANET, are adept at deploying mesh networks with redundant channels and resynchronization capabilities to ensure users can continue their work.

Looking ahead, organizations must choose software and partners that offer a modular and open architecture to avoid vendor lock-in. This foresight allows for the integration of new features and capabilities, such as sovereign self-hosted AI models, without costly and time-consuming dependency on a single vendor.

Finally, Anderson stressed the importance of "post-quantum cryptography" and future-proofing security protocols.

With quantum computers projected to break current encryption methods within 10 to 30 years, governments must start planning now to protect sensitive information for the long term. This proactive approach ensures that secure communication systems remain impenetrable against future adversarial capabilities. 🚀



**Watch and listen to the full discussion with [Mattermost's Bill Anderson on ensuring secure mobile collaboration through smart technology](#)**