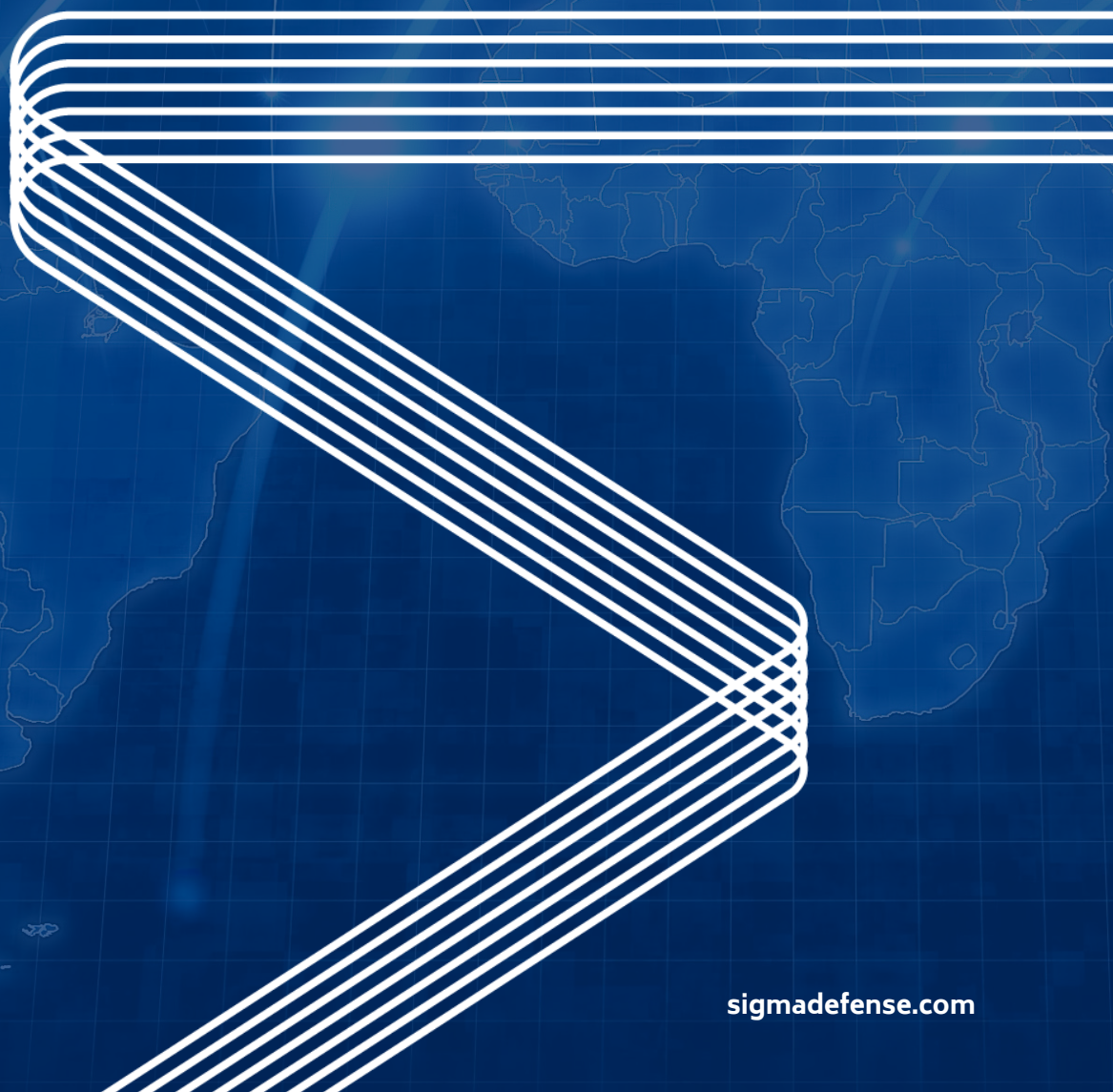
Sigma Defense

Delivering the CJADC2 Mission of "Sense, Make Sense, and Act."



sigmadefense.com

Delivering the CJADC2 Mission of "Sense, Make Sense, and Act."

Fusing Multi-INT Sensor Data at the Edge for Decision Dominance

Sigma Defense specializes in integrating Command and Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) systems and data across the Joint and Partner Force environments.

Our focus is delivering capabilities—not hardware. The success of the Combined Joint All-Domain Command and Control (CJADC2) initiative can and will be achieved by integrating new and existing hardware and software through an agile DevSecOps framework. Through software, we create seamless connections across DoD's existing systems. This allows decision makers to access and share data from throughout the U.S. military ecosystem while unlocking new capabilities across the battlespace.

This approach differs from the business model most legacy large prime integrators use. Not only does it demonstrate a nuanced understanding of CJADC2's challenges, but also our willingness to commit to a new approach for best outcomes at myriad organizations across the U.S. government.

What follows is Sigma Defense's vision for achieving CJADC2 success in both the short and long term.

What is CJADC2, and Why Does it Matter?

"[C]JADC2 will enable the DoD to act at the speed of relevance to improve U.S. national security," said Deputy Secretary of Defense Dr. Kathleen Hicks. "[C]JADC2 is delivering capabilities beginning now, and it will continue to be funded in the coming years."

CJADC2's stated goal is to enable the Joint Force to quickly "Sense, Make Sense, and Act"—as DoD terms it—on information across the battlespace. It aims to do this by using automation, Artificial Intelligence (AI), predictive analytics, and Machine Learning to deliver informed solutions via a secure, resilient, robust, reliable shared network environment. A successful CJADC2 environment will give U.S. and allied forces a superior advantage on the battlefield—a goal since the dawn of warfare.

Sigma Defense understands CJADC2's scope and its importance in maximizing the potential of all military operations. To create the "connective tissue" among land, sea, air, space and cyber assets and their data, we focus our vision on DevSecOps. This allows us to integrate information rapidly, accurately, and securely from all spheres.

But while the name "CJADC2" is relatively new, there has been a requirement for this kind of rapid interoperable, interactive communications flow for decades. Though DoD has the data and systems to create the CJADC2 end state, it has struggled to marry the two. Why hasn't this been the default modus operandi for DoD before now? What challenges must DoD overcome to fully realize the CJADC2 vision?

Barriers to Overcome for Effective CJADC2 Deployment

Acquisitional Challenges

Several challenges to CJADC2's success stem from the structure of the DoD network architecture, the burdensome acquisition process, and the lack of a true vendor-agnostic framework.

1. **Disjointed network architecture** – Companies and programs attempting to solve DoD's technical networking challenges in isolation will not meet CJADC2's needs. If an endpoint solution in one area won't "talk" with an endpoint solution in another area, the DoD cannot achieve an end-to-end mission thread.

2. **Slow and complex acquisition process** – The DoD acquisition process is well known to be very slow and price-driven – two characteristics that do not fit the rapidly changing IT environment. And DoD acquisition officers are risk-averse, which reinforces their reluctance to accept emerging technology solutions.

3. **No vendor-agnostic IT framework** – The largest DoD contractors often propose a holistic solution. These tend to be proprietary offerings that work well only if the customer invests in an entire ecosystem. Meanwhile, solutions based on policy changes, DoD-wide "Standardization," and/or synchronized acquisition are either doomed to fail or won't deliver on relevant time scales.

Yes, policies should be changed, and acquisition should be modernized. But overly prescriptive Standardization—with a capital "S"—does not have a successful track record for innovating solutions that can complete with adversarial modernization. Instead, the DoD can benefit from small-s "standardization" that sets the frameworks and the discipline of expectations while providing flexibility. This encourages CJADC2 implementation to focus more on future development while accommodating and accepting what the DoD already has in place.

Organizational Challenges

1. **Siloes** – Military organizations have had a long history of identifying, developing, and purpose-building solutions for their own specific operational requirements. As a result, the various Services and subordinate organizations in the DoD conducted R&D, procurement, and deployment of material solutions independently of each other. Typically, this meant they did not consider how other service branches could integrate and leverage capabilities of their solutions. For this reason—and because each Service's mission is unique—interoperability among services is virtually unheard of.

   This stems from DoD's understandably low tolerance for risk, given its "no-fail" mission requirements. Unfortunately, this has led to a tendency to "reinvent the wheel" when a "wheel" already exists in another service branch, or a new solution exists within the commercial sector. These duplicative efforts also tend to take longer, cost more, and lag behind novel commercial innovation.

2. **A walled-garden business model** – In today's highly contested technology environment, the DoD can't afford to wait to acquire agile or cutting-edge technologies the way it acquires complex, long-lead-time items, like aircraft.

   In the past, as the Defense-Industrial Complex grew, contractors used the DoD culture to build a business model based on providing large, expensive, closed, proprietary solutions with very long use cycles. For instance, the B-52 bomber was fielded by the U.S. Air Force in 1955—roughly 70 years ago. Boeing built fewer than 750 of them for the Air Force, and about 10% of them are still in use; the company has been providing support and upgrades throughout their entire existence.

   That mindset endures today, even as missions accelerate. With that approach, the DoD will always be late to meet mission needs.

3. **Slow accreditation and certification** – Another challenge to implementing CJADC2 has been accreditation and certification, especially in cybersecurity. Obtaining required approvals dramatically slows the delivery of new systems while the outdated systems they're intended to replace are riddled with security vulnerabilities. Although it's permissible to share developmental/testing toolkits, they are typically bespoke and therefore unshared. And while accreditation reciprocity is an authorized action that could reduce fielding timelines, few ever use it, as they do not know the process to request it, or they do not have cross-service approval.

Technical Challenges

The organizational challenges are steep, but they're not uncommon for large entities navigating change. Similarly, the technical challenges facing CJADC2 are also fairly rigid—but not insurmountable (with one caveat). Generally, they fall into one of three categories:

1. **Poorly functioning software**
   - *Closed systems* – These systems were not designed to be integrated with a common platform and lack an interface to get data in or out; they need to be assessed individually to determine if/how this can be remedied.
   - *Proprietary systems* – These systems have their own interfaces. Their proprietary nature means vendors often will not share documentation on the standards they use. This makes it difficult to fuse and integrate data.
   - *Unintuitive and poorly designed Human-System Interfaces (HSI)* – These make data entry cumbersome and error-prone; data visualization is confusing and non-intuitive, if available at all. These can be addressed with better-designed UI, automation, and AI/ML.
   - *Lack of cybersecurity engineering resources* – Solutions must fit the requirements of a Zero Trust architecture, but this requires making scarce engineering resources more available. This is important, because as more networks and systems become connected, an increasingly connected environment expands the threat surface. This potentially enables adversaries to gain entry, compromise a system, and then migrate from one system to another.
   - *Long capability delivery cycles* – This has been the norm whenever the DoD upgraded its system capabilities. The components of CJADC2 must be agile to succeed and remain relevant, so it's essential to integrate DevSecOps capabilities into the engineering framework, allowing more frequent and secure iterations.
   - *Non-networked systems* – These are less common than before, but the DoD still has many operational systems and sensors that were not built to be network-enabled for cross-organization data sharing. An important caveat: Some can be retrofitted to become network-capable—but in extreme cases, others cannot. These will need to be re-thought and redeveloped within a short timeframe.

2. Fragile networks

- *Segmented networks* – There are sensors, systems, applications, and people spread across local and global networks that either don't connect or require cross-domain solutions. This makes it virtually impossible to share data into a greater DoD "data fabric" and disseminate the right data to the right user, at the right time. The DoD can address this with the aforementioned cross-domain solutions, but this requires careful planning to minimize the number of nexus points required.

- *Challenging environments at the tactical edge* – Many networks are susceptible to both normal operation demands and actions by adversaries; CJADC2 solutions in this area must be equally robust and flexible. Development and testing must start at the tactical edge and work backwards to ensure that systems will work when disconnected from higher headquarters and networking entities.

3. Ineffective/inefficient data management

- *Too much data* –This is the blessing and curse of the information age. Challenges include identifying what data is the most important, knowing which data to use when and where, verifying that the data hasn't been compromised, and confirming that a system will even be able to use the data format or protocol. Commercially available solutions, particularly the use of AI and ML, will help declutter the abundance of data.

- *Data movement* – The movement of data is more than just whether there is a link from the sender to the intended recipients; it also encompasses attributes such as security, latency, resiliency, and throughput. Networked endpoints that are mobile and even communicate on the move (COTM) create additional constraints and limitations. While both unclassified and classified networks are an endemic challenge, operating secure networks can be significantly riskier in a highly contested cyber environment.

  Additionally, we can expect the tactical edge to be immensely challenging with a peer/near-peer adversary who will work to degrade our freedom of movement in the electro-magnetic/digital spectrum.

A Different Approach to CJADC2

Sigma Defense's philosophy for solving CJADC2 creates a unique framework that aligns with our customers' challenges and priorities.

To enact our CJADC2 vision, Sigma Defense is vendor-agnostic—encompassing an open source, open standards, and open data posture. We take an open-ecosystem approach and focus on partnerships with government and industry alike to deliver the best set of solutions for the specified requirements. Additionally, we are committed to enabling additional mission capabilities using the systems the customer already has in place, if possible. By taking advantage of what is already deployed, our approach increases the value of the fiscal investments the DoD has already made—while also increasing speed, effectiveness and efficiency to capability.

Specifically, Sigma Defense uses a comprehensive Modular Open Systems Approach (MOSA) vendor-agnostic integrated solution built on our proven and accredited (USN/USMC ATO) DevSecOps

framework. This delivers an agile solution for edge multi-INT sensor data ingestion, processing, management, AI/ML analytics, COP/CIP, and data queuing for potential semi-autonomous/autonomous effects. In this way, whether cached offline or collected online, these MOSA solutions powered by the Sigma Defense DevSecOps framework create a domain that enables the DoD to manage integrated solution sets.

We approach solutions holistically by identifying end-to-end mission threads (think Joint Warfighting Concepts) and synchronizing investments to address the key problems in all technical areas. This means making incremental progress in multiple technical domains that, together, deliver new capacity for warfighter success—enabling the DoD to move at the speed of relevance, and faster than adversarial iterations.

We can achieve this because we've identified what to do and where to do it within the CJADC2 matrix. Following this process means that individual technical advancements are evolutionary (i.e., involving continuous iterations and improvements)—but the unlocked capability is revolutionary. The underlying technologies are well proven and do not require unproven technologies to be added to the mix. This delivers real capabilities with far less risk.

Significantly, Sigma Defense's trusted and shared gateway provides the ability to run a developmental environment that allows multiple users, even partnered forces, to collaborate. These applications allow the individual user to share, distribute, and host the ecosystem. The architecture allows the end user to create a VM or container tailored to ensure everyone is connected to enriched sensor data at the edge or across all domains. Technical integration allows for C2 capabilities for a Continuous Integration/Continuous Deployment (CI/CD) pipeline and rapid dissemination information to all forces.

Critical to the flow of data is "baked-in" software for sensor data encryption that integrates accredited Cross Domain Solutions (CDS) to transmit sensitive data between boundaries, enclaves, and federated environments. This ultimately provides an unprecedented real-time information advantage by enabling Joint and Partner force data sharing, which enables information dominance over adversaries.

The Scenario: Analytics and Comms at the Tactical Edge

An operational team has been inserted into a non-permissive environment. Initially the team shares video and other sensor data via a Team Awareness Kit (TAK) application, soldier to soldier, over a Mobile Ad-hoc Network (MANET) radio. The TAK provides positioning data, mission planning and shared overlays, and real-time chat. The team places motion-detection video cameras and sensors around the target area, and the sensors distribute the videos via TAK when triggered.

One team member carries a Sigma Defense Project Olympus Edge node, an edge compute device capable of running virtual machines to host AI and ML tools, and other software for scalable effects and dynamic data dissemination capabilities. A next-gen drone is deployed to receive the video and sensor data from the team and uses locally provided AI applications to conduct object recognition to identify who or what triggered the motion detection.

The team also deploys soldier-carried UAVs to provide additional ISR for further battlefield awareness. As the UAVs gather information, they transmit it to the edge device, which analyzes and distributes the videos to the team. Operators can select from multiple reach-back options to also send the data it's collecting back to a secure commercial cloud. The data can then be disseminated to various classified networks.

While all the data makes its way back to the classified network, the team on the ground uses the Olympus Edge's compute capability for near-real time analysis, applying built-in AI to assess the overall picture—the COP. It draws from built-in algorithms, such as recognizing predefined images (trucks, people, etc.), so the operator can simply turn it on, ingest data feeds, process results instantaneously, and communicate intelligence across multiple domains.

If the algorithms, protocols, or even the mission profiles need adjustment on the fly, the edge node can be reprovisioned quickly to modify the new software set or mission software profile(s). Establishing DevSecOps in a cloud environment provides dedicated secure enclaves for plug-and-play capability, creating an environment where multiple disparate applications are connected within the DevSecOps framework.

This scenario knits together several communications methods: the AISR transmissions, mesh line-of-sight radios, cellular 4G/5G that the Sigma Defense solution can use to reach the public internet, and satellite data (pLEO, MEO, and GEO)). The team can share audio and video over the MANET mesh and tactical Wi-Fi networks.

Sigma Defense has conducted several live demonstrations of Project Olympus Edge—an expeditionary Multi-INT sensor fusion solution to the U.S. Special Operations Command, incorporating data processing, AI/ML at the edge, and cloud dissemination. In one notable instance, the compute node included an AI tool and algorithm designed to identify attendees in uniform—except no military attendees wore a uniform. The demo's on-site engineer was able to real-time reconfigure the AI baseline and program through Sigma's Olympus Hub Platform DevSecOps software, train the model in the cloud, download and deploy the new algorithm back to the device. As a result, the AI was successfully used to identify all attendees wearing baseball caps with very high-fidelity results.

Conclusion

At its core, CJADC2 is the rapid creation, collection, management, synthesis, analysis, and secure multi-path distribution of data across all domains in which the U.S. government operates—specifically across the Department of Defense and Partner forces. Sigma Defense's vision of Multi-INT sensor fusion, edge processing and compute and data distribution is coming to fruition through our family of Project Olympus solutions. This uses multiple remote sensor streams, local processing, AI and ML edge compute tools, and on-demand DevSecOps capabilities.

In short:

Sigma Defense specializes in hardware and software integration across the Joint Forces.

- We see a common DevSecOps framework and agile software development as critical to the success of CJADC2.
- We focus on delivering capabilities, not bespoke hardware; and
- We enable capabilities by enabling dissemination and access to data.

Sigma Defense is approaching CJADC2 from a different business model than the traditional large prime integrators. Our plan for CJADC2 reflects this unique business model—it's all about integration. We don't build moats; we build bridges.