01/09/2026

Reframing CDS Architecture Through Mission-Adaptable Design

Prepared by:

Nteligen, LLC

6716 Alexander Bell Drive, Suite 120

Columbia, MD 21046

info@nteligen.com

(443) 864-5042

This page is intentionally blank

Change History

Version	Name	Description	Date
1.0	Ben Rosenfeld / John Spicer	Final Draft	01/09/2026

TABLE OF CONTENTS

1.0 INTRODUCTION

Cross Domain Solutions (CDSs) exist to securely and efficiently transfer data between different security domains in support of mission objectives. Their value lies in enabling operational effectiveness while managing risk. To achieve this, CDSs must balance technical robustness against usability, providing security guarantees that support rather than constrain mission execution. As missions and technologies evolve, CDS design must adapt to increasingly dynamic, complex, and unpredictable operational environments. However, current architectural approaches, somewhat anachronistic and often rigid, struggle to keep pace. Tight coupling between system functionality and risk mitigation results in systems that are challenging to maintain, evaluate, and deploy, thereby slowing the pace of operational integration and responsiveness for missions that require data flows to change at the speed of world events.

Compounding this issue, the CDS industry's focus has drifted towards a mindset of policy compliance and validation, based on checklists, at the expense of a contextualized understanding of mission risks and agility. This adds to the lethargy of architectural advancement. While cross-domain systems are more robust and secure than ever before, the methods by which they achieve this tend towards a one-size-fits-all approach to risk management and architectural design.

Ultimately, operational decision-makers bear the heaviest burden of this trend. They not only need secure systems for data exchange but also must focus on improving outcomes by prioritizing mission-specific risk management. This necessity should, in part, drive the adaptability and innovation of cross-domain architecture.

This paper advocates shifting towards mission-adaptable CDS architectures, prioritizing flexibility, modularity, and alignment to evolving operational needs. A mission-adaptable architecture maintains high-assurance security platforms while allowing for mission-driven configuration of security posture, performance, and scalability. It provides flexibility to optimize operations across varying trust environments without compromising mission assurance. It enables operational decision-makers to select configurations that maximize operational impact without incurring the constraints of risk tolerances that they don't need to satisfy.

2.0 ARCHITECTURAL AND OPERATIONAL MISALIGNMENT

Despite their critical role in enabling secure information exchange, current CDSs face growing challenges rooted in architectural inertia and long-standing policy frameworks. Many CDS implementations are still based on premises and risk models that don't reflect the pace and complexity of modern missions. As a result, these systems are increasingly misaligned with the operational environments that they are intended to support.

CDSs are traditionally developed as tightly controlled, self-contained systems built around rigid security standards. While this model provides security assurances, it limits adaptability. The emphasis on static rule adherence has created architectures that are expensive to evolve and inherently resistant to change, even when mission requirements shift or technological capabilities advance. This rigidity has led to a widening gap between what new mission architectures demand and what CDSs can efficiently deliver. As missions become faster, more asymmetric, and increasingly reliant on real-time data, legacy CDS' risk becoming bottlenecks, impeding rather than enabling

operations. The inability to quickly integrate new data types, adopt emerging technologies, or efficiently scale to meet growing needs compromises mission agility. Moreover, the current approach to CDS development and certification delays innovation. The closed and highly integrated nature of these systems makes it difficult to assess and incorporate improvements without triggering time-consuming reevaluations. As a result, organizations can feel discouraged, even if unofficially, from experimenting with more agile or modular approaches that could offer better performance without sacrificing appropriate levels of assurance.

3.0 MISSION-ADAPTABLE ARCHITECTURE

Addressing this growing misalignment would suggest a shift in how CDSs are conceived and implemented towards one aimed at mission adaptability. Such an approach would provide responsiveness to operational needs by building flexibility into a standardized foundation that can be configured according to mission-specific requirements. Traditional CDS architecture inherently enforces maximum-security postures, ensuring the highest levels of protection. This is their default architectural posture. This, however, creates levels of rigidity that can hinder missions with different risk profiles or operational priorities. A mission-adaptable approach aligns security and performance of a given deployment with its mission context, allowing configurations that uphold core protection principles while being right-sized to operational objectives. For example, a mission prioritizing near-term adaptability over higher levels of confidentiality could tailor deployments to be less rigid, while another that prioritizes integrity may require the opposite. This shift replaces the one-size-fits-all architectural model with a responsive framework that strikes a balance between security, policy compliance, and operational agility. Central to this approach is a commitment to the philosophy of distributing risk-based architectural decisions throughout the entire CDS lifecycle, not just in the design and evaluation phases. Rather than developing to the most secure standard by default, architects should design a system to accommodate a range of risk tolerances, enabling mission leaders and authorizing officials to configure/deploy a CDS, tailoring its architectural configuration based on contextualized risk.

Mission-adaptable architectures can support multiple transfer types, protocol specifications, service types, synchronicities, and varying request-response characteristics. Similarly, they are better at rapid adaptation without the need for extensive redevelopment or recertification. Adding new data types can be done at the pace of the application lifecycle, decoupling mission timelines from lengthy system certifications that slow mission responsiveness. Finally, mission-adaptable architecture provides network topology independence, ensuring boundary interconnects can be federated and scaled to meet demand, connecting new networks without requiring architectural redesign or software expansion.

Evolutionary mission needs should not require architectural changes to an already approved CD architecture, nor should their growth. Expansion should be achieved through the scaling of computer resources, the logical configuration of endpoint services, and the configuration of routing capabilities, thereby eliminating the need for additional engineering of the core system architecture.

The need for mission-adaptable architecture implies engineering principles that decompose CDS capabilities into modular, deployable services, supporting multiple hosting strategies. Heavy-

compute activities, such as filtration and data normalization, should be offloaded to scalable environments while cross-domain interconnects are managed with highly secure controlled interfaces. Well-defined interface standards enable capability-based certification, rather than a monolithic platform-based certification, providing modular and varied deployment approaches. Multiple hosting and filtration options supported by a single architecture can work to accommodate varying risk tolerances and mission requirements simultaneously. All of which can be approached while still respecting the security concerns and objectives outlined in current architectural guidance.

4.0 BENEFITS OF MISSION-ADAPTABLE ARCHITECTURE

One key benefit of considering mission-adaptable architecture is the space it creates for exploring more innovative solutions. The current approach to architecture creates headwinds against developing new and creative architectures (or the use of emerging technologies) as they continually bump up against current 'rules'. Because cutting-edge solutions often operate outside the boundaries of established policy, they are typically excluded, not because they are insecure, but because they don't fit within an existing policy framework and require extra work to promote. A mission-adaptable mindset encourages the exploration of novel approaches because it opens the aperture of risk tolerances to be supported. Vendors can propose solutions that are tailorable to different operational contexts using existing technologies and strategies not previously considered when current policies were established.

Additionally, this shift has the potential to reduce the burden placed on policymakers. Today, policymakers function as centralized gatekeepers, reviewing and adjudicating every architectural approach against existing standards and the worst-case scenario. However, with limited bandwidth and growing complexity, this model is increasingly unsustainable. A mission-adaptable architecture can redistribute responsibility, empowering vendors to design systems that accommodate a range of mission needs and risks. They would be expected to demonstrate (through detailed, risk-informed rationales) how their architecture meets or exceeds established security expectations across that range, meeting targeted threats and robustness benchmarks. Policymakers, in turn, shift from reactive gatekeeping of architectures to strategic oversight, focusing on setting high-level priorities, benchmarks, and ensuring that mission risk is adequately understood and addressed throughout the industry. Authorizing officials would have more ability to tailor the architecture, configuration, and costs of deployment, accepting risk based on a balanced view of risk tolerance, mission imperative, and resources.

In this ecosystem, each stakeholder benefits. Policymakers are better positioned to influence the direction of CDS policy and investment, shaping the long-term strategy of meeting mission needs, rather than being bogged down in tactical review. CDS vendors gain the maneuvering space to innovate with solutions that are responsive to modern mission demands, creating architectures that encourage risk decisions throughout the entire lifecycle. Mission stakeholders, those who execute and oversee the missions, can gain a clearer understanding of their risk posture and tailor solutions that best support operational success.

5.0 CONCLUSION

While mission requirements should be the primary driver of the cross-domain development lifecycle, the CDS industry struggles with this due to the mandate for maintaining architectural alignment with policies that evolve based on tradition and the central management of ideas. In contrast, today's missions are rapidly developing their capabilities in response to accelerating global and technological changes. Demand scaling, distributed processing, IaaS/PaaS/SaaS business models, and DDIL requirements are just a few of the factors that have changed how mission organizers conceptualize, develop, and deploy their capabilities.

To effectively support the warfighter and stay ahead of emerging demands, the CDS community must adopt a forward-leaning approach that builds upon its history of security and robustness. It must provide flexibility and adaptability at the point of integration, and it must integrate with modern compute platforms more easily than it has with legacy ones. As with the missions themselves, adaptability is required for future success.

Ultimately, CDSs that fail to evolve risk becoming obstacles rather than enablers. A mission-adaptable approach enables a smarter alignment of risk, performance, and agility, ensuring that CDS architectures are not only secure but mission-effective.