

7/18/2025

Risk Perspectives of CDS

© 2025 Nteligen LLC. All rights reserved.

This page is intentionally blank

© 2025 Nteligen LLC. All rights reserved.

Change History

Version	Name	Description	Date
1.0	Ben Rosenfeld	Final Draft	7/18/2025

© 2025 Nteligen LLC. All rights reserved.

TABLE OF CONTENTS

1.0 Introduction 3
2.0 Stakeholder Perspectives 3
2.1 Government Policymakers 3
2.2 Mission Personnel 3
2.3 Authorizing Officials (AOs) 4
2.4 CDS Vendors 4
3.0 Careful Balance of Security and Efficiency 5
4.0 Nteligen's Perspective 5
5.0 Conclusion 6

Table 1: Summary of Stakeholder Perspectives 4

© 2025 Nteligen LLC. All rights reserved.

1.0 INTRODUCTION

Data transfer between network segments of differing security sensitivities is a challenge whose complexity is often underappreciated by those unfamiliar with the cross-domain problem space. To address these complexities, Cross Domain Solutions (CDS) are carefully engineered to uphold critical data-sharing principles, ensuring that both security and mission needs are met. Nteligen's perspective is that the primary purpose of a CDS is the efficient transfer of data in support of mission objectives. Within this context, however, efforts related to the design of CDS and CDS policy should be focused on maximally meeting related risk tolerances without compromising a mission's ability to execute against its imperatives.

To make truly informed design decisions and develop practical cross-domain / information sharing principles, it is essential first to understand the foundational elements of the cross-domain problem. While questions such as "What is the purpose of CDS?" and "What is its primary focus?" may seem basic, the answers are often more complex than they appear, influenced by a range of competing priorities and operational contexts. Similarly, asking "Who benefits from a CDS?" can yield very different answers depending on the audience. Perspectives vary significantly across the CDS lifecycle. Government policymakers, mission personnel, and CDS vendors all approach these questions through the lens of their unique objectives and responsibilities. These varied viewpoints highlight the need for a comprehensive and normalized approach to understanding CDS design and deployment as it applies to enabling mission while managing risk. This paper explores diverse perspectives, those of policymakers, mission personnel, and vendors, as the key stakeholders in the CDS ecosystem, in order to provide a broad understanding of the purpose of cross-domain solutions.

2.0 STAKEHOLDER PERSPECTIVES

2.1 Government Policymakers

The mission of government policymakers in the context of information sharing is to ensure that government networks and data remain secure and available, particularly when connecting networks across different security levels. To achieve this, policymakers view CDS as critical security components positioned at the boundaries between these networks. They tend to view the core function of a CDS as enforcing strict security policies, ensuring that information is allowed to cross a domain boundary only when it complies with the appropriate information sharing policies. This perspective places a strong emphasis on safeguarding classified data and maintaining the reliability of security protocols. By controlling and monitoring data flows at these boundaries, CDS plays a central role in upholding the confidentiality, integrity, and availability aspects of sharing architectures.

2.2 Mission Personnel

The primary objective of mission personnel, including operators and other mission personnel, is to ensure effective and efficient execution against mission goals. As such, supporting technology must align with that purpose. While CDSs are often instinctively associated with enhancing security, mission operators see their actual value in enabling the efficient transfer of data between domains to support mission needs. Without a mission-based need, there would be no justification for

© 2025 Nteligen LLC. All rights reserved.

sharing information across security boundaries in the first place. From this perspective, a CDS does not inherently improve the security of two isolated networks; instead, it introduces additional risk by linking them to facilitate data movement. There are more secure methods for mediating traffic between networks of different security levels, such as human-mediated data review. Although such a solution is possible, it is typically slow and labor-intensive, making it impractical for ever-increasing time-sensitive and high-volume mission needs. In the context of CDS, missions prioritize the availability of data. Thus, mission operators view the implementation of a CDS through the lens of efficient data transfer for mission enablement, not as a standalone security capability.

2.3 Authorizing Officials (AOs)

Authorizing Officials (AOs) play a critical role of balancing operational efficiency with network security. Unlike government policymakers, whose primary goal is providing guidance to ensure networks and data remain secure. AOs are responsible for the entire CDS architecture and its maintenance, including approving the use of CDSs and associated data exchanges. As such, they contextualize security policy in terms of mission need, determining a prioritization between specific mission objectives and security posture. Their deeper awareness of mission context equips them to make informed security decisions tailored to operational needs. However, as these officials bear direct responsibility for their choices, they commonly exhibit a heightened sensitivity to risk compared to mission personnel focused on mission objectives.

2.4 CDS Vendors

The goal of CDS vendors is fundamentally to develop and sell a product that meets market demand. When understanding the purpose of a CDS, vendors often find themselves navigating between the differing priorities of government policymakers and mission personnel. As the end users and primary customers, mission personnel view CDS as a tool for efficiently transferring data to support their objectives. Vendors must address these operational needs to create a successful product to satisfy their customers. However, vendors must also align closely with government policymakers and AOs, as policy alignment is essential for their CDS products to be authorized for use. Compliance with stringent government security policies is non-negotiable. No matter how well mission personnel appreciate the functionality of a CDS, without alignment to security policy, the product will struggle to get authorization for deployment into mission environments. This dual pressure shapes how vendors prioritize competing priorities in the design and position their CDS offerings.

Government Policymakers	**Mission Personnel**	**Authorizing Official**	**CDS Vendors**
Focused on keeping data and networks secure.	Focused on getting the mission done as efficiently as possible.	Focused on keeping data and networks secure within the context of mission efficiency.	Focused on building products that solve mission needs but within the directives of policy.

Table 1: Summary of Stakeholder Perspectives

© 2025 Nteligen LLC. All rights reserved.

3.0 CAREFUL BALANCE OF SECURITY AND EFFICIENCY

It is widely acknowledged that security and operational efficiency are often in tension with one another. This becomes clearer after examining the diverse, and frequently competing, viewpoints within the CDS landscape. As discussed, there is no single, universally accepted view of a CDSs primary function or who its primary beneficiary is. Recall that maximum security can be achieved by entirely isolating networks and relying on manual data transfer, but this approach is highly inefficient. At the other extreme, direct connectivity with minimal safeguards offers transfer speed and efficiency but introduces significant security risks. This represents the endpoints of the continuum in which CDSs operate. As such, a CDS is not a one-size-fits-all solution; rather, it is a system designed to strike a careful balance between operational efficiency and security and should be tailored to the specific objectives and risk tolerance of a given mission environment. It offers higher assurance than standard controlled interfaces by enforcing policy-driven data transfers across security boundaries. Because of the varied motivations of stakeholders, ranging from policymakers to mission personnel, achieving balance likely involves compromise from each perspective's ideals. When such a compromise is calibrated correctly, a CDS becomes an adaptable solution that benefits all parties, aligning technical capability with mission-specific security policy and operational requirements.

4.0 NTELIGEN'S PERSPECTIVE

Nteligen believes that the primary purpose of a CDS is the efficient transfer of data in support of mission objectives. In this context, the design of the CDS and associated security policies must be aligned with established risk tolerances while ensuring that the mission's execution capabilities remain uncompromised. As previously noted, without a mission, there is no basis for sharing information, and by extension, no need for a CDS. If data remains stationary, CDSs become irrelevant. Ultimately, CDSs and associated security policies should support and enhance mission effectiveness without needing missions to bend to rigid security requirements unnecessarily.

To be most effective, collaboration across stakeholders (to strike this balance) should prioritize managing risk over compliance with security frameworks that don't consider the risk tolerance of the mission scenario. While such frameworks generally approach security by identifying and mitigating cyber threats/vulnerabilities (a valuable and necessary activity), they struggle to balance the associated costs/impacts of such mitigations against the likelihood or impact of the threats themselves. Prioritizing a risk management perspective can provide a way to contextualize compliance models to mission needs.

For example, a risk management perspective would consider the risk of a cybersecurity vulnerability and a wide range of other potential risks that can impact mission success. Not all critical risks are cyber-related, even within a cyber-focused system like a CDS. Consider that the inability of mission personnel to efficiently and effectively carry out their mission may represent an operationally unacceptable risk, one that a CDS itself could unintentionally introduce as a byproduct of its security model. Restated, it is possible for a security architecture to inject some risk into the mission space that is greater than the risks being mitigated by that architecture.

Approaching this issue from a risk management perspective provides a dynamic trade space where the perspective of diverse stakeholders can be represented and balanced. While this idea may seem

© 2025 Nteligen LLC. All rights reserved.

straightforward when articulated, it often gets lost in the shuffle of systems and lifecycle engineering. By focusing on overall risk management, stakeholders can gain a more comprehensive understanding of both challenges and opportunities, leading to more resilient strategies and better-informed decision-making.

We note, however, that this is not a trivial thing to do, especially when done across the lifecycles of mission needs, policy guidance, and architecture/product development. Each of these, while having their own competing priorities, must come together into a comprehensive ecosystem that addresses mission objectives while minimizing risk. Focusing too narrowly on any given stakeholder's area of expertise, without considering others, can easily lead to stakeholders making decisions that inadvertently, or even intentionally, affect the others' ability to be successful.

5.0 CONCLUSION

For CDS to effectively support the efficient transfer of data for missions (their primary function) while also limiting the Government's exposure to inappropriate data loss and cyber threats, cross-domain architectures must be approached with the perspective of holistic risk management. It must consider the risk concerns of all stakeholders (including any associated compliance frameworks) and do so in a way that provides coherence and deference across the parties.

This will become increasingly important as mission architectures become more complex and technological advancements change the landscape of compute capability and operational methodologies. Without a complete risk management perspective, effectively balancing the competing needs and risk concerns of all stakeholders will become increasingly difficult.

© 2025 Nteligen LLC. All rights reserved.