Concurrent Technologies Corporation

100 CTC Drive | Johnstown, PA 15904 | 814-269-6880
Email: CDS@ctc.com | Website: www.ctc.com

Cross Domain Solutions Services

Navigating Critical Considerations for Successful CDS Implementation and Deployment

This white paper is intended to provide insights for organizations requiring a Cross Domain Solution (CDS). Sometimes known as a guard solution, a CDS is an integrated hardware and software system that facilitates secure access to and/or exchange of information between networks with differing security postures. The primary purpose of a CDS is to provide users with secure, automated methods to rapidly share information while minimizing the risk of information exposure.

Concurrent Technologies Corporation (CTC) has designed, developed, and maintained cross domain solutions for nearly two decades for government clients.

In this capacity, CTC helps clients:

- Promote a common approach to cross domain activities across the U.S. government
- Advance the state of the art for cross domain technologies by conducting research and developing guidance to improve the security and capabilities of cross domain solutions
- Develop and operate cross domain community outreach programs and forums
- Operate the Cross Domain Solutions Testing Program

CTC has also been integral to the successful implementation of the U.S. government's strategy for improving CDS security and capabilities from a design, development, assessment, implementation, and operational perspective. Our decade-long partnership with our clients and execution of their critical missions has helped to protect U.S. government classified information and all CDS solutions being sold for export.

Critical Considerations

Implementing a Cross Domain Solution can be a substantial undertaking that requires careful consideration of often competing factors, including functional needs, fielding and operations & maintenance (O&M) challenges, and information security concerns.

Based on our experience, we prioritize these key factors when designing a CDS:

1. Every CDS product and each CDS deployment is unique.
2. Flaws in CDS implementation and deployment create direct and meaningful impacts to mission objectives and security.
3. The software and system engineering for CDSs are different from other application development processes.

This white paper discusses each of these considerations to assist organizations in defining, developing, testing, and fielding Cross Domain Solutions to support mission success.

CONSIDERATION ONE: Every CDS is Unique

Unlike other integrated hardware/software solutions, CDSs provide a complicated challenge for system administrators and network architects when attempting to design a holistic approach for secure data access or transfer. Every network and client environment is different, requiring a high degree of customization when integrating a CDS that meets:

- The client's mission requirements
- The agency's or organization's strict guidelines
- Federal government protection requirements for sensitive data traversing network domains

Most CDSs contain robust configuration and administration options designed to provide flexibility to meet both organizational and government requirements. However, this poses a steep learning and implementation curve for system administrators that could result in a system that is not as secure as it should be. Due to the specialized requirements and configurations of CDSs, it is possible that without appropriate knowledge and experience implementing CDS components, your entire cybersecurity posture could be diminished. Therefore, it is strongly recommended that the solution design and development process be disciplined, comprehensive, yet flexible to account for the organization's evolving security needs. This should be accompanied by a well-defined and measurable assessment process to ensure effective testing and operational compliance, given the constant emergence of new cybersecurity threats.

CONSIDERATION TWO: Deployment Flaws May Compromise Security/Mission Objectives

Misconfigured CDSs may result in serious consequences, potentially preventing the inability to meet mission objectives. The flow of critical data may be inadvertently circumvented, incurring operational disruptions or increasing the risk of data breaches and disclosure. Improper configurations may also result in non-compliance and failure to meet security standards.

Robust security practices, regular system audits, and continuous monitoring are essential to maintaining operational integrity and protecting sensitive data. A poorly implemented solution could erode trust and credibility and could have wide-ranging effects on finances, data, reputation, and productivity. It could also create competitive disadvantages and legal/regulatory consequences. Organizations requiring a CDS should:

- Actively engage with government organizations that provide relevant guidance, lessons learned, and awareness of emerging threats
- Engage relevant subject matter experts with CDS design, implementation, and operational experience to help guide and accelerate the end-to-end process

CONSIDERATION THREE: CDS Development Differs from Traditional Application Development

A CDS securely automates information transfer between domains with different security levels, focusing on preventing data leaks and mitigating attacks. Unlike traditional software development, CDS development is highly specialized, prioritizing security, compliance, and meticulous development and testing practices. Regulatory oversight is stringent, with demanding compliance requirements from the U.S. government. And governance, maintenance, and updates require continuous scrutiny and recertification.

Software and systems engineering for developing CDSs differ from typical software and systems engineering primarily in seven major areas:

Typical Application Development vs. CDS Development		
	Typical	**CDS**
Purpose & Functionality	General software applications can range widely in purpose from business productivity and entertainment to information management, without the inherent need to operate over multiple security domains.	The main function of a CDS is to securely facilitate the access to, or automated transfer of, authorized information between networks of differing security postures, while maintaining the confidentiality, integrity, and availability of each network.
Risk Management	In typical software development, risk management involves identifying, assessing, and mitigating risks related to software performance, user data integrity, and system reliability. The focus tends to be on maintaining operational continuity and protecting against common threats.	Risk management for CDSs is much more complex due to the high stakes of potential data breaches and the severe consequences of system failures. The primary risks involve the unauthorized disclosure of sensitive information, data corruption, and the infiltration of malware from less secure to more secure domains. These risks necessitate not only rigorous preventive measures but also robust detection and rapid response strategies to mitigate potential security breaches. CDS developers must implement comprehensive risk management protocols that go far beyond typical practices, focusing heavily on security risk assessments, continuous monitoring, and the stringent enforcement of security policies to protect against elevated threats.
Development & Testing Environments	Development and testing environments are usually less complex and often simulated with a variety of tools, not requiring deployment in multiple security domains. These environments are typically connected to the Internet, allowing for rapid development and easier dependency management.	CDS development occurs in tightly controlled networks. System dependencies must be meticulously selected, scrutinized, and approved before being used. Testing environments for CDS must closely mimic the operational environments, which can include multiple networks with different secure domains. Testing is rigorous and often includes both penetration testing and attempts to breach data containment measures. The CDS must continue to be effective in hostile environments where it is constantly under attack.
Regulatory & Compliance Oversight	Regulatory requirements can vary depending on the industry and application. Some software, like those in healthcare or finance, may have high compliance demands, but these are generally less stringent in security specifics than those governing CDS.	CDSs in the U.S. must adhere to and pass assessments as prescribed in various U.S. government standards and guidance, and strategies before being authorized for deployment.

Typical Application Development vs. CDS Development (*continued*)		
	Typical	**CDS**
Security Requirements	While security is important in typical software development and systems engineering, the level of scrutiny and specific security requirements are less stringent than those for CDSs, unless the software is intended for sensitive environments. Security is focused primarily on the software application itself.	CDSs must meet rigorous security standards and are subject to formal certification and accreditation processes. They must handle data sanitization, validation, and disrupt steganography to prevent data leaks between domains while also mitigating malware threats. They must adhere to specific prescribed designs and pass rigorous security assessments before being authorized for use. CDS development involves a comprehensive and deeply layered security approach that extends far beyond typical software engineering requirements. From the ground up, security measures are implemented including secure boot, operating system hardening, runtime integrity monitoring, and detailed logging. Compliance with standards such as FIPS (Federal Information Processing Standards) ensures strong cryptographic security. CDS development adheres to industry best practices and specific compliance requirements, such as NIST SP 800-53 and other U.S. government standards, and guidance, and strategies. This intricate security framework is critical to protect against the high risks associated with operating cross domain systems.
Integration & Interoperability	Integration concerns are focused on compatibility with various operating systems and third-party application programming interfaces and services rather than crossing security domains.	The CDS must often integrate seamlessly with existing systems across different, otherwise disconnected, security domains, which requires a detailed understanding of the data formats, protocols, and systems used in these environments. The CDS is typically part of a larger ecosystem that includes integrated landing servers for pre- and post-processing of the data crossing the domains.
Maintenance & Updates	While maintaining security patches and updates is important, the process is usually more flexible and less bound by strict re-approval processes.	Updates to CDSs are highly controlled and may require some level of recertification or at least a thorough security review, as changes can affect the security posture of the networks they bridge.

These seven major differences between typical application development and CDS development reinforce the unique nature of Cross Domain Solution development and operations, highlighting why experience, discipline, auditability, and accountability are so critical to success.

Summary

The critical role of CDS in safeguarding sensitive information across varied security domains cannot be overstated. The specialized nature of CDS development, marked by stringent security requirements and rigorous testing environments, underscores the necessity for expertise in this field. As outlined in this white paper, organizations must recognize that every CDS deployment is unique, demanding solutions tailored to specific mission requirements and security standards. The complexity of integrating and maintaining a CDS, coupled with the high stakes of potential data breaches, mandates a comprehensive, methodical approach to the implementation of a CDS.

Why CTC

Concurrent Technologies Corporation (CTC) has more than 20 years of in-depth experience and subject matter expertise in the design, development, deployment, support and sustainment of secure CDSs. Coupled with our U.S. government partners, we are an industry leader in this area. Our subject matter experts can help you create robust, compliant, and optimally configured systems to support mission success. We specialize in fine-tuning solutions to meet your specific operational needs and ensure a solution that your mission requires. We provide guidance, technical support, and innovative solutions to navigate the intricate landscape of cross domain security.

CTC's dedicated team of experts combines technical prowess with proven best practices, delivering unparalleled results. We have a deep understanding of the fundamental requirements that drive CDS technologies and are active in the cross-domain community to refine both the requirements and the threat mappings. We are eager to apply our expertise to assist you in maintaining the strongest cybersecurity posture possible.

We would love to become your trusted partner in driving your mission success with cross domain solutions, so please email us at CDS@ctc.com.