AFRL

THE AIR FORCE RESEARCH LABORATORY

LEAD | DISCOVER | DEVELOP | DELIVER

Cross Domain Portfolio

AFRL

CROSS DOMAIN SOLUTIONS & INNOVATION

(315) 330-7657

SecureView

secureview@us.af.mil

Multi-Level Virtual Platform

- Supports secure, remote access to classified for teleworking
- Compatible with NSA CSfC
- Supports multiple classification levels on a single computer
- Raise The Bar (RTB) compliant
- Supports BOTH 'Thick' and 'Thin' guest VMs simultaneously
- Intuitive user interface that requires minimal training for end users
- Ensures 100% Trusted Boot and Secure Isolation in the hardware
- Supported by multiple desktop and laptop manufacturers

(315) 330-7838

X-ARBITOR

rrs.lsse.pmo@us.af.mil

X-domain Agile Rules-Based Information Transfer OrchestratoR

- Next Generation scalable, highly-configurable, bi-directional, multi-domain, multi-purpose Cross Domain Transfer Solution
- Raise The Bar (RTB) compliant
- Secure Agility: secure modular architecture enables rapid updates with plug-in content filters & network protocol adapters
- Filter Orchestration: flexible fine-grained configuration & policy enforcement simultaneously supports different mission needs
- Schema-based content filters: add new data types w/o new code
- All-in-one single-box CDS reduces footprint & maintenance

(315) 330-2003

V2CDS

rrs.ccolt@us.af.mil

Voice and Video Cross Domain Solution

- Enables cross-domain VoIP and video calls
- Integrates with existing VoIP infrastructure
- Raise-The-Bar compliant
- Uses Interactive Voice Response to provide easy to follow instruction
- Supports two-party and multi-party calls, and one-to-one video calls
- Announcement and Video Banner for Classification Level of Call
- Audio/Video Filters to eliminate high bandwidth covert channels

(315) 330-2003

CDFMV

rrs.ccolt@us.af.mil

Cross Domain Full Motion Video

- Cross Domain FMV Streaming, Low-to-High or High-to-Low
- Supports MPEG2 transport stream, H.264 video, AAC audio
- Supports High Definition (1080p) streams
- Supports Key-Length-Value (KLV) metadata
- Supports multicast and unicast data sources
- Geo-Fencing – designate blackout regions

(315) 330-2378

CDIS

afrl.rieba.cdis@us.af.mil

Cross Domain Innovation & Science

- Investigates, researches and develops novel cross domain technology
- Facilitates secure exchange of information across security and administrative domains
- Partners to achieve Governance, transition to cross-domain solutions, and technology innovation
- Transitions technologies to fill cross-domain enterprise and tactical technology gaps
- Supports AF, DoD, and IC enterprises and tactical environments

INFORMATION HANDLING BRANCH

AFRL

RIEB

THE AIR FORCE RESEARCH LABORATORY

AFRL

Cross Domain Solutions 101

How to securely share information for mission operations in Enterprise Environments

WHAT IS A CROSS-DOMAIN SOLUTION?

A Cross-Domain Solution (CDS) is a mechanism to ***access*** or ***transfer*** information between two or more networks of different security classifications.

WHY ARE CROSS DOMAIN SOLUTIONS NEEDED?

Cross Domain Solutions are needed to enable secure information sharing – getting the right information to the right people at the right time. In fact, the lack of information sharing was a key reason behind the 9/11 attacks. Information sharing, however, must be done securely in order to maintain the necessary data characteristics of Confidentiality, Integrity and Availability (CIA).

WHERE ARE CROSS DOMAIN SOLUTIONS USED?

Cross Domain Solutions are often used in large enterprise data centers where there are many different networks and security enclaves, each with a different classification and/or releasibility. A CDS may also be deployed at the tactical edge in order to meet site or mission specific needs.

HOW DO CROSS DOMAIN SOLUTIONS WORK?

A CDS must simultaneously protect the confidentiality of high-side data, protect the data integrity and protect the availability of high-side resources. In layman's terms, a CDS must prevent both data spills as well as attacks against classified networks. A CDS will use cryptography and mandatory access control (MAC) mechanisms to isolate different networks and data flows. Additionally, a Transfer CDS will use various filters to inspect data in transit to ensure compliance with security and releasability policies, as well as to reduce the risk of attack from embedded content.

HOW AFRL CAN HELP

AFRL has designed, developed and revolutionized secure information sharing and cross domain technologies for over 30 years. AFRL offers both cross domain access and transfer solutions to meet your mission needs. AFRL Cross Domain Solutions include:

SECUREVIEW A Cross Domain Access solution that supports multiple classifications on single machine using both "Thick" & "Thin" VM clients simulataneously

ISSE Guard A Cross Domain Transfer solution that enables bi-directional and uni-directional secure information flows, with extensive message filtering capabilities for both structured and unstructured data

X-ARBITOR The Next Generation Transfer solution, featuring secure yet flexible Filter Orchestration Engine and Protocol Adapter plug-in architecture.

V2CDS The Voice & Video Cross Domain Solution from the CCOLT PMO enables users to make secure cross domain one-to-one audio or video calls, as well as audio conference calls

Please contact us today to discuss your specific cross domain requirements find out how AFRL can revolutionize your mission!

(Continued on page 2)

(Continued from page 1)

WHAT TYPES OF CROSS DOMAIN SOLUTIONS ARE THERE?

There are two basic categories:

(1) Access solutions allows a user to ACCESS differently classified networks from a single machine. In the desktop Access model, users can have separate Virtual Machines, each at different classification levels and accessing separate, isolated networks. A site's Virtual Desktop Infrastructure (VDI) can also be supported.

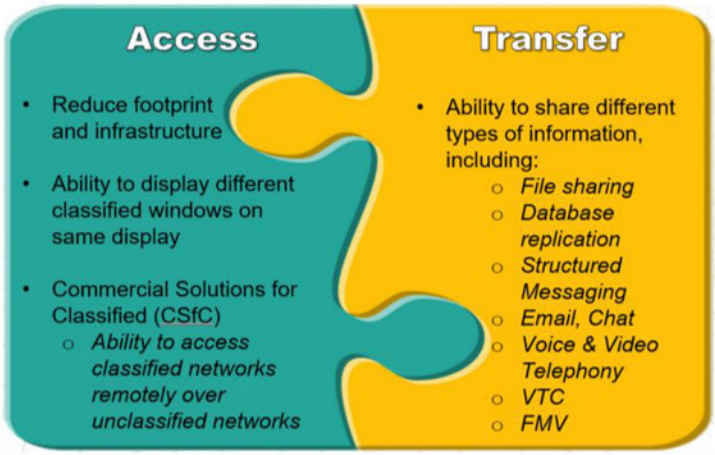
(2) Transfer solutions send or TRANSFER data between different security domains. There are several sub-categories, including Diodes (a one-way transfer) and bi-directional Guards that can support the transfer of different data types and applications between multiple (3+) domains. There is also a special case of Transfer Solution known as a Multi-Level Security CDS, which uses mandatory labeling to store data at different classifications and allows users to query and retrieve the data based upon their security domain and credentials.

WHEN TO USE AN ACCESS VS A TRANSFER CDS?

The type of CDS used depends on the mission requirements. For example, does information need to be transferred between security domains, or do users simply need to access resources within multiple/different enclaves?

Additonal criteria to consider when selecting a CDS include:

- The environment where the CDS will be hosted
- Number of networks to be supported and their classifications
- Interoperability with existing applications and infrastructure
- For an Access CDS, is there a VDI in place or planned?
- For a Transfer CDS, what data types and protocols are required?



WHAT IS THE ACQUISTION PROCESS FOR A CDS?

The acquisition process for a CDS depends on many factors, including the agency, Authorizing Official (AO), networks involved and other criteria.

For Agencies and Organizations that require Top Secret and Below Information requirements, the AO will be integral to the process, and it would be best to enage the AO and CDS provider.

For DoD Agencies that have Secret and Below Information requirements, it is best to first contact your Cross Domain Service Element (CDSE).

Generally speaking, if possible, first use an enterprise Cross Domain service or enterprise-hosted CDS. If this option is not possible then use an existing CDS solution without modification. Finally, if neither of those options are possible, modify an existing CDS solution to meet the mission requirements (e.g. define new data filters to support new data types).

SecureView PMO:
Web: https://intelshare.intelink.gov/afrl-idhs/web/sv/default.aspx
Email: afrl.rieb.secureview@us.af.mil
Phone: (315) 330-7657

ISSE and X-ARBITOR PMO
Web: https://intelshare.intelink.gov/afrl-idhs/web/isse/default.aspx
Email: rrs.isse.pmo@us.af.mil
Phone: (315) 330-7838

CCOLT PMO
Web: https://intelshare.intelink.gov/afrl-idhs/web/ccolt/default.aspx
Email: rrs.ca.pmo@us.af.mil
Phone: (315) 330-4887

AFRL

COMPLIANT RTB COMPLIANT

SecureView®

Secure, Cost Effective Access to Multiple Independent Levels of Security

WHAT IS SECUREVIEW?

SecureView® is the premier Cross-Domain Access Solution developed by the Air Force Research Laboratory (AFRL). SecureView provides users with the ability to access Multiple Independent Levels of Security (MILS) on a single workstation. When used with the Commercial Solutions for Classified (CSfC), SecureView provides secure remote access to classified networks, enabling telework from home or on the road.

HOW DOES SECUREVIEW WORK?

SecureView is a flexible solution which provides secure access through a combination of traditional and leading-edge connectivity solutions. An organization's existing network infrastructure can be merged seamlessly to deploy SecureView workstations – thereby minimizing deployment cost, complexity, and disruption. If new or additional networks are needed, SecureView can connect to them using Virtual Private Network (VPN) tunnels over the existing infrastructure, including unclassified Internet, while maintaining the required separation and protection of the classified networks. SecureView integrates seamlessly with existing Virtual Desktop Infrastructure (VDI) to enable quick and easy access to network resources. Unlike other MILS solutions that require extensive infrastructure upgrades or investment as part of their deployment, SecureView can often be deployed with minimal change to network infrastructure – drastically increasing cost savings and the speed of deployment.

THE SECUREVIEW DIFFERENCE

SecureView was built from its inception to provide unparalleled security, agilty, and performance for IC and DoD workstations while ALSO minimizing the total cost of ownership. Best of all, SecureView is government-off-the-shelf (GOTS) technology, which keeps the IC and DoD from getting locked into a proprietary or single-vendor solution that would limit their flexibility and scalability. Furthermore, lifecycle costs are kept low for ongoing support, training ans software patches or upgrades.

Capability

- Supports NIPRNet, SIPRNet, and Coalition access on a single PC or laptop
- Intuitive user interface that requires minimal training for end users
- Enables secure mobility solutions for Executive Communication and traveling personnel
- Seamlessly supports high performance and high-bandwidth applications

Security

- Type I bare-metal hypervisor enhances the cyber defense posture of government workstations
- Minimizes Type I encryptors by integrating support for NSA's Commercial Solutions for Classified (CSfC)
- Ensures 100% Trusted Boot and Secure Isolation in the hardware
- Has received highest MILS evaluation to date against NIST 800-53 Criteria

Flexibility

- Supports either Standard Desktop Configuration (SDC) or Thin Virtual Desktop Infrastructure (VDI)
- Enables rapid provisioning, management, and re-configuration of workstations
- Government off-the-shelf (GOTS) solution based on OpenXT which meets DoD's open-source requirement

Self-Encrypting Drive Support

SecureView now supports Self Encrypting Drives (SED), according to the requirements and recommendations set by the NSA Commercial Solutions for Classified program (CSfC). We targeted hardware encryption to maximize performance, partnering with Micron and Digistor to leverage their self-encrypting drives. This is a tremendous cost savings over implementing Data at Rest in each SecureView VM, while providing efficient protection for the entirety of SecureView platform.

- Hardware-implemented encryption with minimal performance impact
- Supports multiple users and roles (*users, admins, security*)
- Exportable configuration simplifies deployments
- Supports a multiple form factors (*M.2, SATA*)Supports username/password, smartcard, & Yubikey authentication

ABMS DeviceOne SecureView (ADSV)

ADSV is a remote telework capability providing users with secure access to SIPRNet from home.

Composed of 3 Core Elements

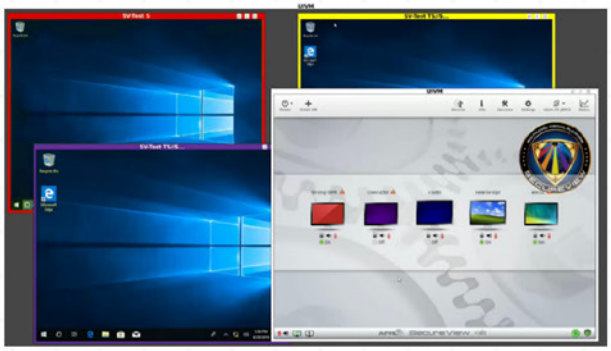
1) ***AFRL's SecureView multi-level access solution***
   Highly secure end user device, supports multiple classification levels simultaneously
2) ***NSA's Commercial Solutions for Classified (CSfC)***
   Ability to tunnel classified networks over commercial comms
3) ***Virtual Desktop Infrastructure (VDI) "backend"***
   Installed in the SIPR datacenter; provides the user desktop, apps and storage

SecureView Management

The SecureView Management Server (SVMS) enables mission sites to remotely deploy and manage virtual machines (VMs) on indivdual workstations or by groups of workstations. Additionally, configuring and/or upgrading the workstations is simple using the SVMS. New VMs can be created and seamlessly deployed to establish new Communities of Interest or to support new domains.

SecureView MOSAIC

SecureView MOSAIC provides users with a secure and seamless windows environment to view information on a single desktop for multiple security domains and network classifications. The benefit is a tremendous increase in personal proficiency without compromising security or creating any potential vulenerabilities in SecureView.



SecureView MOSAIC

Email: secureview@us.af.mil **Phone:** (315)-330-7657
Web: https://intelshare.intelink.gov/sites/afrl-idhs/web/sv
https://www.milsuite.mil/book/community/spaces/svinfoshare

AFRL

Voice & Video Cross Domain Solution

Enabling Secure, Real-Time Communications for the Warfighter

What is V2CDS?

V2CDS delivers secure, real-time Voice over Internet Protocol (VoIP) communication and conferencing with point-to-point video capability across two domains. V2CDS maintains the security assurances necessary to protect sensitive information between multiple security enclaves.

Using a VoIP phone, users can make two-party direct and multi-party conference calls, allowing users across two security networks to communicate simultaneously.

In addition, V2CDS includes video support that enables users to initiate, run and securely close point-to-point videophone calls for cross-domain communications. This solution authenticates users and maintains an acceptable security posture, while simultaneously maintaining quality point-to-point video capability.

What Benefits Does V2CDS Provide?

- One-to-one Voice Calling
- Audio Teleconferencing
- One-to-one Video Call, including High Definition (1080p)
- Room-to-Room VTC
- Integrates with Existing COTS VoIP Infrastructure and Phones
- Security Classification Banner and Announcement
- One Phone on Desk for Single and Cross Domain Calls

What Security Features Does V2CDS Have?

V2CDS is compliant with the NCDSMO Raise-The-Bar (RTB) guidelines and maintains the security assurances necessary to protect sensitive information between multiple security enclaves. Unlike other Cross Domain Solutions, V2CDS filters not only the packet headers, but also filters the audio and video media payloads. to filter not only packet headers, but also the media payload V2CDS authenticates users and enforces strict security policies, while simultaneously maintaining quality point-to-point video capability.

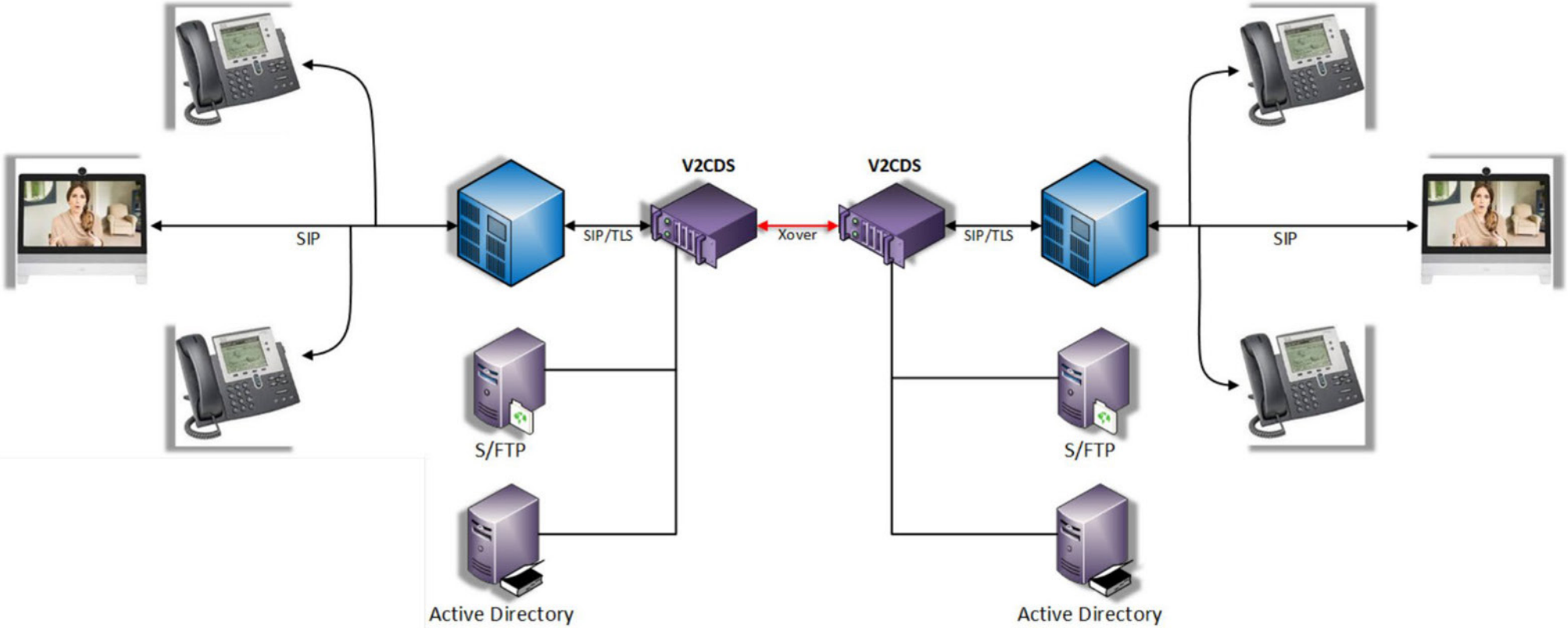
V2CDS includes:

- NCDSMO Phase 1 RTB Compliant Architecture
- Security Classification Banner
- Media Security Filters for Audio & Video to prevent covert channels

What is a Cross Domain Solution?

Government information systems are connected to a variety of networks, each controlled by different security policies. These domains are isolated from each other, typically to protect sensitive/ classified information and network resources. A CDS enables users to securely access or share information between these differently classified networks.

THE AIR FORCE RESEARCH LABORATORY

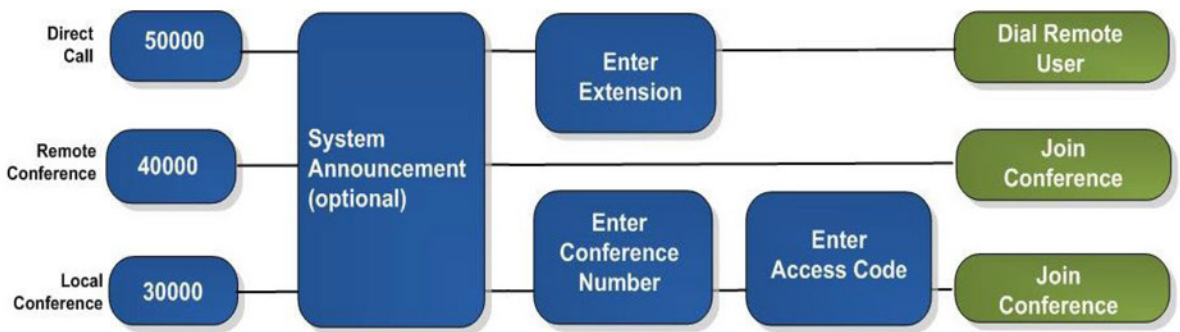


Contact Information

Email: rrs.ccolt@us.af.mil
Comm: (315) 330-2003 DSN 587-2003
Mailing Address: AFRL/RIEB, 525 Brooks Road, Rome, NY 13441

Websites

- https://intelshare.intelink.gov/sites/afrl-idhs/web/cg/index.html (NIPRNet)
- https://intelshare.intelink.sgov.gov/sites/afrl-idhs/web/cg/index.html (SIPRNet)
- https://intelshare.intelink.ic.gov/sites/afrl-rieb/web/cg/index.html (Intelink)



About CCOLT

The Cross-domain COLlaboration Technology (CCOLT) Program Management Office (PMO), hosted by the Information Handling Branch at the Air Force Research Laboratory (AFRL/RIEB), creates solutions for secure single domain and cross-domain sharing of information, to enable effective collaboration in multiple types of environments.

AFRL

Cross Domain Full Motion Video

Enabling Real-Time FMV for the Warfighter

WHAT IS CROSS DOMAIN FULL MOTION VIDEO?

Available with Voice & Video Cross Domain Solution (V2CDS) version 2.0, Cross Domain Full Motion Video (CD FMV) enables secure, real time streaming video across network security boundaries. Designed to meet stringent Army performance requirements, CD FMV supports up to 18 FMV streams at 1080p, 30 fps. (60 fps can also be supported.) Additionally, CD FMV will filter Key-Length-Value (KLV) metadata and enables redaction using geo-cameras, as well as data walls for the operations floor.

WHAT BENEFITS DOES CD FMV PROVIDE?

- Cross Domain FMV Streaming, Low-to-High or High-to-Low
- Supports MPEG2 transport stream, H.264 video, AAC audio
- Supports up to 18 HD (1080p) streams concurrently
- Supports KLV metadata
- Geo-Fencing –Designate blackout regions
- Interfaces with cameras, UAVS
- Supports both multicast and unicast data sources

WHAT SECURITY FEATURES DOES CD FMV HAVE?

CD FMV is compliant with the NCDSMO Raise-The-Bar (RTB) guidelines and maintains the security assurances necessary to protect sensitive information between multiple security enclaves. Unlike other Cross Domain Solutions, CD FMV filters not only the packet headers, but also filters the audio and video media payloads. to filter not only packet headers, but also the media payload CD FMV authenticates users and enforces strict security policies, while simultaneously maintaining quality point-to-point video capability.

CD FMV includes:

- RTB Phase 1 compliant architecture
- Security Classification Banner
- Media Security Filters for Audio & Video to prevent covert channels
- Key-Length-Value (KLV) Filtering
- Geo-Fencing redaction tool

WHAT IS A CROSS DOMAIN SOLUTION?

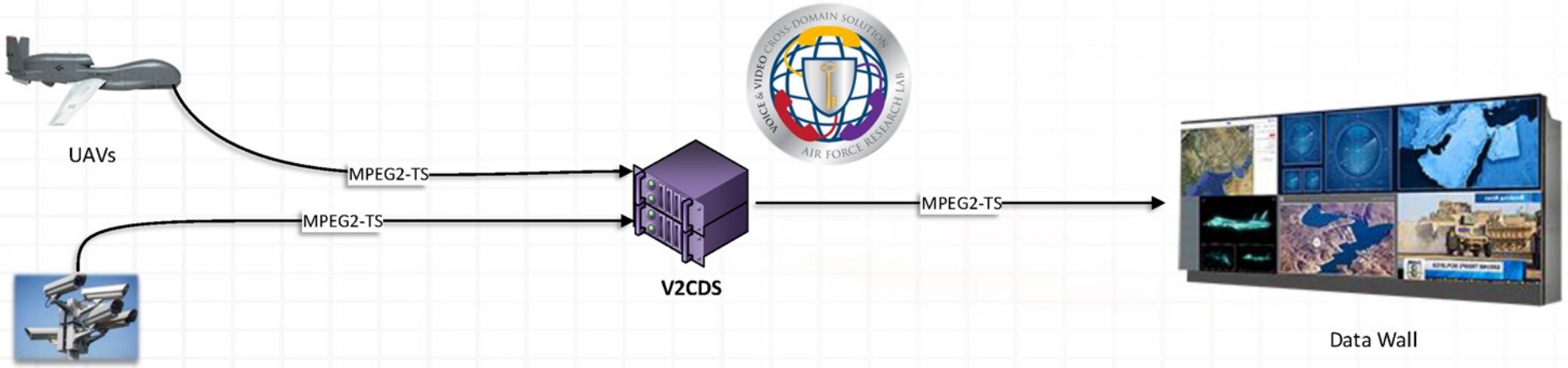
Government information systems are connected to a variety of networks, each controlled by different security policies. These domains are isolated from each other, typically to protect sensitive/ classified information and network resources. A Cross Domain Solution enables users to securely access or share information between these differently classified networks.

History

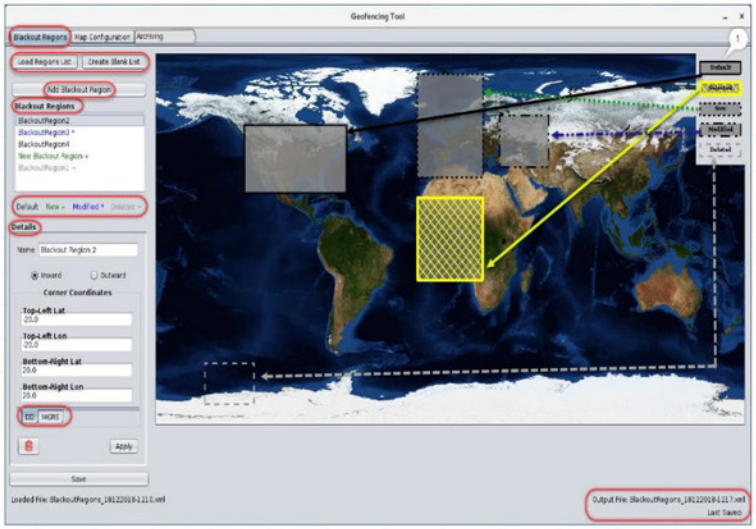
The **C**ross-domain **COL**laboration **T**echnology (CCOLT) Program Management Office (PMO), hosted by the Information Handling Branch at the Air Force Research Laboratory (AFRL/RIEB), creates solutions for secure single domain and cross-domain sharing of information, to enable effective collaboration in multiple types of environments.

RTB COMPLIANT PHASE 1

THE AIR FORCE RESEARCH LABORATORY



CD FMV



- *Multi-cast or Unicast FMV MPEG2 Transport Streams*
- *KLV Metadata Filtering*
- *Supports Decimal Degrees and MGRS coordinate system*
- *Native and off-board Geo-Fencing Tool to define blackout regions*

Contact Information

CCOLT Program Office
Email: rrs.ccolt@us.af.mil
Commercial: 315-330-2003
DSN: 587-2003

Websites
https://intelshare.intelink.gov/sites/afrl-idhs/web/ccolt/index.html
https://intelshare.intelink.sgov.gov/sites/afrl-idhs/web/ccolt
https://intelshare.intelink.ic.gov/sites/afrl-rieb/web/ccolt

Mailing Address
AFRL/RIEB
525 Brooks Road
Rome, NY 13441

AFRL

X-ARBITOR

NEXT GENERATION CROSS DOMAIN TRANSFER SOLUTION

WHAT IS IT?

X-domain Agile Rules-Based Information Transfer OrchestratoR is THE next-generation cross domain transfer solution, advancing cross domain solution (CDS) technology through a groundbreaking, innovative architecture designed from the ground-up to be Raise The Bar (RTB) compliant. Supporting simultaneous, bi-directional transfers between multiple different security domains, X-ARBITOR delivers a secure, scalable, and extensible framework engineered to enable rapid deployment of cross-domain data inspection, sanitization, and transfer capabilities, leveraging modularity and configurability not seen in traditional CDS.

SECURE AGILITY

X-ARBITOR's architecture development was guided by the principle of "Secure Agility" - the ability to quickly adapt to changing mission needs while simultaneously enforcing stringent RTB security requirements mandated for CDS.

HOW IS SECURE AGILITY IMPLEMENTED?

X-ARBITOR leverages a rigorously vetted secure framework to establish a trusted foundation, and integrates modularity and configurability to achieve built-in agility.

SECURE FRAMEWORK

- Raise-the-Bar Compliant
  - RTB's Acceptable Design Pattern (ADP) is based on X-ARBITOR's architecture
- NIAP Evaluated OS – Red Hat Enterprise Linux®
- SELinux Enforcing Mode – Granular MAC policies
- Root of Trust – Industry-standard Secure Boot
- Audit/Log Archive & Streaming
- File Integrity & Process Monitoring
- Role-Based Access Control
- Compile Time Security
- Rules-Based Security Event Management

BUILT-IN AGILITY

- Secure CDS Orchestration Engine (SCOrE)
  - Filtering policy defined per data flow
  - Supports Filter Plug-ins
  - Configurable via intuitive GUIs
- Pluggable Filters & Protocol Adapters
- Modular SELinux Policy
- Signed RPM Package Updates
- "Zero Code Change" Filter Additions (DFDL)
- Agile Development with Integrated IV&V
- 100% GUI-Driven Administration
- API Libraries for Mission Application Integration

AND, SO MUCH MORE....

X-ARBITOR PROGRAM MANAGEMENT OFFICE
Commercial Phone: (315) 330-7838, Email: rrs.isse.pmo@us.af.mil

THE AIR FORCE RESEARCH LABORATORY

Approved for Public Release, Distribution Unlimited, AFRL-2021-3867

X-ARBITOR

X-ARBITOR PROGRAM MANAGEMENT OFFICE
Commercial Phone: (315) 330-7838, Email: rrs.isse.pmo@us.af.mil

MISSION SUPPORT CAPABILITIES

As a successor to the ISSE Guard, X-ARBITOR maintains a robust GUI-driven administration capability, and provides a backwards compatible API to support existing mission applications:

- **DataSync+ and MLDBR**: Multi-Level Database Replication/Synchronization
- **SAWES**: Security and Workflow Enforcement Services
- **HEVELFT**: High Enterprise Volume / Extremely Large File Transfer
- **PrintUP**: Secure Cross Domain Print (Low-To-High)
- **Reliable Human Review (RHR)**
- **Web Services Adapter**

CORE COMPONENTS

X-ARBITOR incorporates several core components that enable *Secure Agility* including:

- **Protocol Adapter Framework** – Pluggable modules to support diverse mission communication needs
- **Filter Orchestration Engine (FOE)** – Secure Cross Domain orchestration engine to control data flows across multiple domains (up to 22)
  - Recursive Decomposition of embedded file types/objects
  - Signed Orchestration Policies
  - Filter Flow Cryptographically enforced
  - RPM-based Filter Plug-ins
- **Filters – Pluggable Filter Modules**
  - X-ARBITOR transfers a wide variety of file types, including both highly structured messages (e.g. XML) and complex file types such as Microsoft™ Office and PDF files
  - Data Format Description Language (DFDL) Filter – no code changes needed to add filters, just schema definition
- **Management** – Dedicated network interface to support SIEM
- **Administration** – 100% GUI-driven system administration