

Table of Contents

- 1 Training to Win
- 2 SimShield Benefits
- 3 SimShield Features
- 4 Architecture
- 6 Implementation
- 7 Certification and Accreditation
- 7 Conclusion

Technical Abstract

SimShield

Training to Win

Troop readiness for mission critical deployment is essential to national security, and realistic, relevant modeling, simulation, and training are key. As a modern fighting force, our troops must know what to look for and what to expect in the field. They must be able to identify dangerous situations and how to avoid them. They need first-hand expertise in the use of equipment and weaponry and must become familiar with varied battlefield conditions.

The United States armed forces have recently launched major efforts to reshape training focused on war-fighting. War-fighting exercises are an integration of live, virtual, and constructive forces. For example, a training exercise might include:

- live training that takes place in a physical environment for example, on firing ranges or onboard ships;
- virtual simulation training that uses real crews, leaders, and units working together in a virtual environment such as a simulated theater that can be accessed by war-fighters across the world; and
- constructive training that provides computer models and war type scenarios to allow training staff to execute normal war-fighting missions for the exercise environment with no constraints.

These blended training environments often require interfacing geographically separated simulations, creating a global simulation-training environment. This represents a realistic mock training exercise enabling the war-fighters to gain more relevant training experience.

Securely Training Together

Today, war-fighter simulators operate in controlled domains and cannot communicate electronically with other simulators without the risk of accidentally disclosing sensitive data. In many cases, the result is that the war-fighters are isolated from other members of the simulation community, limiting the effectiveness of the training exercise. Isolation means that war-fighters cannot participate in simulation exercises that mimic multiple sensitivity levels inherent in daily real-world operations. SimShield™, developed by Trusted Computer Solutions (TCS), meets the challenge of securely interfacing classified, geographically separated systems (live, virtual, and/or constructive) in a realistic synthetic training environment.

SimShield

SimShield is a Cross Domain Solution (CDS) or guard that allows training assets operating under different security classifications to fully communicate and interact securely. SimShield consists of two components: the Policy Editor™ and the Trusted Bridge™. The Policy Editor is an easy-to-use Graphical User Interface (GUI) that allows the creation of security classification and reclassification rules to be enforced later by the Trusted Bridge. The Trusted Bridge is the guard component that allows the connectivity of training and simulation networks operating at different security classification levels. SimShield can be used for a High Level Architecture (HLA) environment, as well as, a Test and Training Enabling Architecture (TENA) environment.

Behind the Scenes:

A Trusted Operating System

All TCS software products require a trusted operating system as a primary mechanism for security policy enforcement. SimShield utilizes a trusted operating system on both the Trusted Bridge and the Policy Editor. Trusted operating systems extend the capabilities found in standard operating systems by providing additional safeguards against internal and external threats. The employment of Discretionary Access Controls (DAC), Mandatory Access Controls (MAC), Multi-Level Security (MLS), and Type Enforcement (TE) offers powerful and customizable levels of protection for users and data. Additional security policy enforcement mechanisms are required to meet the “trusted” designation and include protection profiles that must be engineered in the operating system.

These protection profiles include Labeled Security Protection Profile (LSPP), Controlled Access Protection Profile (CAPP), and Role Based Access Control (RBAC). The unique combination of these security attributes provides for full segregation and protection of all data on the system. The technical design is based on trusted computing practices and trusted OS security enforcement at both the server and desktop layers.

The User Experience

SimShield addresses the challenges of both HLA and TENA environments.

The SimShield Trusted Bridge provides a near real-time automated secure two-way data transfer between exercises executing at different

security levels in either an HLA or a TENA environment. The CDS supports these protocols through specific engineering that enables SimShield to act as a guard for HLA or TENA compliant assets used in both DoD combat joint training and Home Land Defense training. SimShield allows training assets operating under different security classifications to fully communicate and predictably interact securely.

The Policy Editor provides an easy-to-use GUI that permits security classification and data domain experts to enter and review the rule sets that establish the reclassification policy governing the intercommunication between how data should be transferred between training enclaves operating at different sensitivity levels. Additionally, data domain experts can enter and review the reclassification rules that govern the intercommunication between single-level training enclaves. Once all reclassification rules are approved, the new policy can be installed on the Trusted Bridge in a matter of minutes. The Trusted Bridge enforces the rule set that is created by the Policy Editor.

SimShield Benefits

SimShield provides benefits for Budget Stakeholders, Administrators, Users, Security Officers, and Certification and Accreditation Officers.

For **Budget Stakeholders**, SimShield makes use of low-cost commodity hardware, allowing cost-effective support of large training

exercises. Additionally, the Trusted Bridge and the Policy Editor can be purchased together or separately depending on the network topology and the requirements for the rule set team’s physical location. Additionally, there is no need for a vendor or consultant to be a part of the rule set team. The Policy Editor is designed for the rule set team to enter and review the rule set that identifies all data elements produced by the host system that must be protected through blocking or guising.

As stated above, interconnecting multiple security level training networks in the past meant executing the entire training exercise at the High Side classification level. This required upgrades to training facilities, equipment, and personnel clearances which proved to be costly and nonproductive.

For **Administrators**, the Policy Editor allows the building and maintaining of rule sets without C++ knowledge or external consultants. Additionally the rule sets are stored in a Postgres database with role based access.

For **Users**, near real-time performance enhances their ability to train more realistically. SimShield handles any fixed-format data type, and it can be customized to any environment that requires near-real-time bi-directional content filtering, by converting to either HLA or TENA. Additionally, there is the opportunity, through TCS Technical Services, to customize a specific data type by writing code to translate the customer’s data to either HLA or TENA.

HLA Challenges

The HLA environment provides the ability to interconnect two or more simulations (HLA Federations) that operate at different security classification levels. The conventional approach to handling this multiple security level challenge is to operate the entire simulation environment at the highest security level of the participating simulations. This approach is difficult and impractical because operating at the System High level typically requires upgrades to simulation facilities, equipment, personnel clearances and other associated security mechanisms. Also, the System High approach often limits training because it limits participation.

TENA Challenges

Current day TENA compliant assets operate in controlled domains with specific security measures in place, including different Department of Defense (DoD) classifications. Communication between these assets is not possible without an approved CDS. Therefore, many cases exist where these assets cannot be utilized in their respective training communities. This isolation means that these training assets are not participating in environments that mimic multiple security levels inherent in daily real-world operations, thus negatively impacting mission requirements and objectives.

Security Officers and Certification and Accreditation Officers benefit from simple, cost-effective accreditation processes that are both attainable and repeatable. From inception, SimShield development has involved government certifiers, and the product was designed to meet stringent security policies for Cross-Domain Solutions. TCS also provides Certification and Accreditation (C&A) templates for use in preparation for the accreditation process. TCS has fielded hundreds of applications that are part of accredited systems and has engineered its product to satisfy Cross-Domain Security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) Cross Domain Solutions C&A processes.

Additionally, Security Officers and Certification and Accreditation Officers benefit from the inherent requirement that TCS products use a trusted operating system where the pairing of Multi-level Security (MLS) and Type Enforcement (TE) security polices provide a strong platform protecting against application misbehavior, both accidental and intentional. SimShield is available on two trusted operat-

ing systems, Trusted Solaris™ 8 and Red Hat® Enterprise Linux® 5 (RHEL5). Both trusted operating systems meet the Common Criteria's Labeled Security Protection Profile (LSPP). The Trusted Bridge uses rule sets generated by the Policy Editor to provide security filtering for training data in the HLA and TENA environments. This design simplifies the certification and accreditation process, as only the rule set library must be revalidated when changes are made to the object models used by participating training assets. To the existing systems in the High and Low side networks, the near real-time CDS guard activities of SimShield will be transparent; thus, providing best-in-class data throughput from one domain to another.

SimShield Features

SimShield provides a solution to the multi-level interconnectivity challenges faced by the simulation and training communities. Below is a workflow architecture diagram illustrating the two SimShield components, the Policy Editor and the Trusted Bridge.

The Policy Editor is a stand-alone system that provides the opportunity for human review and approval in addition to automated system checkpoints for ensuring that the rule set is built accurately before being loaded into the Trusted Bridge.

Policy Editor

The Policy Editor is the tool for defining the rules on which the Trusted Bridge operates. The most important functions of the Policy Editor are to:

- support security domain and data experts in defining classification filtering and sanitization rules between training networks communicating through the Trusted Bridge;
- provide persistent storage for rules and associated reclassification justifications; and
- provide a user-friendly environment.

The GUI design is based on the Model-View-Controller (MVC) architecture supported by Java™ (commonly referred to as Swing). In this approach, application behavior and presentation are the responsibility of the Swing controller and view components; examples of which include trees for displaying hierarchical data, buttons for initiating action processing, and fields for inputting data.

The rules built by the Policy Editor are at the heart of the Trusted Bridge's functionality. The Policy Editor identifies each system user and applies access controls over what data a user can read, create, or modify. This is accomplished by using a Database Management System (DBMS) that provides a robust set of security features including identification and authentication, user roles, and fine-grained audit controls and logging. Therefore, the Policy Editor uses a two-tiered (client/server) architecture as seen in Figure 2. The application architecture is partitioned to show the presentation logic encapsulated in a client application while the data and processing logic are maintained in the server.

Figure 1 - Workflow Architecture Diagram

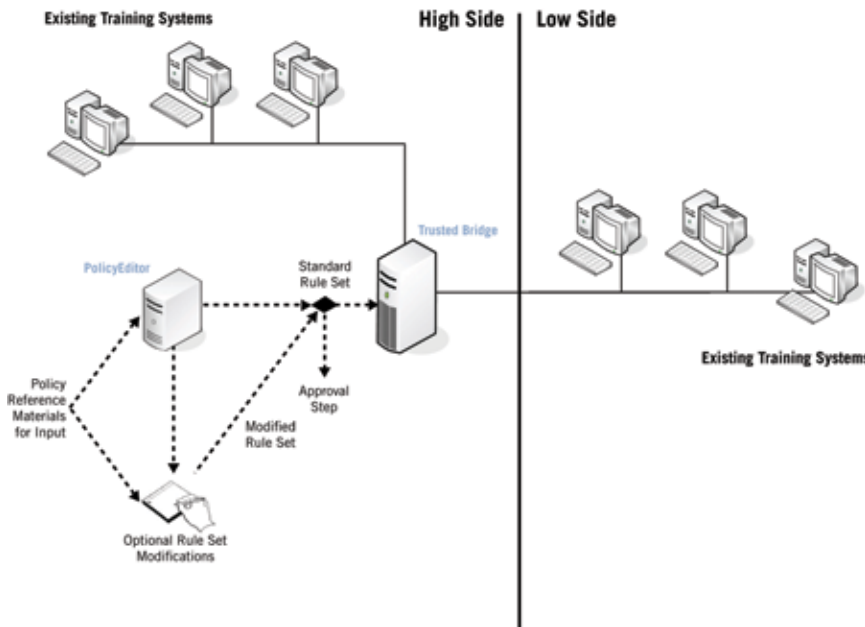
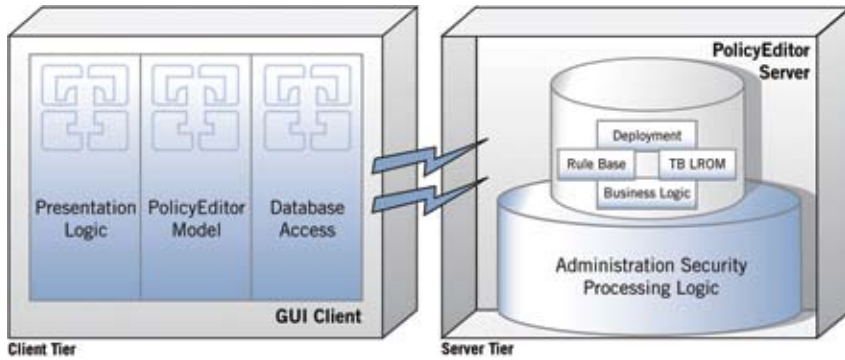


Figure 2 - Policy Editor Architecture



Policy Editor model classes provide the data portion of the MVC paradigm and also communicate with the data access layer by means of well-defined interfaces. The data access layer manages database connections and implements the methods needed to query or update the database. This approach of separating the data representation seen by the user from the data access details provides flexibility and extensibility. Changes or enhancements to the Policy Editor server data structures or functionality need conform only to the interface for communicating with the model, not to the presentation and control portions of the application.

The client partition is the only part of the Policy Editor application seen by the user. It is responsible for presenting data to the user, interacting with the user, and communicating with the server tier. The client supports application logic designed to facilitate the presentation and navigation of the Policy Editor rule processing components, as well as, a number of utilities for remotely creating and administering a rule base.

Trusted Bridge for HLA and TENA Environments

- The Trusted Bridge in both HLA and TENA environments provides bi-directional filtering capabilities by managed rule sets. The rule set checks the data for type and content and then Passes, Fails, or Sanitizes the data.
- The “trusted process” of the Trusted Bridge stores incoming data in separate caches designated for the High side domain and

the Low side domain. Additionally, the rule set enforces separate and distinct filter rules for data flowing from High to Low and from Low to High.

- The Trusted Bridge has three separate roles:
 - The *Administrator* role is able to create new user accounts as well as access specific configuration files.
 - The *Operator* role is assigned to users who can only start and stop the Trusted Bridge. These users are restricted from changing the rule set library that is installed on the system as well as any other configuration files.
 - The *Watch Officer* role is assigned to users who can change the rule set library that is installed on the system.
- Fixed format data is dissected for content so that the Trusted Bridge can make a decision to Pass, Fail, or Sanitize the data.
- Malicious code detection is handled by dissecting fixed format data. The Trusted Bridge drops any malicious code that does not have the content expected and required by the rule set. Due to this content based filtering, other mechanisms such as virus checking are not required.
- Multiple Security Level (MSL) capability is provided through labeling, segregating, and protecting to ensure classified information is prevented from transfer and disclosure to a network or application that is not authorized to access the data.
- Trusted Bridge auditing capabilities:
 - Standard auditing of user operations (logging in, opening a terminal, running the Trusted Bridge, changing configuration files, etc.).

- Standard audit of rule set configuration.
- An audit is maintained consisting of the message ID, time stamp, incoming network (High or Low side), and whether the data was Passed (as is), Failed, or was Sanitized (data modified), then allowed to pass to the other enclave.

Architecture

The exchange of data between HLA or TENA networks operating at different security levels presents security challenges. One important challenge is ensuring that classified data is labeled, segregated, and protected to prevent the transfer and disclosure of classified information to a network that is not authorized to access the data.

The Trusted Bridge provides an MSL capability to label, segregate, protect, and exchange data between training networks executing at different security levels. This capability is designed to meet the data format and near real-time performance requirements of distributed training enclaves executing in this capacity. It is also designed to meet the security certification and accreditation requirements for multi-level guard systems.

Trusted Bridge Architecture in an HLA Simulation Environment

An MSL environment is one in which multiple, single security level networks (in this case, federations) are interconnected by the use of a multi-level secure (MLS) device (in this case, the Trusted Bridge). The entire distributed simulation configuration is not considered MLS because that would imply that each component has multi-level security capabilities. The fundamental security requirements are to:

- protect classified information appropriately at all levels;
- protect information from tampering, loss, and destruction—whether malicious or accidental;
- protect the Trusted Bridge system from foreseeable denial of service conditions; and
- manage changes affecting the security of the Trusted Bridge and the impact of these changes on accreditation.

The Trusted Bridge includes a single Trusted Bridge Process (TBP) and, for each federation, an Untrusted Surrogate Federate (USF). The USF processes operate as federates on the trusted operating system component to handle the cross-federation operations. This can be illustrated with the example of object publication—a USF forwards and publishes all objects between its parent federation and all other participating federations as allowed by the TBP.

Note: Notice that two similar terms are used throughout this section: Trusted Bridge and Trusted Bridge Process (TBP). To reduce confusion, this document will consistently differentiate between the TBP, which is the central process that checks, validates, and filters data between the two USFs, and the Trusted Bridge, which is the entire system made up of the TBP and the USFs.

- performing any necessary modifications of the data in accordance with the security policy;
- guaranteeing the integrity of the data; and
- including all the processing necessary to manage asynchronous communication between the USFs.

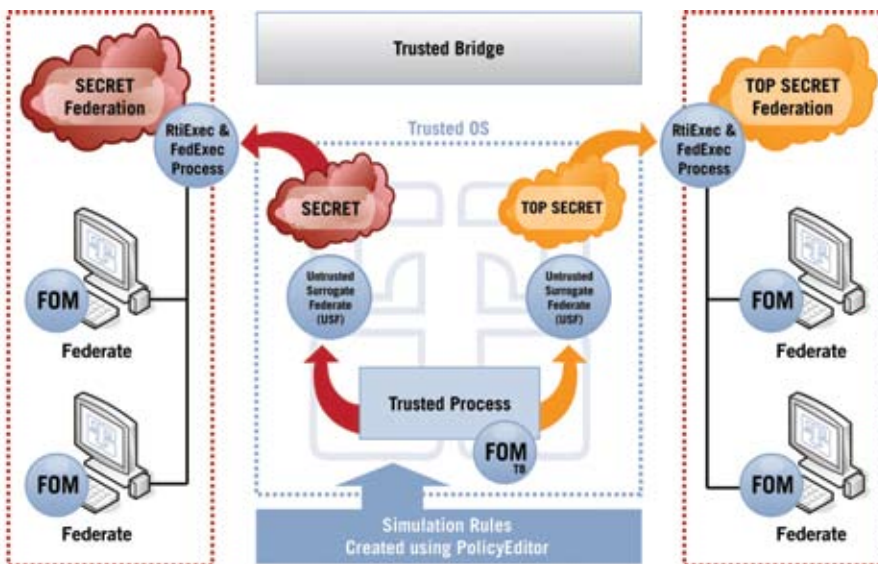
In the Trusted Bridge architecture, each federation and its USF use the same Federation Object Model (FOM). The Trusted Bridge FOM describes the objects and interactions that will be passed between federations and should correspond to the set of objects and interactions for which there are security filter rules. The TBP security filter passes data between the USFs only if: (1) there is a security policy for that object or interaction; and (2) the data meets the security policy rules for that object or interaction. The TBP does not perform conversion of object, attribute, interaction, or parameter definitions.

Bridge, there are two USFs along with one TBP that controls the execution and communication between the USFs.

The following are the Trusted Bridge's software units, which are collections of classes that together perform a cohesive task:

- The TBP contains all the actions necessary to read the configuration files, start logging, load the Rule Set Library and call the Rule Set Library Initialization, create the Message Passing Interface, and start the USFs. During operation, it uses the Rule Set Permissions and Rule Set Filter Functors to Pass, Fail, or Sanitize data.
- The USF software unit reads the USF configuration files, initializes communication with the Trusted Bridge through the Message Passing Interface, and coordinates communication with the federation through the HLA API.
- The FOM Support software unit is a collection of classes that all the TBP and the USFs read in the attributes.txt file, and then parse to understand the FOM and assign unique Trusted Bridge handles to object classes, interaction classes, attributes, and parameters.

Figure 3 - HLA Architecture



There is no direct communication between the dissimilar labeled USF processes. Communication between the USFs occur solely through the TBP. The responsibilities of the TBP are:

- mapping and processing data from one federation to another federation;

The Trusted Bridge is composed of two main process types: USFs and the TBP. Each USF encapsulates all the HLA functionality required to communicate with other federates. The TBP encapsulates all the security-relevant functions as well as all communication with the USFs. For each instance of the Trusted

Trusted Bridge Architecture in a TENA Training Environment

SimShield satisfies the following TENA requirements:

- It provides a flexible, extensible and portable simulation platform (not a single, monolithic simulation) that satisfies the needs of all users and subscribing systems.
- It accommodates the need for future technological capabilities and a variety of operating configurations.
- It provides interoperability of simulations and reuse of their components, which is critical.

The core of TENA is the TENA Common Infrastructure, including the TENA Middleware, the TENA Repository, and the TENA Logical Range Data Archive. TENA also specifies the existence of a number of tools and utilities, including those necessary for the efficient creation of a logical range. Range instrumentation systems (also called range resource applications) and all the tools interact

with the common infrastructure through the medium of the TENA object model. The TENA object model encodes all the information that is transferred between systems during a range event. It is the common language with which all TENA applications communicate.

For TENA executions in the High and Low domains, the near real-time communication provided by SimShield is transparent. TENA Middleware provides common communication services within a single-level TENA execution. SimShield allows distributed networks to communicate by using the TENA interface specification and operating under different security classifications. SimShield uses plug-in libraries to provide security filtering and object reclassification.

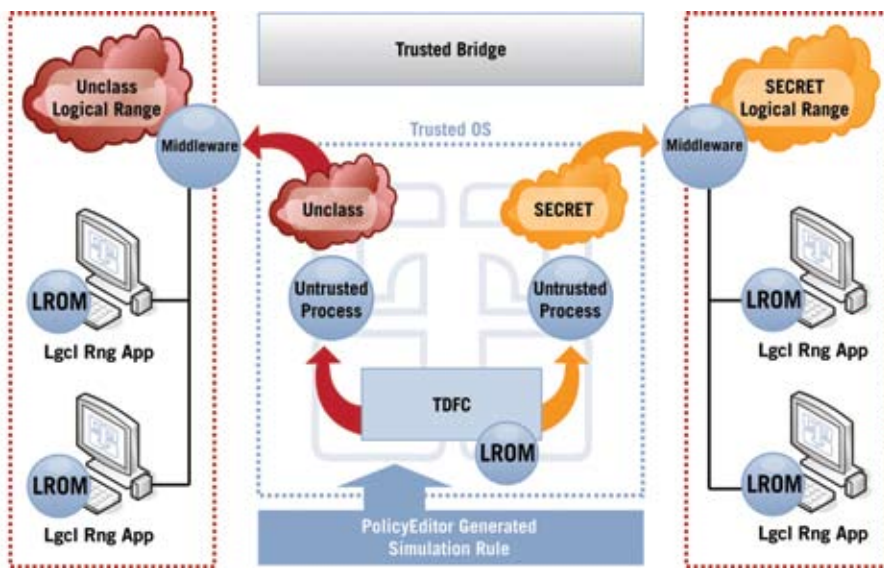
ing to the rule set as to whether it should Pass, Fail, or be modified and then passed as Sanitized. All data that is transferred through the CDS is evaluated by the rule sets that were generated by the Policy Editor. The rule set is configurable and developed by the end user and/or a designated security officer.

Implementation

When TCS brings SimShield into your environment, we leverage more than a decade of experience implementing Cross-Domain Solutions by using a proven process tailored to each customer's mission. The objective is to deploy a functional, manageable, and creditable solution within which users and

- TCS orders and delivers all requisite software and hardware (if applicable) to the customer
- TCS conducts a project kickoff meeting with the customer. The primary objectives of the kickoff meeting include:
 - Introduction to the project team players
 - Project-specific overview of the technical and C&A processes
 - Resolution of administrative details, such as the confirmation of required security clearances
- The TCS Project Manager sends the SimShield technical site survey to the customer to complete and return prior to the installation.
- The technical implementation process includes:
 - Customer completion and return of the technical site survey
 - TCS-conducted on-site survey if needed
 - Resolution of technical issues and preparation for installation
 - On-site installation and requisite C&A approval as needed
 - Administrator training
 - Post-installation support as needed based on contract
- In parallel, TCS pursues the C&A process with the customer based on the customer's specific needs and the number and type of networks requiring access. Basic activities TCS performs include the following:
 - Work with the customer C&A counterpart to complete the appropriate C&A documentation and coordinate with relevant accreditation parties.
 - Facilitate attainment of appropriate C&A approval to allow connection to production networks for system installation.
 - Provide C&A testing support, which can include coordination, updating relevant C&A test procedures, and preparing for test events.
 - Facilitate attainment of appropriate C&A approval (such as Authority to Operate, or ATO) allowing operation on production networks.

Figure 4 - TENA Architecture



The Trusted Bridge component of SimShield uses the TENA protocol and securely restricts the flow and distribution of data between a Low side and a High side as pictured in the architecture diagram (Figure 4) as unclassified and classified enclaves. SimShield subscribes or "listens" to all the data that is to be passed through the CDS. The data is then passed to the "trusted process" and evaluated accord-

ing to the rule set as to whether it should Pass, Fail, or be modified and then passed as Sanitized. All data that is transferred through the CDS is evaluated by the rule sets that were generated by the Policy Editor. The rule set is configurable and developed by the end user and/or a designated security officer. Most SimShield implementations entail two parallel but equally important paths: technical implementation and C&A support. SimShield implementations typically include the following steps:

Certification and Accreditation

SimShield is engineered to satisfy the Cross-Domain Security requirements imposed by C&A processes such as Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) Cross-Domain Solutions. TCS is involved in C&A process development and improvements for a variety of directives and programs. Active participation in the accreditation communities and accreditation authorities ensures that the products, processes, and documentation evolve to meet changing requirements. Involvement and continued leadership in many of the key forums and process assessments provide TCS with the depth and breadth of experience needed to field operational systems.

For those instances in which customers need a head start on the C&A process and desire to do the rest of the work themselves, TCS provides templates, based on availability, for customers to complete and facilitate the appropriate C&A process. This includes C&A document templates and test procedure updates. TCS involvement in community C&A activities includes the following:

Process and Documentation

- Director of Central Intelligence Directive 6/3 (DCID 6/3)
- Joint Air Force–Army–Navy (JAFAN 6/3)
- DoD Information Assurance Certification and Accreditation Program (DIACAP), which supersedes DITSCAP
- National Institute for Standards and Technology (NIST) C&A Process

Accreditation Communities and Authorities

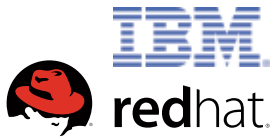
- Unified Cross-Domain Management Office (UCDMO)
- Department of Defense Intelligence (DNI)
- Information System Cross-Domain Management Office (DoDIIS CDMO) Secret and Below Interoperability (SABI)/Cross-Domain Solutions (CDS)
- Top Secret/SCI and Below Interoperability (TSABI) DoD Security Accreditation Working Group (DSAWG)
- DIA Information Assurance
- NSA Information Assurance Directorate
- SIPRNET Connection Approval Office (SCAO)

TCS Community Leadership

- Contributions to Director of National Intelligence (DNI) C&A Revitalization Tiger Team Forums
- Contributions to NIST C&A Process Development
- Enhancements to DITSCAP/DIACAP

Conclusion

SimShield provides a secure solution to the difficult problem of providing training to war-fighters with training assets that operate under different security classifications to fully communicate and interact securely.



Genuine Innovation in Cross-Domain Solutions on Linux with IBM and Red Hat

IBM, TCS, and Red Hat bring to government the first Cross-Domain Solutions on a Linux trusted operating system. Playing to each company's strength, the alliance offers the reliability of over 100 years of hardware innovation from IBM, the security of accredited Cross-Domain Solutions installed in operational systems from TCS; and the flexibility of an open, mainstream operating system from Red Hat.

About Trusted Computer Solutions, Inc.

Founded in 1994, Trusted Computer Solutions (TCS) is an industry leader in Cross-Domain Solutions. The company's SecureOffice® Suite of software products enable government and industry to securely share information, striking the right balance between information protection and information sharing, a vital component to national security. All SecureOffice products adhere to the most stringent security standards set by US Government Agencies such as the Defense Intelligence Agency and the National Security Agency. SecureOffice products, which run on trusted versions of Linux and UNIX, are installed and accredited in operational systems around the world today protecting our nation's most sensitive digital information. TCS is headquartered in Herndon, VA with offices in Champaign, IL and San Antonio, TX.

For more information, visit www.TrustedCS.com



TCS Corporate Office

2350 Corporate Park Drive Suite 500
Herndon, VA 20171
703.318.7134

TCS Trusted Operating Systems Lab

2021 S First St Suite 207
Champaign, IL 61820
217.384.0028

TCS Texas Office

10010 San Pedro Suite 220
San Antonio, TX 78216
210.340.3151

SecureOffice is a registered trademarks of Trusted Computer Solutions, Inc. Linux is a registered trademark of Linus Torvalds. All other trademarks and registered trademarks are the property of their respective owners.