

## Table of Contents

- 1 Introduction
- 2 SecureOffice Trusted Gateway Benefits
- 3 SecureOffice Trusted Gateway Features
- 3 The User Experience
- 4 File Transfer Management
- 4 Key Components for Managing Secure File Transfers
- 5 Architecture
- 6 Implementation
- 6 Certification and Accreditation (C&A)
- 6 Hardware Requirements and Supported Configurations
- 7 Conclusion

## Technical Abstract

# SecureOffice Trusted Gateway

## Introduction

### A SecureOffice Cross-Domain Transfer Solution

Sharing the right information at the right time is one of our nation's best weapons against terrorism and other security threats. Civilian, intelligence, and military communities need to make critical data immediately available, requiring the transfer of information between networks at different classification levels.

SecureOffice® Trusted Gateway™, developed by Trusted Computer Solutions (TCS), is a Cross-Domain Solution application running on the Red Hat® Enterprise Linux® 5 (RHEL5) trusted operating system. This application provides rapid, multi-directional transfer of any data type between numerous security levels, such as Unclassified, Secret, Secret Releasable, and Top Secret/Sensitive Compartmented Information (SCI) networks. Multi-directional transfer of information includes sending sanitized information from a higher-level network to one at a lower level, moving data from a lower level to a higher level, and moving files laterally across network boundaries. SecureOffice Trusted Gateway can move one or more files from any level to any level, allowing many high or many low destinations.

As a significant upgrade to the Trusted Gateway System on Trusted Solaris™ (which has been fielded and operational for almost a decade), SecureOffice Trusted Gateway continues to provide one-way secure transfers (including bulk transfers) while also supporting multi-directional transfer capabilities. A web-based interface for two-person reliable human review and support for the industry standard Secure Shell (SSH) for file uploads can be customized to meet site and security requirements.

All TCS software products require a trusted operating system as a primary mechanism for security policy enforcement. 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 combination of these security attributes provides full segregation and protection of all data on the system. RHEL5 is the first secure Linux operating system to receive an Evaluation Assurance Level 4 (EAL4) under the National Information Assurance Partnership (NIAP) against the Common Criteria requirement associated with Cross-Domain Solutions, which includes LSPP, CAPP, and RBAC protection profiles.

SecureOffice Trusted Gateway was designed to meet and exceed the requirements for a Protection Level 4 (PL4) system under the Director of Central Intelligence Directive 6/3 (DCID 6/3) and Department of Defense (DoD) Information Assurance Certification and Accreditation Program (DIACAP). The technical design is based on secure systems engineering practices and trusted operating system security enforcement at the server level.

SecureOffice Trusted Gateway strikes the right balance between information protection and information sharing. All SecureOffice products adhere to the most stringent US government security standards, enabling access and sharing while maintaining the data protection levels required by national security standards.

SecureOffice Trusted Gateway supports an unlimited number of networks to upgrade, downgrade, or move data swiftly and securely across network boundaries.

hardware and requiring minimal training and maintenance costs. Product access through a user-friendly web interface results in a short learning curve, minimizing training and support costs. The SecureOffice Trusted Gateway workflow streamlines the information transfer approval process, which enhances staff productivity and allows faster mission completion. Current staff can easily support SecureOffice Trusted Gateway, with no additional engineering resources required to manage or maintain the implementation(s). SecureOffice Trusted Gateway is installed

additional product support requirements. Full support of DoD and Intelligence Community (IC) Public Key Infrastructure (PKI) means current systems do not need to be duplicated. Access rights can be configured by user, file type, source, and destination policies. SecureOffice Trusted Gateway manages the file movement, ensuring that the network is protected while blocking unauthorized network intrusions. Administrators can easily add, delete, or modify user accounts and permissions.

SecureOffice Trusted Gateway **Users** benefit from an easy-to-use interface for initiating, approving, or managing transfer requests. The web-based workflow guides users through the process of initiating jobs and managing approvals. Upon login, a summary page shows users both pending and approved job requests. Simple desktop functions such as drag-and-drop, preloaded global address books, and job workflow minimize the need for training and enhance the user's ability to quickly get up and running in the application.

SecureOffice Trusted Gateway requires a trusted operating system as the mechanism for security policy enforcement and meets **Security Officer**, agency, and accreditor requirements for secure information transfer. SecureOffice Trusted Gateway maximizes the operating system security features and additional security mechanisms to include restrictive integrity policy. The security policies protect against both accidental and intentional application misbehavior. All processing happens at the level at which the job is created. Each job must clear virus scanning and file typing procedures, after which dirty word search, content validation, manual file review, archive, audit, and quarantine policies are processed as configured. Both automated and user-assisted archiving procedures are supported.

**Certification and Accreditation Officers** benefit from simple, cost-effective accreditation processes that are both attainable and repeatable. From inception, SecureOffice Trusted Gateway development involved government certifiers and was designed to meet the stringent security policies for Cross-Domain Solutions. TCS also provides Certification and



The graphical user interface provides users with simple workflow tools to initiate, track, and respond to all file transfer requests.

## SecureOffice Trusted Gateway Benefits

SecureOffice Trusted Gateway provides benefits for Budget Stakeholders, Administrators, Users, Security Officers, and Certification and Accreditation Officers.

For **Budget Stakeholders**, SecureOffice Trusted Gateway provides a low total cost of ownership (TCO) by using commodity

on a single server that runs the open, mainstream RHEL5 operating system, offering lower-priced hardware platform choices to further reduce the TCO over proprietary and government-developed systems.

**Administrators** benefit from a low-maintenance solution that enforces security requirements. Internet Explorer® and Firefox® customers can use their current browsers to access the web-based interface, eliminating

Accreditation (C&A) templates that can be used to streamline the accreditation process. TCS has fielded hundreds of applications that are part of accredited systems and has engineered its products 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. TCS products are built on the security mechanisms in the RHEL5 operating system, which is certified by NIAP for Common Criteria Evaluation & Validation Scheme at EAL4+.

## SecureOffice Trusted Gateway Features

The key attributes of SecureOffice Trusted Gateway include a host of usability, security, and manageability features.

### Usability:

- Web-based interface for multi-directional file transfer management and workflow including drag-and-drop capabilities
- Data movement from and to an unlimited number of approved classified networks supporting
  - File transfer by data push or email distribution
  - Any-to-any classification level jobs
  - Multiple file job requests
- Workgroup and enterprise deployment
- Secure transfer management from request through destination
- Transfer of any pre-authorized file type
- Automated one-way transfer for low-to-high bulk uploads

### Security:

- Complete file protection and management to include virus scan, file type, dirty word search, content validation, manual file review, archive, audit, and quarantine policies
- Strong authentication support using DoD/IC PKI (X.509 digital certificates)
- Encrypted communication connections throughout the data transfer process
  - Enhanced transmission security with Secure Copy Protocol (SCP) over SSH for low-to-high transfers
  - Secure Sockets Layer (SSL) transmission security for high-to-low transfers

- Runs on RHEL5, the first Linux operating system certified by NIAP for the Common Criteria Evaluation & Validation Scheme for EAL 4+, LSPP, CAPP, and RBAC protection profiles
- Strengthened security from pairing the SELinux TE and MLS security models
- Compliance with Automated Intelligence Community Inter-Domain Transfer Policy featuring Two-person Reliable Human Review
- Foreign Disclosure Officer (FDO)—compliant review process
- Configurable archive and auditing processes

### Manageability:

- User access through standard browsers; such as, Internet Explorer or Firefox
- Web-based access requires no software installations on users workstation
- Wide range of commodity hardware supported
- Operates on a mainstream, open source operating system
- Complete archive and audit management capabilities

## The User Experience

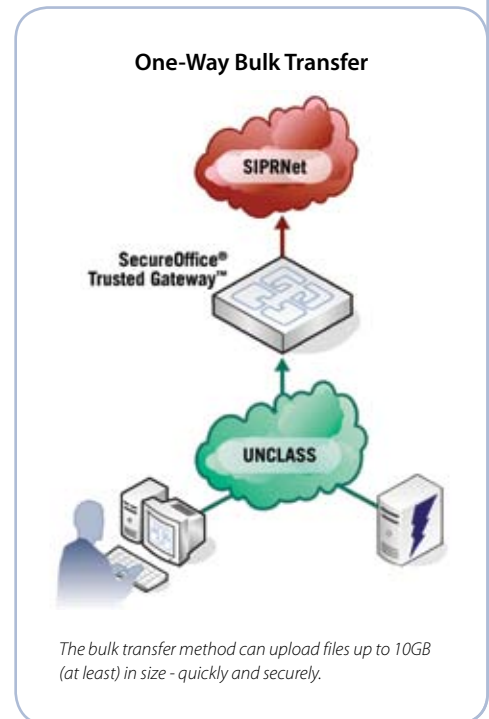
Customers need to communicate critical information, such as imagery, maps, documents, and data files, to people and systems in different security enclaves while keeping the data secure and preventing any unintended release. SecureOffice Trusted Gateway provides a web interface for users to create and manage jobs. The web interface permits users to transfer files from any level to any level, as allowed by policy.

In addition, SecureOffice Trusted Gateway provides a one-way bulk transfer mechanism to facilitate automated file uploads. This is generally used when transferring large quantities of files from low to higher level classified networks.

The graphical user interface provides users with simple work flow tools to initiate, track and respond to all file transfer requests.

## Automated One-Way Bulk Transfers (Low-to-High)

SecureOffice Trusted Gateway provides rapid, one-way bulk transfer to defined high-side destinations at varying security levels. UNIX® desktops support direct file transfers with SCP delivering files directly to SecureOffice Trusted Gateway for processing. The destination, transfer speed, and SCP version can be customized to meet specific site policies and procedures. An optional SecureOffice Trusted Gateway service can be used on any PC running Windows 2000 or later, allowing users to maintain local input directories. SecureOffice Trusted Gateway monitors the local folder and automatically copies the file securely for processing. Users can copy or drag-and-drop files into the designated directory to submit them for transfer. A right-click shortcut allows users to send files to defined destinations, which are configurable and can be secure FTP (SFTP) servers, FTP servers, or email addresses at permitted classification levels. This operation moves the file to SecureOffice Trusted Gateway, which automatically manages transfers to approved lateral or higher classification network(s) upon detection. For security reasons, only configured hosts can access the input directory through SCP. All other connection attempts are denied.



### Web-Based Multi-Directional Workflow

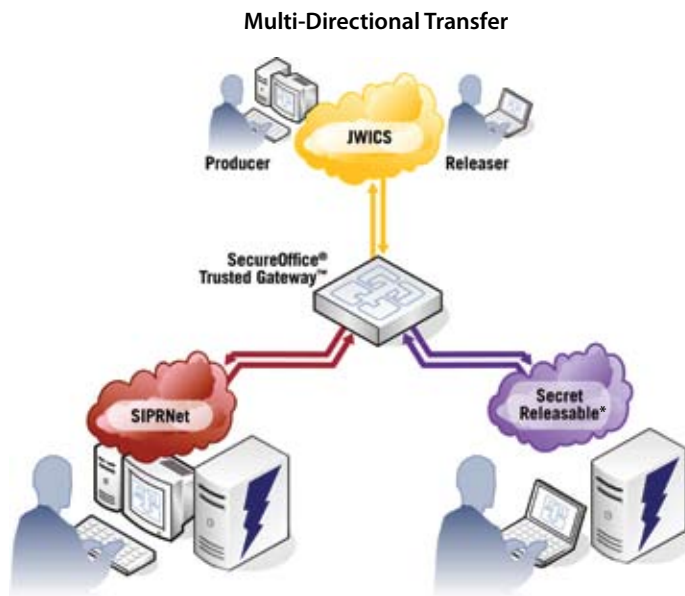
The web-based interface provides users with a simple workflow process that guides them through each transfer. The web-based interface offers drag-and-drop, queue notification, and end-to-end workflow capabilities for managing each transfer. Users can request to move data in any direction based on their clearance, site security policies, and account access rights. The web-based interface is required for any transfers requiring two-person or FDO review. Upon login, each user must authenticate through his or her X.509 digital certificate and accept standard terms of use indicating that all actions are being monitored.

tent validation based on configured policies. If all implemented validation checks pass after the virus scan and file type process, the job can be submitted to the specified Releaser(s).

Reliable Two-Person Human Review, typically used for all high-to-low classification transfers, requires Releasers to view requests and, for each included file, review and accept initial dirty word search results. Files can then be approved for release to the designated network(s). Before delivery, the files are again screened for viruses and must meet set file type policies at the time of release. Once approved by a Releaser, the request is completed and the job status is updated for the Producer.

Regardless of how the job is initiated, SecureOffice Trusted Gateway manages the process to ensure safe and approved file movement between secure networks and across classification levels following site security policies. SecureOffice Trusted Gateway is configured based on customer requirements.

Once a request is made to transfer files, either through the bulk upload mechanism or the web-based interface, SecureOffice Trusted Gateway receives the files beginning with a secure network connection through SCP or SSL. Based on the security policy for the transfer, virus scan, file type, and all configured checks are processed meeting site security and operational requirements. Once the file clears all these steps, it is securely moved to the intended destination network through SFTP, FTP, or email.



SecureOffice Trusted Gateway supports an unlimited number of networks to upgrade, downgrade, or move data swiftly and securely across network boundaries. \*A firewall and Intrusion Detection System (IDS) may be required.

Producers have rights to initiate transfer requests. Each new request allows the Producer to select one or more Destination, establish a job name, and designate Releasers. Destinations can only be set up by the Administrator and may consist of the destination classification level, SFTP servers, FTP servers, or email addresses. Releasers have rights to validate and permit the Producers' request(s). The Producer then uploads all necessary files and the SecureOffice Trusted Gateway manages virus scan, file type, dirty word search, and con-

### File Transfer Management

SecureOffice Trusted Gateway performs all processing at the level at which the file is submitted for transfer. File transfer rights can be based on user, file type, source, and destination policies. This is an end-to-end process that ensures and protects data movement and meets both national security requirements and file management best practices, providing swift and secure file transfers.

### Key Components for Managing Secure File Transfers

The configuration of SecureOffice Trusted Gateway is managed to a granular level, ensuring that user, file type, source, and destination policies are followed. All files are required to pass virus scanning and file type policies prior to movement. Dirty word search, content validation, manual file review, archive, audit, and quarantine policies can be configured to meet the most specific requirements and policies.

#### Virus Scanning

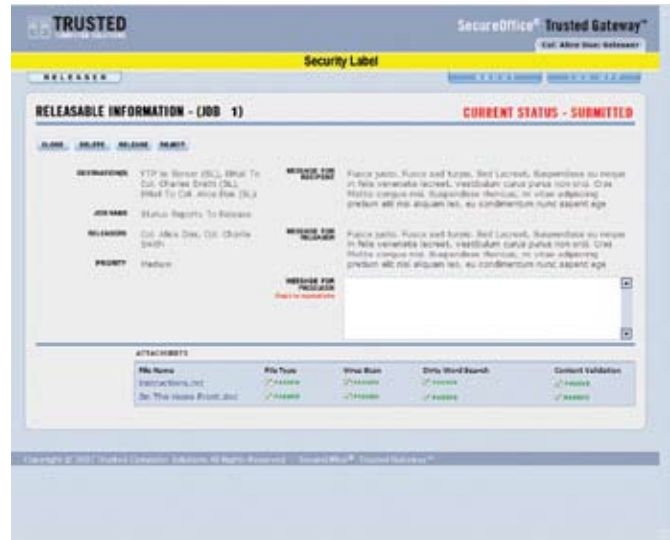
SecureOffice Trusted Gateway incorporates CyberSoft™ VFind to scan files or can be customized to exclude certain trusted types from virus scanning for performance enhancement.

#### File Type Verification

Three different varieties of file type checking are employed in SecureOffice Trusted Gateway. Extension matching, TCS signature algorithm, and the Universal Atomic Disintegrator (UAD) algorithm from CyberSoft allows user-configurable options for file type verification. The file verification signatures can be customized to accommodate unique file types, configured by both source and destination policies.



From the web-based interface, Producers select the destination level(s), distribution point(s), and the Releaser(s).



The Releaser can view instructions, destinations, and status as well as check the results of the dirty word search prior to releasing the file.

### Dirty Word Search

SecureOffice Trusted Gateway checks files for sensitive or “dirty” words that should not be released to other networks. The set up also allows for the designation of “clean” words, which are common words that contain within them dirty words. For example, the word “secretary” contains the word “secret” but it is considered a false positive and can be ignored. Administrators can create and customize a master list of both dirty and clean words, as well as create lists that are used in the case of specific source and destination pairs. Once these lists and transfer pair rules are configured, each file uploaded to SecureOffice Trusted Gateway is searched against the list for matches.

The process ignores spaces, carriage returns, and other formatting information. Therefore, if “Top Secret” were listed as a dirty word, “TOP SECRET” and other variations would be identified. Dirty words can span lines, contain embedded white space, and be embedded within other words.

If dirty words are found in a document, the user is given an option to override and accept the word. The user’s acceptance of

each dirty word is recorded and stored in a database available for audit. Every dirty word must be overridden before the job containing the flagged document can be submitted for release. The Releaser can be optionally required to review all the dirty words before releasing the job. All additional actions and overrides are stored in an audit-able database.

### Content Validation\*

If configured, files are scanned to identify and remove a wide range of hidden or embedded data and metadata within Microsoft Office documents. This option provides added assurance to prevent inadvertent or malicious disclosure of sensitive or proprietary information when government documents are downgraded and released.

### Manual File Review

By default, the Releaser must download and review all files.

\*Third party software is required. Contact TCS for additional information.

### Archive and Audit

SecureOffice Trusted Gateway supports archiving and audit procedures.

### Quarantine

Established parameters can be created to quarantine specific requests and files in a designated folder, meeting each site’s security policy.

### Architecture

All programs and the SecureOffice Trusted Gateway processes are run at the configured sensitivity labels to provide strong domain separation.

All original uploaded files are stored in a protected area until archived by the administrator. All web-based traffic is filtered and logged by a web server that provides identification and authentication of the user’s X.509 certificate against an internal Certificate Store including all known root Certificate Authorities. The certificate is also compared against the Certificate Revocation List, which can be updated automatically based on site security policies.

The servlet engine generates viewable web pages, while the database stores all actions. User interactions are validated (uploading a file or viewing the status of a job) against authorizations provided by the database. Additionally, the state of each job is stored.

Each job is then managed through the workflow, which calls and manages all configured business logic and processes. When all the workflow steps are complete and passed, files are transferred to the approved destination(s).

## Implementation

SecureOffice Trusted Gateway can be deployed locally for a single purpose, as part of an enterprise implementation, or as part of a complete Cross-Domain Solution, providing a closed-loop connection from the end-user to the backend network connections.

When TCS brings SecureOffice Trusted Gateway to your environment, the company leverages more than a decade of experience implementing Cross-Domain Solutions using a proven process tailored for each customer's mission. The objective is to deploy a functional, manageable, and accreditable solution with which users and system administrators are productive. TCS has learned that engaging customers in a project team approach with our engineers is the most effective method to achieve this objective. Most SecureOffice Trusted Gateway implementations entail two parallel but equally important paths: technical implementation and C&A support.

## Certification and Accreditation

SecureOffice Trusted Gateway is engineered to satisfy the cross-domain security requirements for processes such as, Top Secret/SCI and Below Interoperability (TSABI) and Global Information Grid Interconnection Approval Process (GIAP)/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. Continued leadership in many of the key forums and process assessments provides 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 can provide templates (based on availability) to complete and facilitate the appropriate C&A process.

## Hardware Requirements and Supported Configurations

### Recommended User Requirements

Internet Explorer 6 or 7, or Firefox 2.x  
Contact TCS for additional information regarding unlisted browsers.

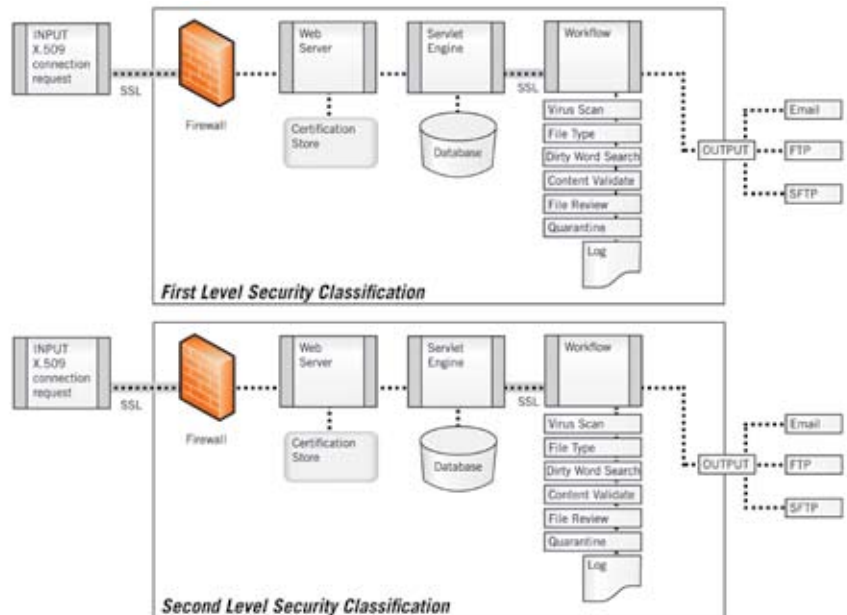
### Recommended Trusted Gateway Server Sizing

2 GHz 2x Dual-Core Intel® Xeon®  
4 GB RAM  
250 GB hard drive, preferred 2X 250 GB in RAID configuration  
CD writer (for audit archival)  
Network interface cards: 1GB/sec with one interface to support every connected network (minimum of two interfaces)

### Optional Windows User Configuration for Automated Bulk Transfers

Any PC running Windows 2000 or later

Contact TCS for additional information on configuration and sizing recommendations for your specific environment.

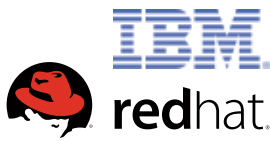


SecureOffice Trusted Gateway architecture can be duplicated to manage all transfer-level requirements, ensuring domain separation. Additional classifications can be added based on customer requirements.

## Conclusion

With hundreds of government clients and more than a decade of success, TCS is an industry leader in Cross-Domain Solutions. The company's products offer simple solutions that enable government and industry to securely access and transfer information, striking the right balance between information protection and information sharing—a vital component to national security. SecureOffice Trusted Gateway provides a secure solution to the difficult problem of satisfying file transfer security needs without sacrificing user access to information or productivity for both enterprise and local installations. Through SecureOffice Trusted Gateway, users have the capability to share information across any number of different security domains at different classification levels—from a single desktop. SecureOffice Trusted Gateway is designed to satisfy the information assurance accrediting community requirements, eliminate any potential leaks and risks, and provide users with a familiar and easy-to-use interface.





### **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](http://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 and Trusted Thin Client are 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.