

# Choosing the Right Platform for Trusted Cross-Platform Information Sharing

---

## WHITE PAPER

Sponsored by: Trusted Computer Solutions

Shawn P. McCarthy  
March 2008

---

## INTRODUCTION

True national security is achieved through protected information sharing — conducted as close to real time as possible. Often such data sharing is achieved by building systems that allow professionals, ranging from the intelligence community to first responders, to have access to the timely information needed to help protect both citizens and infrastructure.

Today, data, security alerts, and other safety- or defense-related information may be classified and may reside on multiple machines across multiple agencies or levels of government. Sharing this information is paramount, but to do so, government officials may find themselves facing a choice between sharing need-to-know data and protecting the secure environment of their networks. This isn't a viable choice in today's world. Agencies need to do both.

To answer this challenge, agencies must deploy specific technologies to allow all relevant parties to securely share intelligence data and other information. Government employees must be able to move sensitive data from one level of classification to another level, allowing for reliable and secure dissemination as needed across networks and secure domains.

A trusted Linux operating system (OS), running cross-domain applications, is a reliable way to meet these challenges. And it's one of the few solutions that are open and affordable. Today, that solution is delivered by the alliance of Trusted Computer Solutions (TCS), Red Hat, and IBM. TCS provides key pieces of the accredited cross-domain applications that run on the Red Hat Enterprise Linux 5 trusted OS, which, in turn, runs on IBM hardware platforms. The Red Hat Enterprise Linux 5 trusted OS on IBM provides a foundation for secure cross-domain situational awareness data collection; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); and other mission-specific applications.

## **BRIEF BACKGROUND ON TRUSTED LINUX**

The original trusted operating systems evolved in the 1970s as highly secure computing solutions. They improved accountability by associating each account with a specific user, auditing every action, and then associating each action with a specific user on the system.

The National Security Agency's (NSA) Security-Enhanced Linux (SELinux) specification took a solid step toward developing an open source version of a secure operating system. Red Hat then integrated SELinux into mainstream Linux by including SELinux in its Red Hat Enterprise Linux 4. This provided an OS with an open "trusted solution" that the NSA approved in 2006. The result: The government and the systems integrator community that serves the government now have a powerful, yet secure, platform upon which to build new sets of applications.

Trusted Linux has appeared at a time when government agencies are being tasked with improving their data-sharing efforts in the name of national security while also being tasked with reducing enterprise expenses by consolidating similar applications and merging redundant systems or full datacenters.

With major support from a partnership of TCS, Red Hat, and IBM, trusted Linux has already evolved into a powerful secure platform favored by systems integrators that work with government organizations in the areas of defense, intelligence, and homeland security.

---

### **Why Trust in an OS Is Important for Both Security and Interactive Systems**

It's fair to define a trusted system as one that meets a specific set of requirements that enable it to serve as a trusted resource by other machines. Thus, it's attractive for designers of trusted systems to build their solutions atop an OS that is enhanced with special security mechanisms and services to allow a computer to compartmentalize data and protect information and connections. Government agencies, especially those with a strong need to protect classified data or to protect any sort of data or system from hackers or other foreign threats, have a strong need for trusted solutions. Organizations that have an interest in the following tend to have a particularly strong interest in trusted computing:

- The National Information Assurance Partnership's (NIAP) operating system requirements help support the Common Criteria Evaluation and Validation Scheme (CCEVS) with an evaluation assurance level (EAL) of 4 or higher

- The Defense Information Systems Agency Common Operating Environment (COE)
- Systems with mandatory access controls, role-based access, labeled security, and controlled access for multilevel security (MLS)

Developing true cross-domain solutions is not just an academic exercise. There are multiple real-world applications for these types of systems. Being able to share data between agencies is vital for national security, and when there is an added element of classified data and vital protection of that data, then secure cross-domain systems become a vital part of the government's approach to data sharing. Another driving factor is the current trend in government toward consolidating large datacenters. As the number of datacenters is reduced, some government applications may need to interact with servers and databases that are located far away.

These types of cross-domain solutions require a trusted operating system. It's the most effective way to establish secure connections between machines and multiple sites. While cost savings are often a driving factor for system and/or datacenter consolidation, establishing secure connections between trusted systems should be the first step when building such solutions.

Only a handful of government-approved trusted operating systems have been made available in recent years. At the moment, the trusted Linux operating system from the TCS, Red Hat, and IBM alliance is the most actively evolving solution. As an open source operating system, it has the potential to help with overall cost savings.

As more information is made available over networks, the cost and complexity of trusted systems have actually increased, at least when it comes to using older trusted systems that had expensive licensing fees and slow upgrade paths. But within the past 18 months, Red Hat Enterprise Linux 5 has emerged as a cost-effective solution to this intricate issue. Being an open solution that can be tapped by any government agency or service provider, this solution has helped to drive down costs when deploying highly secure systems. In fact, deploying a secure server is now nearly as affordable as deploying a nonsecure server, thanks to the availability of the Red Hat Enterprise Linux operating system. This is a major sea change that is sparking strong interest among government agencies in migrating their secure systems as they work toward system and datacenter consolidation.

---

## **The Importance of Vendor Cooperation for Secure Solutions**

The ability to provide secure cross-domain access to classified data and to securely transfer this data requires a collaborative effort among vendors. Multiple stakeholders are involved with the federal government to ensure a high level of security:

- TCS develops and sells software products that allow government users to access information and securely transfer information across multiple secure networks at varying classification levels. These solutions all require certification and accreditation testing before becoming operational. TCS solutions today are widely implemented across defense, intelligence, and civilian agencies.
- Red Hat Enterprise Linux 5 is certified on several IBM server brands, including System x, System p, System z, and BladeCenter. Having Red Hat Enterprise Linux on multiple IBM servers meets government security standards, allowing Linux to be used in homeland security projects, in command-and-control operations, and throughout government agencies that previously were limited to just a few other secure systems.
- IBM Blade platforms and trusted solutions provide a fully trusted OS and a set of tools aimed at lowering the total cost of ownership of a trusted system, without sacrificing performance. Combined with a trusted thin client solution from TCS, this type of system simplifies the employee working environment by providing a single point of access to multiple secure networks while meeting the security and regulatory compliance needs of federal agencies.
- Other institutions, companies, and individuals have also contributed to the development of trusted Linux, and this community will have a strong interest in providing a clear upgrade path for this secure solution.

Compared with other solutions controlled by a single vendor, the trusted Linux approach has the potential to quickly close any software defects (if discovered) in a cooperative manner. It also has great potential for providing a common approach to secure computing that can be adopted by multiple vendors.

This type of hardware, combined with a powerful and secure OS, is prompting some government organizations to rethink their server strategies. Agencies realize the potential for cutting costs as they move toward large-scale system consolidation.

Potential cost savings for this type of migration include:

- Reducing operational costs by consolidating machines and moving toward open source solutions
- Simplifying infrastructure by focusing on a secure IT architecture that can integrate multiple IT services into an integrated solution housed on fewer machines
- Reducing complexity and streamlining server management
- Offering thin client solutions (Linux-based thin client architecture holds the potential for more processing power and functionality at the desktop using capable, yet still stateless, desktop devices. So, in the Linux version, substantially less processing horsepower is required in the back-end servers, allowing for the use of smaller, less costly Intel servers.)

## **BENEFITS WHEN RUNNING "CROSS DOMAIN"**

Government employees have unique security requirements when they need cross-domain access to multiple resources. Defense Department and intelligence agency personnel may require access to resources on a combination of Top Secret, Secret, Classified, and Unclassified networks. Meanwhile, local first responders and international partners may need to share data on their systems without having to worry that they are compromising their resources.

A cross-domain solution may or may not be the best choice for a specific installation. If government employees' jobs require them to access multiple secure domains, such as Secret Internet Protocol Router Network (SIPRNET), Stone Ghost, or Coalition, at different classification levels, the federal rules mandate that they do so securely. That entails either a separate physical, isolated connection to each network (multiple boxes at the desktop) or an accredited cross-domain solution that allows access to all authorized networks via a single thin client or desktop box.

A true cross-domain solution that supports access to multiple domains at various security levels from a single machine can meet the needs of most of those users. If the price is affordable, this kind of solution has great potential to become the platform of choice for end users, ranging from military field personnel to government datacenter personnel.

One example of how an agency can leverage the trusted Linux system for sharing data on multiple security levels can be found at the U.S. Coast Guard.

The U.S. Coast Guard achieved the first Authority to Operate (ATO) at the Top Secret and Below Interoperability (TSABI) level for a cross-domain system running on a mainstream trusted Linux operating system. The ATO was granted by the Accrediting Authority for the Joint Worldwide Intelligence Communications System (JWICS). The accredited system provides access to the top secret JWICS network and SIPRNET from a single desktop.

---

### **Major and Minor Migration Issues**

In many ways, migration to new operating systems is useless if agencies don't also move to a standardized configuration for their networks and data sharing rules.

When is the right time to migrate? Migrations should include hardware inventory assessments, application compatibility testing, and plans for data and software migration. All of these components are needed for proper time and costs planning associated with any system migration.

Often government agencies avoid moving to a new solution because they don't see a compelling business reason for the migration, especially when migrating from one trusted OS to another trusted OS solution. The compelling reason in this case is national security and the chance to enhance data protection and productivity for the long term by focusing on a robust open platform that will enjoy technical support for several years to come. Some proprietary solutions may not enjoy the long-term cost savings and extended user base found in today's open source communities. System consolidation should be top of mind when migrating to any new platform. Government systems became increasingly sprawling and redundant in the 1980s and 1990s. Any migration to a cross-domain secure solution should also investigate ways to retire older systems. In many cases, the cost savings from such retirements may help fund the new solutions, with the added benefits of closing security holds and improving national security.

---

### **Background: Risk Assessment for Operational Systems**

The CCEVS and the Certification and Accreditation (C&A) processes are "sister," but separate, processes that address risk. The CCEVS process focuses on "evaluating" a product independent of its environment, and the C&A process focuses on "accrediting" a whole system in a particular environment. Evaluated products can benefit the process of accrediting a system in its environment, but it is never correct to state that a *product* is "accredited," only that a product is part of an accredited system. All government agencies and divisions implementing cross-domain solutions are required to complete the C&A process before a system can be made operational.

IBM and Red Hat were the first to receive NIAP CCEVS at EAL4+ approval for a Linux distribution, Red Hat Enterprise Linux 5. Red Hat Enterprise Linux 5 on IBM systems now meets government security standards for assured information sharing within and across government agencies. It is anticipated that this globally recognized achievement will further drive the adoption of Linux among businesses and governments worldwide. No mainstream operating system in the world offers a higher level of security certification.

TCS' Trusted Thin Client solution has an ATO at the TSABI level, granted by the Accrediting Authority for the JWICS. In use today, the accredited system is part of the Coast Guard Intelligence Program (CGIP) designed to provide access to the top secret JWICS and SIPRNET classified networks from a single desktop. Trusted Thin Client is in evaluation at the Coast Guard for Secret And Below Interoperability (SABI).

### ***TSABI Details***

TSABI certification is easier to obtain than SABI certification, and government agencies do not have to achieve an ATO for one before doing the other. Many agencies tackle a single-level (versus multilevel) implementation as a starting point when their organization needs access to a single secure domain, with an eye toward multiple domain access in their future.

With this type of arrangement, IT managers can build from a secure foundation rather than try to construct everything at once.

## **CONCLUSION**

Clearly, protected information sharing is a way to achieve results when national security is on the line. The intelligence community, Defense Department, and various first responders need timely access to relevant information no matter what platform it's on. This means that they must deploy specific technologies. The alliance of TCS, Red Hat, and IBM offers a trusted Linux operating system, running cross-domain applications, that answers these challenges.

Sharing data between agencies is vital for national security. When the need to protect and share multiple levels of classified data is added to the mix, the need for secure cross-domain systems becomes paramount. The trusted Linux operating system from the TCS, Red Hat, and IBM alliance not only has NSA approval as a platform for meeting these challenges but also is the most actively evolving solution in this market.

Agencies with a need for such a solution are encouraged to investigate this platform not only from a performance standpoint but also as a solution that has the potential to be significantly less expensive than other alternatives.

---

### **Copyright Notice**

Copyright 2008 Government Insights, an IDC company. Reproduction without written permission is completely forbidden. External Publication of Government Insights Information and Data: Any Government Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Government Insights Vice President. A draft of the proposed document should accompany any such request. Government Insights reserves the right to deny approval of external usage for any reason.