

TRUSTED INFORMATION INFRASTRUCTURE (TII)

THE CHALLENGE

The Department of Defense (DoD) currently has many redundant network environments in place to support and maintain classified information. Each of these environments requires a separate facility, security and technical support staff, hardware, and software, as well as separate accreditations despite the fact that they process the same information. These redundant environments are operated at a Protection Level (PL) one or two, with all users of the systems having access to all data. CSCI recognized the glaring deficiencies of this setup, and set out to develop a PL3 environment that would reduce the number of redundant infrastructures and support personnel required to maintain them, while facilitating the secure sharing of information between segregated agencies and departments and providing robust auditing capabilities.

THE STRATEGY

In 1995, CSCI began the process of gathering requirements for what would come to be called Trusted Information Infrastructure™ (TII™). By interviewing potential customers, such as infrastructure personnel and professionals in the fields of security and information assurance, CSCI was able to identify their various needs and the factors that make for an optimum operational environment.

CSCI mapped approximately 1,500 operational requirements from these prospective clients, as well as nearly 600 security requirements from DoD directives, the Director of Central Intelligence Directive (DCID) 6/3, and Common Criteria 2.0. CSCI then spent two years designing the architecture for TII and analyzing commercial off-the-shelf (COTS) products to be used within the infrastructure.

With the architecture complete and the COTS products selected, CSCI commenced the actual development of TII. Prospective clients were brought in during this effort to demonstrate current and assess future capabilities. In addition, CSCI worked with DoD accreditors to gain a no-waiver, PL3 accreditation utilizing all COTS products, and presented the documentation in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

THE RESULTS

CSCI's TII uses PrOMIS™ as its compartmented data repository and collaborative workflow solution to achieve the goal of securely sharing information across an enterprise while fully taking advantage of current organizational assets. All data movement consists of electronic processes, whereby appropriately cleared, data-knowledgeable personnel approve the information-sharing release and security personnel allow the compartmented transfer of information. This greatly reduces the overhead associated with sharing data on isolated, redundant systems.

In TII, CSCI has designed a PL3 solution that meets all of the federal and DoD standards and regulations for IT systems operating in a classified environment, and which utilizes the Microsoft® Windows® platform used by many federal organizations. As such, those organizations, along with the many other businesses using Windows, do not have to overhaul their entire infrastructure in order to take advantage of TII capabilities, nor incur the costs of retraining personnel on how to operate a new platform.

As the activities of a classified IT system must be audited on a weekly basis, TII is designed with a centralized audit reduction tool capability to lower the manpower necessary to satisfy the requirement. Utilizing one central location for all security audit logs, TII reduces the amount of time security personnel must dedicate to reviewing them. These centralized audit logs can also be easily searched, thus meeting the requirement for audit reduction and reducing the weekly audit requirements from 32 hours to as little as 2.

TII utilizes fully automated tools like Enterprise Management and Software Delivery that reduce the demands of maintenance and administration of a complex environment.

CSCI's TII solution addresses the problem of the mishandling and misuse of information that many organizations face. It does this by taking a "least privileged" approach, whereby individuals have access to data strictly on a need-to-know basis, while simultaneously fostering collaboration within the compartmentalized environment. Processes are simplified, time is saved, and valuable information is secured.

Copyright © 2006 Computer Systems Center Incorporated (CSCI™) – All rights reserved.
6225 Brandon Avenue, Suite 520, Springfield, VA 22150-2519.

CSCI™ is a trademark of Computer Systems Center Incorporated. Microsoft® is a registered trademark of Microsoft Corporation. All other trademarks and registered trademarks are owned by their respective companies.