



Cardinal Environment™

THE CHALLENGE

The United States Department of Defense (DoD) currently has thousands of network environments in place to support processing of classified information at varying levels of classification. 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 similar or related information.

These environments are operated at a Protection Level (PL) one or two, with all users of the systems being briefed and thus having access to all data. CSCI recognized the glaring inefficiencies of this multiple network configuration and set out to develop a robust PL3 environment. A single PL3 environment can collapse the number of 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

CSCI mapped approximately 1,500 operational requirements from 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. From those requirements, CSCI spent several years designing the architecture and engineering the solution.

During the engineering process, prospective clients were brought in to demonstrate current capabilities and advise on future direction. In addition, CSCI worked with DoD accreditors to gain a no-waiver accreditation utilizing all commercial off-the-shelf (COTS) products, and presented the documentation in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

To support the continued development of the environment, the component COTS products are regularly reviewed in order to upgrade the system and improve its capabilities by utilizing

the latest technologies, while ensuring the overall stability is never compromised.

THE RESULTS

Cardinal Environment™ is a fully accredited no-waiver PL3 system using the familiar Microsoft® Windows® platform.

The Environment is Collaborative

Cardinal Environment utilizes CSCI's Cardinal Collaborate™ product as its compartmented document repository and workflow solution to achieve the goal of securely sharing information across the enterprise. All data movement occurs by way 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.**

The Environment is Secure

Because the activities of a classified IT system must be audited on a weekly basis, Cardinal Environment is designed with a centralized audit reduction tool capability. These logs can be easily queried and filtered, providing the appropriate Information Assurance staff the data required to perform their job. Using CSCI's proprietary audit-flagging algorithm, **the number of audits required for review on a regular basis is reduced by over 80%.**

Users also have the ability to secure devices and applications. Removable drive access can be denied and audited, and unapproved applications can be restricted from execution.

The Environment is Managed

Best practices recommend and government regulations demand effective and consistent Configuration Management. Cardinal Environment implements several tools to manage the deployment of software, to inventory hardware, and to remotely control machines. **These systems management tools meet CM requirements while enhancing the productivity of the system administrator, thereby reducing the total cost of ownership.**