



## Cardinal ID™

### THE CHALLENGE

CSCI was challenged to create a multi-user product to track personnel accesses and billets, documents, programs, facilities, and organizations, and that provides organizational reporting and management functions within a secure, compartmented environment. The product would allow CSCI to produce accurate results for inquiries made by government security staff and action officers. While the need for these capabilities was immediate, no formal requirements had been established.

### THE STRATEGY

To meet this challenge, CSCI's strategy was to gather the requirements, map them to specific customer needs, formally document the requirements, and then implement a spiral development process to build the final product. CSCI collected requirements through an exhaustive process of assessing the relevant policies, then reviewed and mapped features and deficiencies of the legacy management processes and prototyped a "requirements gathering tool" before beginning the actual development process. The result of this rigorous analysis and the seven year development effort that followed was the creation of Cardinal ID™.

The initial release of Cardinal ID (originally named SARMIS™) was built in an easily-modifiable relational database package and used for iterative requirements gathering and field testing. As the requirements evolved and matured, CSCI implemented the next spiral in the development process and moved to a more structured, controlled database package to better support the multi-user, multi-agency requirements. The current spiral development effort has produced a multi-user product specifically designed to fully compartment access to all database information, ensuring that only the right person, in the right place and with the right privileges, can access the data.

Throughout the development life-cycle, CSCI has fostered interaction between the various disciplines to provide the best solution to meet our customers' needs. By beginning at the requirements-gathering level, CSCI was able to make informed, detail-oriented decisions about

security, computer, and management needs. Experts with various specialties were brought together to balance the competing interests of security, information assurance, software architecture, quality assurance, and operator usability. This cross-functional team continues to meet regularly to address development issues associated with the prioritization of new features and modules.

A critical area of excellence within Cardinal has been to break the development effort into modules so that capabilities can be delivered more efficiently. This approach has allowed CSCI to more easily add features that fully integrate with the product's existing capabilities. These development decisions result in a uniquely capable security management suite of services that is not commercially available from any other source.

### THE RESULTS

CSCI has provided its customers with the ability to ensure the right information is provided to the right people in a timely, secure manner. The role-based, compartmented access offered by Cardinal ID allows customers to tailor access requirements for sensitive information. Within this secure environment, users are provided the capability to view and manage the data required to perform their unique jobs, thus reducing the need for centrally located security personnel at each work site.

Cardinal ID enables CSCI's customers to electronically store program access-related paperwork and to track and manage personnel security reviews. This has streamlined the process of coordinating program accesses, reduced the processing time from days to minutes, and, at one customer's location, allowed for the removal of a five-drawer safe previously used to store the abundance of maintained documentation. With Cardinal ID, CSCI has operationally replaced multiple software products with an integrated, multi-user solution that fully addresses customers' security management needs, improves data standardization and commonality, and that is able to integrate with existing legacy security management tools and data.