

## CTA INFORMATION SECURITY CASE STUDY:

### SECURING DISASTER RECOVERY MOBILE COMMAND CENTERS

#### CLIENT DESCRIPTION:

Our client is the major contractor responsible for engineering services support for a mobile command center program for a major government agency.

#### CTA PROJECT DESCRIPTION:.

Provide system engineering, security engineering, system security certification and accreditation, and test support. Develop system security requirements, coordinate with certification and accreditation authorities, and provide security documentation including System Security Authorization Agreements (SSAA) in accordance with DoD and Delegated Approval Authority (DAA) guidelines. Plan, prepare, and perform security test and evaluation (ST&E) on system components, prepare test reports and risk assessments in accordance with test results and operational security requirements.

#### PROJECT REQUIREMENTS:

The focus of the security support to the program is to:

- identify, define, and clarify security requirements for mobile automated information systems;
- evaluate proposed architectures and system designs for satisfying security requirements;
- perform system security documentation, track requirements implementation, perform security tests and evaluations on implemented systems, and report evaluation results and asset risks;
- maintain the status of each operational site system security actions and activities.

The security support objective is to provide required security engineering and accreditation measures for the development, integration and implementation of new or upgraded mobile information systems. Additionally, certification and accreditation support is provided to the operation and maintenance units for the continued secure operation of implemented information systems.

#### SYSTEM ARCHITECTURE:

The program platforms represent the ground-mobile implementation of military command and control capabilities. The architecture employs an infrastructure for secure processing and communications at three distinct and separate classification levels. The multi-domain secure infrastructure provides for a single ATM backbone network with IP switches and routers for each classified local area network. Processors and workstations conform to client-server models with tailored interfaces for communications systems for landline, military satellite, and classified wide area networks. Voice, video, and data are carried across the same infrastructure. Sun Solaris servers and Windows NT servers and workstations predominate.

#### WORK ACCOMPLISHED:

Major CTA achievements are identified below:

##### **System Security Engineering**

CTA developed and defined security requirements for new and upgraded program information systems including an advanced messaging system, the multi-domain secure infrastructure, and upgraded operating systems for mission processors. Proposed systems, or products, and implementation

architectures were evaluated for security requirements satisfaction and inputs provided to adjust designs for identified deficiencies. CTA participated in Preliminary and Critical Design Reviews for the Data Distribution System presenting security certification and accreditation steps, test and evaluation plans, and documentation requirements.

### **System Security Certification and Accreditation**

CTA performed numerous successful C&A processes for individual information systems and lead the effort for initial accreditation of the multi-domain secure Data Distribution System. Efforts included detail security requirements development, documentation, and tracking; documentation of system implementation and integration architecture in DoD formats; coordination with both C&A approval authorities and unit level Information System Security Managers; and preparation and conduct of ST&E. CTA additionally prepared test reports and performed risk assessments fully documenting the findings. In conjunction with these C&A processes, CTA prepared system configuration standards for Solaris and Windows NT systems, assisted in implementing these standards and performed verification activities as part of ST&E.

### **BENEFITS TO CLIENT:**

Benefits to the customer include continued maintenance of the program platform accreditation posture through systems development and numerous upgrades and modifications. We have provided certified professionals familiar with the program environment, familiar with accreditation requirements for differing classifications and DAAs, and who know where to go for the most current security issues and information required to support mission critical decisions thereby helping the client focus his efforts to the mission objective: the development of a secure, effective command center capable of resuming services of our critical military systems in the event of a effective physical or cyber attack on our primary resources.