

CASE STUDY:

SECURING AND ACCREDITING FINANCIAL MANAGEMENT SYSTEMS

CLIENT DESCRIPTION:

The Defense Finance and Accounting Service (DFAS) has management responsibility for the finance and accounting functions of United States Department of Defense (DoD) organizations. In the course of fulfilling its mission, DFAS has embarked on a program of modernization to improve finance and accounting services for its customers and reduce costs by standardizing and improving procedures and systems, streamlining operations, and eliminating redundancies. Under the direction, authority and operational control of its Director, DFAS is responsible for the performance of the following major functions:

- Providing accounting and reporting services for all levels of DoD management for appropriated, non-appropriated, revolving, and trust funds; paying military members and collecting and disbursing DoD funds, including contract, vendor, security assistance, transportation and travel payments.
- Providing guidance and technical assistance to DoD financial networks around the world.
- Designing, developing, testing, implementing, operating, and maintaining financial systems.

CTA has a long-standing association with DFAS, starting in 1995 as one of its first security contractors. We assisted in training many of the senior security personnel now at the centralized sites and developed certification and accreditation procedures which have been formalized in the DFAS Regulation 8000.1-R. Additionally we have completed security risk management services for many DFAS applications and network infrastructures. For example, CTA led the effort in securing the Enterprise Local Area Network (ELAN) architecture. During the risk assessment of the ELAN, many serious deficiencies were found and remediated based on recommendations of the CTA security engineers. We performed independent network product evaluations for ELAN in our Security Assessment and Monitoring Operations Center. The first complete testing of the security for the ELAN was accomplished by CTA. Penetration testing and policy compliance assessments were included in the certification and accreditation package that was accepted by DFAS HQ. Based on the findings put forth in that package, the ELAN was accredited for operational use.

There are two major DFAS Automated Information Systems (AIS): the Defense Standard Disbursing System (DSDS) and the Defense Cash Accountability System (DCAS). DSDS is the standard DFAS AIS software tool to support disbursing, collecting, processing, recording and reporting for all Services. As a DFAS Corporate Information Infrastructure (DCII) Type III system, DSDS establishes and maintains a permanent interface with the DFAS Corporate Database (DCD). The Enterprise Local Area Network (ELAN) provides connectivity between the user workstations and the network interface to the Defense Information Systems Agency (DISA)-owned and operated Wide Area Network (WAN). (As indicated above, CTA performed a vulnerability assessment and C&A support for the ELAN system. See ELAN Network Security Assessment Case Study.) Through this interface, disbursing personnel interact with existing Entitlement, Accounting and Treasury Reporting systems to provide disbursing capability for DSDS agents and departments.

DSDS resolves past disbursing deficiencies through the introduction of a single standard DFAS AIS for collecting, processing, recording, and reporting disbursement data and transactions and enhances disbursing capability by replacing the current mainframe environment with an open systems environment (OSE) compatible with the DFAS Target Architecture (TA).

The DCAS is a migratory system developed to reengineer and consolidate the interim migratory systems that the Department of Defense Services and Agencies use for cash accountability and reporting for General Fund, Defense Capital Working Fund, and Security Assistance.

DCAS will provide a single Department of Defense-wide cash accountability system that consolidates, standardizes, simplifies, and improves automated support for all DFAS Centers. DCAS will replace the many systems throughout the DoD that currently support this business function.

DCAS will be deployed at DFAS Centralized Sites, DFAS Field Offices, disbursing stations, entitlement stations, and accounting stations located throughout the United States.

When deployed, DCAS will perform general activities that are common for any accounting process and will be capable of:

- a. automating manual processes,
- b. processing electronic input and update/correct data from a single source on a daily basis,
- c. provide a shared data base environment, to include global reference tables,
- d. provide a standardized global edit process,
- e. eliminate cash accountability legacy and interim migratory AISs,
- f. provide full documentation, available on-line, and
- g. utilize advanced technology, including open system features and compliance with DoD standards.

CTA SECURITY ENGINEERING PROJECT DESCRIPTION:

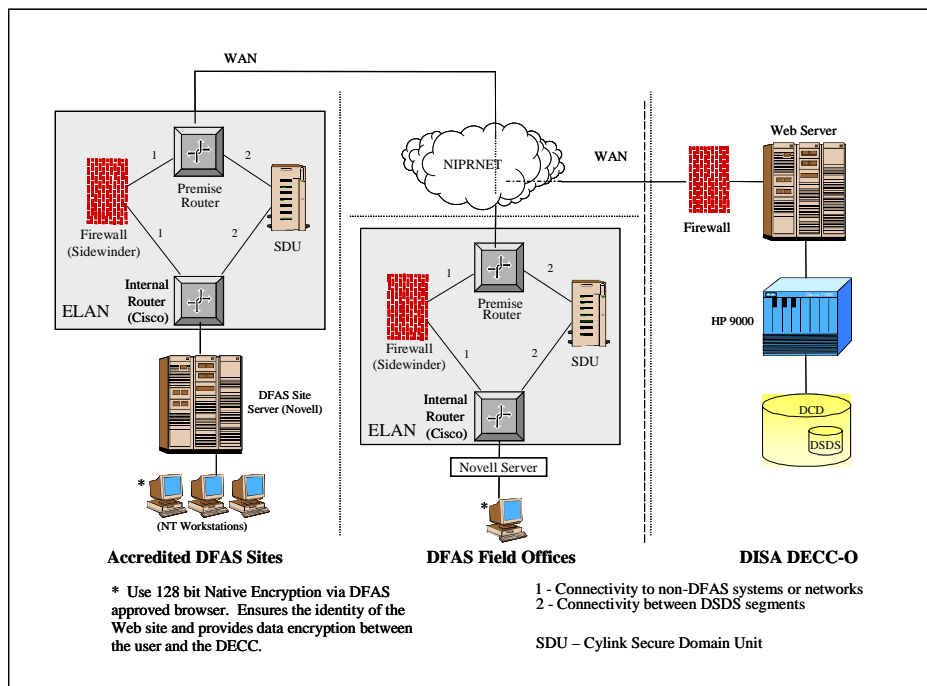
CTA is providing on-going security support during the development life-cycle of DSDS and DCAS, to include security requirements definition, vulnerability assessments, risk assessments, and preparation of documentation leading to approval to operate based on the System Security Authorization Agreement (SSAA).

Defined as "major AIS," DSDS and DCAS will be required to have the certification and accreditation (C&A) processes performed to ensure these systems meets security requirements delineated in "Security Requirements of Automated Information Systems" (DoDD 5200.28) and "DFAS Automated Information Security Policy" (DFAS 8000.1-R).

The certification and accreditation of these DFAS systems is supported by CTA vulnerability analysis and CTA-compiled security documentation identified in the DFAS Certification & Accreditation Handbook and the DoD Information Technology (IT) Security Certification and Accreditation Process (DoDI 5200.40).

SYSTEM ARCHITECTURE:

The figure above defines the operating environment and provides a high level view of the security implemented.



WORK ACCOMPLISHED:

CTA performed the initial site certifications for DFAS centralized sites, including the Pensacola field office. We have hosted seminars and conferences for the DFAS Information Security Officers (ISO), both at our facility in Colorado Springs and at numerous DFAS locations.

CTA is currently providing security engineering and accreditation services in support of two major DFAS Automated Information Systems (AIS): the Defense Standard Disbursing System (DSDS) and the Defense Cash Accountability System (DCAS). Our role includes performing security risk assessments of potential solutions to system requirements, producing security requirements and assisting in integrating their compliance into the development process, developing security procedures and practices to support the system, security awareness and education training for users and support personnel, and risk assessment of the project as it is developed through its phases.

CTA was asked to become involved in the development of the DFAS applications by reviewing the system security requirements. This early involvement during the design phase helped identify areas of risk and helped the PMO make necessary engineering changes directed at ensuring later compliance with applicable DFAS and DoD security policy and directives. Over the last few years, CTA has supported the security engineering and accreditation requirements for the following DFAS programs:

CMSS	Crisis Management Support System
DCPS	Defense Civilian Pay System
DDRS	Defense Departmental Reporting System
DIFS	Defense Integrated Financial System
DRAS-APS	Defense Retiree Annuitant Pay System
DTRS	Defense Transportation Payment System
EDM	Electronic Document Management System
ELAN	Enterprise Local Area Network
EMSS	Employee/Member Self Service
IAPS	Integrated Accounts Payable System
IPC	Integrated Paying and Collecting System
RADSS	Resource Analysis Decision Support System
SMAS	Standard Material Accounting System

In addition CTA has performed site certifications for all centralized DFAS sites and developed the DFAS Certification and Accreditation Handbook.

In support of its work for DFAS, CTA participates in technical conferences involving Public Key Infrastructure (PKI), the annual DISA Defense Enterprise Computing Conference in Park City, UT, and worked with various DISA representatives to obtain necessary information needed to ensure the DFAS C&A submissions are as comprehensive and accurate as possible.

BENEFITS TO CLIENT:

The benefits to the customer were numerous. CTA has provided a broad range of security services and technical support to the PMO. This support includes assisting the PMO in understanding critical security requirements and assessing the risk posture of the proposed architecture.

CTA has also served as a watchdog over the program and tried to provide early warnings of possible technical and programmatic risk that may impact the C&A process.