DECISION SOFTWARE SYSTEMS, INC.®

Cyber Security Engineering Capabilities

In a prior subcontract, supported systems engineering for the JSF F-22 encryptors program. The effort included analysis of the development of the Theory of Equipment Operations (TEO), Fail Safe Design Analysis Report (FSDAR) to meet the vendor's Unified Information Criteria (UIC) requirements for a High Assurance data communications system. Tasking analysis included review of Crypto Ignition compatible pre-placed management keys during startup and upset clearance processing.

Additional efforts entailed using technical analysis of data communications traffic transmitted and received via the encoder(s) interfacing with the AEHF, MILSTAR and GPS satellite communications systems.

In the area of AEHF extensive efforts entailed TEO,FSDAR, UIC analysis of the satellite encoding payload ASICS. The effort incorporated Global Information Grid (GIG) communications to support Asynchronous Transfer Mode (ATM) communications messaging into large secure payload data frames.

In a subcontract for Global Positioning System (Block IIR/III) supported satellite navigation payload systems/software engineering the control channel uplink and downlink message commands. Part of the effort was to resolve the multi-vendor GPS PIRNS to assure compliance of the command message formats accuracy per edition of planned communications updates.

On GPS Block III supported key management import operations for the GPS satellite payload into the internal key management database(s). Here also supported ground based communications message processing to the GPS satellite constellation.

In addition, worked on the Systems Operations Center (SOC) High Assurance Electronic Key Management System(s) (EKMS) Cryptograhic key distribution network. Extensive work with the Local Management Device (LMD) /Key Processor (KP), Data Transfer Device (DTD), End Cryptographic Units (ECUs) and ASN.1 messaging. Worked with the Central Facility (CF) Simulator to generate EKMS Standard Key Material. The CF Key data was then imported into the Central Automated Key Management System (CAKMS) for subsequent processing (An array of LMD/KPs). The CAKMS key material is then imported into a Local Area Key Management System (LAKMS) for further processing. The LAKMS output is then imported to a single LMD/KP and the output is transferred to a Data Transfer Device (DTD). The DTD is then transported to the designated End User Cryptographic Unit(s) (ECU) and the key material is installed into these devices.

Here also supported Cryptographic Verification and development of Testing procedures for approval by the vendor(s).

In a recent project, supported Risk Management Framework (RMF) (NIST SP-800-39 etc) Cyber Security Mitigation. Tasks involved identification and installation of security critical patches for the computing systems (Windows Servers 2008/2012 and Sun Servers) in the network. Introduced to the Patching efforts utilization of the Microsoft Windows Update Services (WSUS) to automate server network patching. Performed analysis for Common Off the Shelf (COTS) periodic security critical and/or comprehensive vendor patching within the designated patch cycle. Patches were applied to both operating systems and applications.

Reviewed Defense Information Systems Agency (DISA), Security Technical Information Guides (STIGs) guidelines and properly configured systems for applicable STIG requirements. Built compliance matrices and support Plan of Action and Mitigation (POAM) on issues identified for Authorization to Operation (ATO). Worked on RMF areas building compliance matrices for identification of program weakness with respect to RMF compliance. (eg. Disaster Recovery, Risk Management Policies and Procedures etc). Here also worked on Window Servers Group Policies used to control access to the AEHF data based on user and data access rights. The policies are enforced by utilization of Active Directory (AD) standards.

Here also supported systems/software engineering and analysis of frequency permutation satellite communications to optimize usage of channel communications usage based on planned usage schedules. The system utilize counter mode communications between the satellite constellation and the end user communications platforms