IT Program Assessment
NPPD – National Cybersecurity Protection System (NCPS)

Review

The DHS CIO conducted a comprehensive program review of the NPPD – National Cybersecurity Protection System (NCPS) program during September 2011. Program observations include the following:

DHS's National Cyber Security Division's National Cyber Security Protection System (NCPS) was developed and implemented to protect the Nation's cyber infrastructure by serving as a focal point for cyber activity and response across the Federal Government. NCPS is a fully integrated, end-to-end system comprising the hardware, software, and other components being procured to support the mission. NCPS is following an incremental system development approach by developing and releasing capabilities in "blocks." They have successfully released Blocks 2.0 (which will be deployed to additional sites) and 2.1 and are developing Blocks 2.2 and 3.0.

The program has had many accomplishments since the FY10 program review including: entering into an interagency agreement to move into detailed design supporting Block 3.0's Initial Operation Capability (IOC); and NCPS received ARB ADE-2B (Acquisition Review Board/Acquisition Decision Event) approval, which provided the authority to award NCPS Block 3.0 contracts. The program rebaselined its Acquisition Program Baseline (APB) for a second time, during FY11 due to delays in Operational Testing and Evaluation of Block 2.1. This APB was approved in an Acquisition Decision Memorandum dated May 5, 2011.

The program faces several risks:

- A Continuing Resolution (C/R) for the FY12 budget with reduced funding for the program. If the PBR for FY12 is not approved, and instead, the NCPS is required to operate under a C/R that funds the program at FY11 enacted amounts, there will be an immediate need to restructure program priorities. This will likely result in a significant reduction of capabilities in all Blocks, most significantly in the development activities of Block 2.x and Block 3.0, and support service contracts.

- If the ISPs do not modify their Service Level Agreements with the Departments and Agencies (D/As) in the Block 3.0 deployment, delays on renegotiations may directly affect the timeline for aggregating traffic and introducing live traffic to Spiral 2 technology.

- If the timeframe required for solidifying requirements for Top Secret/Sensitive Compartment Information Mission Operating Environment (TS/SCI MOE) operations and connectivity exceeds the required schedule threshold, the program schedule will be negatively affected and IOC may be delayed.

Assessment

The program is actively addressing previous concerns and has done a good job identifying risks. Mitigation strategies are in place and they seem to be well positioned to act should the risk arise. The program has the support of NPPD’s upper management who is participating in the risk mitigation by securing funding for the program. The NCPS program should continue along the path they have set for themselves and continue to evolve and mature their program management practices. The CIO assesses the NPPD NCPS program as a Level 4 - Moderately Low Risk.

Score: 4