IT Program Assessment
DHS – Homeland Secure Data Network (HSDN)

Review

The DHS CIO conducted a comprehensive program review of the DHS Homeland Secure Data Network (HSDN) program during September 2011. Program observations include the following:

HSDN is in the operations and maintenance (O&M) phase of its life cycle. It has been deployed to 321 sites across the United States including multiple Fusion Centers and Urban Area Security Initiative sites. HSDN sites comprise over 3,000 workstations and support nearly 7,000 users. HSDN currently operates system-wide capabilities on a 24/7 basis. These capabilities comprise the network operations center, security operations center, four-tiered helpdesk, and system-wide telecommunications infrastructure. HSDN completed an infrastructure upgrade of the Secure Video Teleconference (SVTC) bridge enabling automated access and increased participation to classified SVTC. Over 100 video conferences may be handled simultaneously. HSDN has expanded service to federal Homeland Security mission partners and in support of Continuity of Operations/Continuity of Government plan (COOP/COG). HSDN service is further expanding to Housing and Urban Development (HUD), Health and Human Services (HHS), Federal Aviation Administration (FAA), Patent and Trademark Office (PTO), U.S. Senate Sergeant at Arms, National Nuclear Security Administration (Department of Energy), Commodities Futures Trading Commission, Small Business Administration Board of Governors for the Federal Reserve System. HSDN is operational at both DHS Data Center-1 (DC1) and DC2.

This program success has brought with it commensurate challenges and risks, including:

- Demand for the system (~1000 total sites by 2013) is greater than initial projections, therefore:
    - Projected program funding may be insufficient to support projected customer growth and emerging operational requirements
    - The network may not be able to handle the growth (scalability and extensibility needs)
- The ability to deploy HSDN is totally dependent on the customer’s ability to complete site build out and accreditation

Mitigation Strategy

The HSDN program has mitigation strategies in place to include:

- Seeking additional appropriated funds and exploring other internal and external funding sources (e.g., Working Capital Fund)
- Updating the HSDN Requirements baseline and defining an FY13 – FY17 Target Architecture to support the projected growth and the emerging operational needs of the user base
- Working with the National Security Systems (NSS) Joint Program Management Office (JPMO) to establish requirements, develop an implementation plan, and monitor site installation and accreditation progress throughout the entire process
- Developing a process to vet enterprise requirements through the Information Sharing Governance Board (ISGB) on overall information sharing approaches for DHS. This will be integrated into the overall ISGB governance model for networks.

Assessment

The HSDN program is a well-managed O&M effort and, as so often happens, its success has bred an increased demand for its service. While this is beneficial it brings with it the need to modify program plans and execution supported by the decision makers of the Department. The HSDN program has sound mitigation strategies in place but as it proceeds with re-planning and programming, it will continue to be closely monitored to ensure continued success. The CIO assesses the DHS HSDN program as Level 3 – Medium Risk.

Score: 3