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

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) conducted a program health assessment of the DHS Homeland Secure Data Network (HSDN) program. This assessment represents the program's status through March 2012.

Description and Background:

The Homeland Secure Data Network (HSDN) enables classified information to reach federal agencies that are involved in homeland security missions. HSDN is a classified wide-area network utilized by DHS, DHS Components and other partners, providing effective interconnections to the intelligence community and federal law enforcement resources. HSDN provides DHS the ability to collect, disseminate, and exchange both tactical and strategic intelligence and other homeland security information up to the SECRET level. HSDN also serves as a consolidated backbone that brings together multiple, legacy SECRET-level classified networks across the DHS enterprise. HSDN became fully operational in FY2004 and is currently in the operations and maintenance (O&M) phase of the system life cycle. It is deployed in support of the Homeland Security Act of 2002, Intelligence Reform and Terrorism Prevention Act of 2004, the Presidents National Strategy for Homeland Security, the 9/11 Commission Act of 2007, National Communication System Directive 3-10, and other national mandates to provide a comprehensive IT network architecture for federal, state and local governments to share and collaborate with timely and actionable classified information for Intelligence, Counter Terrorism, Counter Narcotics, Immigration Enforcement, Infrastructure Protection, and Emergency Preparedness and Response missions. HSDN services include full-service network operations, collaboration tools, enterprise applications, and common workstation configurations. Additionally, HSDN provides both primary and backup network operations and security operations centers, data centers and help desk, and is operating out of the DHS Enterprise Data Centers (DC1 and DC2).

Risks and Issues:

The following risks were identified for the DHS HSDN program:

- Remediation of the Wikileaks security issue and other mandated security upgrades may require diverting appropriated funds from planned network enhancements, operations and maintenance.

- 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 program has mitigation strategies in place to address the identified risks and improve the health of the program.

- 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 DHS Homeland Secure Data Network (HSDN) program is a well-managed program in the operations and maintenance lifecycle. As a result, the program's success has bred an increased demand for its service. While this is beneficial, the current projected funding amount for the program may be insufficient to support the emerging demand. The program has sound mitigation strategies in place, but as it proceeds with re-planning and programming, it will be closely monitored to ensure continued success. The program is on schedule to complete the enhancement and implementation of HSDN over broadband by Q4FY12. Additionally, the program is on schedule to complete installation of the State and Local Fusion Centers by Q2FY13. The CIO assesses the DHS HSDN program as **Medium Risk** investment.

Score: 3