![Homeland Security logo]

IT Program Assessment
Customs and Border Protection (CBP) – Infrastructure

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) conducted a program review of the Customs and Border Protection (CBP) – Infrastructure program. This assessment represents the program's status through March 2012.

Description and Background:

CBP – Infrastructure has been able to successfully sustain operations in 10 infrastructure project areas: Wireless, Voice, Video, Site Services, Data Center, Help Desk, Email, Network, Single Sign-On, and Desktop. The program intends to meet mounting capacity needs by successfully transitioning operations and maintenance (O&M) operating support, in parallel with completing vital systems modernization efforts. CBP – Infrastructure will relocate data center computing resources and services (O&M) to virtualized cloud computing platforms to simplify and eliminate configurations, reduce space requirements, and improve overall operating cost performance. The program will ensure end-to-end telecommunications networks connectivity and high availability by reducing single-points-of-failure, establishing continuous technology refresh of critical components, and assuring full alignment with the strategic objectives of CBP/Office of Information Technology (OIT) and key stakeholder. In addition, it will ensure O&M integrity and reliability to meet mission critical requirements day-to-day while reducing operational risk, satisfying increasing demands, and seamlessly transitioning to performance enhancing technologies.

Risks and Issues:

CBP – Infrastructure has shortfalls within its budget and is struggling to keep up with O&M systems costs. As a result of the budget reductions, CBP/OIT has trimmed investments to only highest priority programs and added operational risk, halted aggressive pursuit of modern low cost/high performance technologies, and stopped "best practices-driven" enhancements to streamline and add new capacities to current O&M operations. This will result in antiquated servers as well as an unfunded bandwidth, which may cause outages. In addition, the program has identified the following high risks:

- Funding for infrastructure has remained consistent for several years and has not taken into account the rising software and hardware costs. Without this additional funding, CBP's infrastructure will have a growing number of points of failure and will not have sufficient funds available for technology refresh.

- CBP Infrastructure is dependent on outdated technologies that are very expensive to maintain.

Mitigation Strategy:

CBP has strategic development programs underway to modernize its mission critical applications, its communications networks, its computing platforms, and its data center operations. This is intended to reposition CBP/OIT to continue to meet vital citizen

security services demands, reduce O&M costs, and provide DHS Component business units with more reliable, effective, and high-value shared IT infrastructure services. The program has also identified the following ways to mitigate the risks noted above:

- An independent review of the cost of IT and best business practices is being performed within the next 30-45 days. The CBP Commissioner and Deputy Commissioner will reconsider requests for end of year funds based on the results of this review.

- While CBP/OIT does not have the funding to completely overhaul older technologies, critical components are being evaluated for upgrade and modernized based on mission.

Assessment:

The Infrastructure program continues to meet the requirements of CBP users given the vast locations, users, and processing requirements of the CBP user community. However, the program needs to baseline mission-critical systems and resources, forecast the volume of future transactions, and institute measures to monitor ongoing demands. This will ensure adequate capacity to meet basic, mission-critical requirements to meet mounting capacity demands. It is also recommended that the program leverage resources across CBP OIT to expedite implementation of rapid applications modernization and preparation for target architecture implementation. Due to its risks and mitigation strategies, the CIO assesses the CBP – Infrastructure program as **Medium Risk**.

Score: 3