

IT Program Assessment NPPD - FPS Risk Assessment and Management Program (RAMP)

Review

The DHS CIO conducted a comprehensive program review of the NPPD FPS Risk Assessment and Management Program (RAMP) program in September 2011. Program observations include the following:

RAMP will be a next generation risk assessment tool used to assess and analyze risks posed to Federal facilities from crime, natural hazards, and terrorism. RAMP will replace the current proprietary tool, Federal Security Risk Manager (FSRM), as well as two modules within Federal Protection Service Information Tracking System (FPISTS), the Contract Employment Requirements Tracking System (CERTS), and the Security Tracking System (STS). RAMP shall be the primary system used by FPS to fulfill its strategic mission of securing federal facilities and ensuring occupant and visitor safety. RAMP will assist Federal Protective Services (FPS) Inspectors in producing Facility Security Assessments, performing data collection on Federal facilities and generate reports and other required documentation.

Data collections on federal facilities will be accomplished using specialized hand-held Mobile Computing Devices (MCDs), issued to approximately 800 Inspectors in all 11 FPS regions containing over 9000 facilities. The current RAMP production environment will be upgraded to incorporate ISC standards and will be titled RAMP 2G. Additional enhancements to RAMP 2G will be planned and developed in a phase approach in support of the OMB IT 25-Point plan to reform the federal government.

The following RAMP program risks exist:

- Currently there is no approved acquisition program baseline in place. An approved Operational Requirements Document (ORD) has never been in place for the RAMP program thus a requirement baseline has never been established in accordance with D-102.
- RAMP is currently using legacy equipment for developer testing of new software tools, due to delays in procurement for new hardware components. A high level risk exists due to the possibility of RAMP's legacy enterprise environment not being compatible with enterprise conditions needed for RAMP's new software tools. Delays in procurement for hardware components will also delay the infrastructure needed to perform specific developer testing, training and deployment of new software tools. If these schedule risks are not mitigated the RAMP infrastructure will not meet development and deployment requirements.
- An FPS inspector revealed that the RAMP IT system does not generate any usable assessment reports as planned. This is a high level risk to RAMP's program performance that impacts RAMP in not meeting FPS program requirements.
- RAMP's LCCE has grown from an initial estimate of \$15.9M in 2008 to \$183M in draft 2011 LCCE. RAMP's LCCE growth is attributable to poor initial estimates,

scope increases, reprioritization of capabilities, unplanned fixes to technical issues, and extended system lifespan. Significant scope creep occurred with RAMP for PSO management, countermeasures pricing index, facility information management, and geo-location information.

Mitigation Strategy

RAMP is currently relying on an Functional Requirements Document (FRD) to describe system functional requirements, plan the allocation to system releases and serve as the requirements baseline. The RAMP program manager is aware of current performance risk and has put a plan in place to better coordinate stakeholder communication and manage system development requirements. A plan for more frequent communication and coordination is in place between FPS, Infrastructure Protection (IP), Office of Procurement (OPO) and Department of Energy (DOE) to limit development delays. To ensure that RAMP is meeting Federal Protective Services (FPS) requirements continuous coordination between FPS and IP teams is being managed by the RAMP program manager. Also FPS Inspectors are included on the Modified Infrastructure Survey Tool (MIST) Integrated Project Team (IPT) and a RAMP program manager has been detailed from the region to lead requirements efforts. The DHS CIO has tasked NPPD to generate a report on specific capabilities to be delivered in each release going forward, with associated schedule and cost, so that a firm program baseline can be set. A RAMP Working Group has been established to engage stakeholders and identify user requirements and gather user feedback.

Assessment

The issues with RAMP present high level risk to the program's development schedule, life cycle cost and program performance. RAMP's management has put in place viable mitigation strategies to control risk and improve oversight. RAMP will continued to be monitored closely to see if proposed strategies demonstrate program improvement. The CIO assesses the NPPD FPS RAMP program as a Level 2 - Moderately High Risk.

Score: 2