

## **IT Program Assessment**

### **ICE - Criminal Alien Identification Initiatives (CAII)**

#### **Review**

The DHS CIO conducted a comprehensive program review of the ICE CAII program during September 2011. Program observations include the following:

The CAII program provides the ICE law enforcement community information technology tools that facilitate the identification of criminal aliens for removal from the U.S. in support of DHS Mission Area #2: Preventing Terrorism and Enhancing Security, and Removal of Individuals Posing a Security Threat. The program is on schedule and within budget. CAII has automated manual data processes to increase access to immigration and criminal data contained in federal systems; automated the processing of Immigration Alien Queries (IAQ) concerning high threat subjects; automated information sharing between Alien Criminal Response Information Management System (ACRIME) and other federal systems; and made improvements to CAII system interfaces. These improvements are decreasing law enforcement agencies response time to IAQs, providing an integrated data approach to Secure Communities and improving subject searches for criminal alien tracking programs. The following capability gaps and risks have been identified:

- CAII has process and performance gaps in the following areas:
  - Displaying a consolidated view of a criminal alien data, and productively using data provided by multiple U.S. government systems.
  - Prioritizing IAQ processing by integrating a threat assessment of each criminal alien.
  - Providing automated searches of disparate data sources, making full use of interoperability-provided biometric data that can eliminate the need for time-intensive manual searching and reviewing of the different systems.
- If Test and Evaluation resources are not prioritized according to CAII release schedule, there may be deployment delays.
- If data center migration schedule does not align with CAII project schedule, then there may be delays in deployment.
- If requirements gathering are not complete, then the CAII integrated schedule may be adversely impacted.

#### **Mitigation Strategy**

CAII Program Managers are actively implementing Agile methodologies to improve the software development process of the various projects. Milestones have been adjusted to meet the release requirements of the 25-Point IT Reform Plan by segmenting requirements into smaller, more manageable releases. To improve program

governance CAII interacts directly with the Secure Communities Business Owner at regular IPT meetings, where program efforts are reviewed and discussed. To support system test and evaluations (T&E), the CAII project manager is working to get contractors access to development systems so they can support T&E efforts. Meetings are scheduled with contractor and AHS to actively work on T&E issues.

CAII is working with the enterprise architecture to facilitate requirements discussions with the CAII working group and identify scheduling priorities within the ACRIME project. CAII program manager is also working with Engineering to identify options for deployment prior to scheduled data center migration activities for CAII.

### **Assessment**

CAII is currently in Post-ADE 2B with activities occurring in multiple stages of the ICE System Lifecycle Management (SLM). In the 2Q or FY 2011 Automated Threat Prioritization (ATP) successfully passed the critical design review milestone, and completed development and began testing in FY2011 Q4. ATP is scheduled to enter production in FY2011 Q4, and will be integrated with ACRIME in FY2012 Q2. Delays in the deployment of ACRIME caused related work on the SDS projects to cease. However, requirements definition and design work will recommence on the Data Information, Integrated Case Management and Automated National Crime Information Center (NCIC) Warrants services in FY2011 Q4 and FY2012 Q1. The CIO assesses the ICE CAII program as a Level-3—Medium Risk.

**Score: 3**