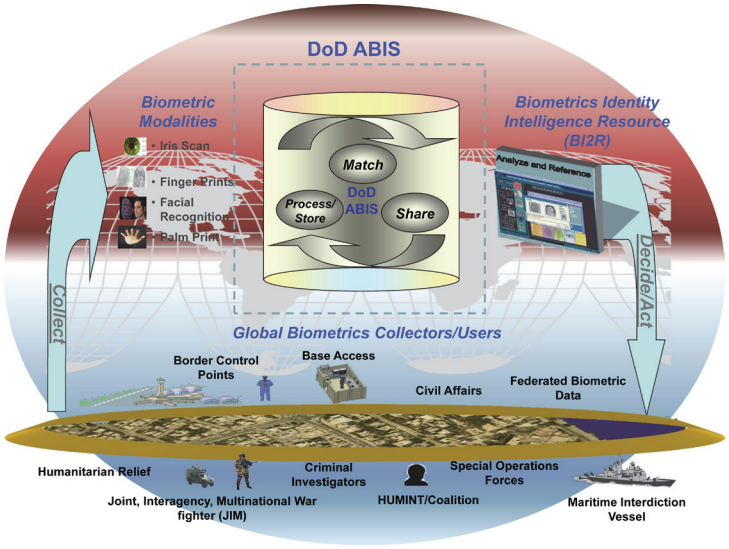
DOD Automated Biometric Identification System (ABIS)

Executive Summary

- The Program Manager Biometrics fielded the DOD Automated Biometric Identification System (ABIS) 1.0 to the Biometrics Identity Management Activity (BIMA) in January 2009 as a quick reaction capability to support storing, matching, and sharing of collected biometric data primarily obtained during Operation Iraqi Freedom and Operation Enduring Freedom.
- The Army chartered the Program Management Office (PMO) in 2007 to foster the establishment of ABIS as a formal program of record to be known as the Biometrics Enabling Capability (BEC) Increment 0.
- In January 2011, USD(AT&L) issued an Acquisition Decision Memorandum establishing ABIS 1.2 as the baseline for the BEC 0 upon completion of a Full Deployment Decision (originally scheduled for FY11).
- In October 2014, the PMO deployed ABIS 1.2 successfully and it remains the authoritative source for biometric transactions upon completion of the two-phased IOT&E that was conducted from August through October 2014.
- Prior to the IOT&E, the Army Test and Evaluation Command (ATEC) performed a customer test in February and March 2014. The test operated at multiple sites, with the primary site being the BIMA facility located in Clarksburg, West Virginia. The purpose of this test was to independently verify the system readiness of the DOD ABIS 1.2 system prior to an operational test. Upon completion of the customer tests, ATEC conducted a two-phased operational test, with Phase One held August 7 – 28, 2014, and Phase Two held October 17 – 22, 2014.
- An independent Red Team assessment in August 2014 revealed significant cybersecurity vulnerabilities that must be addressed. ATEC has planned a cybersecurity assessment to be held during the 2015 FOT&E to demonstrate resolution of critical cybersecurity findings.

System

- The DOD ABIS is an authoritative database that uses software applications to:
  - Process and store biometrics modalities (i.e., fingerprints, palm prints, iris scans, and facial recognition data) from collection assets across the globe
  - Update the biometric database repository with new biometrics data
  - Produce biometrics match results (against stored data)
  - Share responses among approved DOD, interagency, and multi-national partners, in accordance with applicable law and policy
  - Provide tools to monitor the health and status of the system



- For biometric submissions that are unable to produce a match using automated processes, biometric examiners (subject matter experts) use ABIS workstations with specialized software to attempt to manually match submissions.
- ABIS interfaces with global biometrics data collectors and users, as well as outside databases.
  - Military Services and Combatant Commands collect biometrics data (fingerprint, palm print, iris scans, and facial scans) from persons of interest in the field using portable collection devices and submit these data to ABIS.
  - Intelligence analysts analyze and fuse biometrics information via the Biometric Identity Intelligence Resources, an automated database outside the ABIS, and provide information back to the users in the field.
- ABIS 1.2 uses a set of commercial off-the-shelf and custom components including:
  - A transaction manager for managing customer submission workflows
  - A portal allowing authorized operators to perform user management, system configuration, real-time system monitoring, submission tracking, and report generation
- The U.S. Army BIMA currently operates ABIS on the DOD Non-secure Internet Protocol Router Network (NIPRNET).
- The PMO developed ABIS 1.2 as an enhancement to the previously fielded version, ABIS 1.0. The new system is intended to address hardware and software obsolescence and scalability limitations in ABIS 1.0, and increased throughput and storage capacity of biometric submissions and responses.

Mission

- Military Services and U.S. Combatant Commands rely on ABIS to provide timely, accurate, and complete responses indicating whether persons of interest encountered in the field have a prior history of derogatory (e.g. criminal) activity, to assist in identifying potential threats to U.S. forces and facilities.
- The Federal Bureau of Investigation, the National Ground Intelligence Center, Department of Homeland Security, and other Federal agencies interface with ABIS to identify biometrics matches in support of U.S. criminal cases, border control, and intelligence watchlists, respectively.

Major Contractor

Northrop Grumman, Information Technology (NGIT) – Fairmont, West Virginia

---

Activity

- ABIS was first developed as a prototype in 2004 in response to a Joint Urgent Operational Need Statement. ABIS 1.0 was deployed to BIMA in January 2009 as a prototype system to provide multi-modal and multifunctional biometric capabilities to assist in the Global War on Terrorism and subsequently in Overseas Contingency Operations.
- Since 2004, DOT&E designated all biometrics programs be placed on the T&E oversight list as pre-Major Automated Information Systems. As such, although not a formal program of record, ABIS is included on DOT&E oversight.
- In January 2011, USD(AT&L) issued an Acquisition Decision Memorandum establishing ABIS 1.2 as the baseline for BEC 0 upon completion of a Full Deployment Decision (originally scheduled for FY11).
- Between December 2012 and June 2013, the PMO conducted a number of customer (developmental) tests to determine if ABIS 1.2 enabled the operators to access the functions they needed to perform their duties and if the system would react with consistent, accurate, and useful reports, displays, or other responses.
- In August 2013, the PMO deployed ABIS 1.2 as the system of record directly supporting real-world operations for 10 days. During the August 2013 deployment, U.S. Special Operations Command (USSOCOM) documented 31 high-priority deficiencies and U.S. Central Command (USCENTCOM) documented 11 high-priority deficiencies that affected mission accomplishment due to deficiencies in the ABIS 1.2 baseline affecting the effectiveness and suitability of the system. Following the August 2013 deployment, senior-level user representatives from both USSOCOM and USCENTCOM issued memoranda requesting that formal operational testing be conducted on future ABIS upgrades prior to deploying the upgrades, to help prevent further deployments that negatively affect missions.
- In February and March 2014, ATEC performed a customer test. The test operated at multiple sites with the primary site being BIMA. The customer test used a variety of recorded data submissions that were modified to allow submission to operational handheld biometric devices and sample stored submissions selected or designed to cause the system to perform reviews and produce responses in accordance with the user cases related to the specific problems under test.
- ATEC performed a two-phased operational test on ABIS 1.2. The first phase of the operational test was conducted August 7 – 28, 2014. The second phase was conducted October 17 – 22, 2014. The lack of proper Program Office test planning resulted in a compressed operational test plan review and approval timeline. ATEC submitted the test plan for DOT&E approval on August 1, just six days prior to the planned test start date. To correct key test plan shortcomings, on August 5, 2014, DOT&E provided critical comments to ensure test adequacy. DOT&E formally approved ATEC's test plan on August 12, 2014, in time to support Phase 1 of the operational test, which the Army decided to begin on August 7. Due to the compressed timeline, Phase 1 of the operational test was allowed to proceed even though an adequate test plan to address Phase 2 had not been approved by DOT&E.
- The second phase of the test, which was supposed to begin directly following the first phase, was delayed to address problems discovered during the first phase of testing.

Assessment

- During the August 2013 deployment, testing revealed that the interfaces between the current 1.0 system and its customers are not fully defined and documented. Interfaces have been created and sustained on an ad-hoc basis by BIMA in support of mission needs. Documentation of the interfaces and services required by ABIS 1.2 has required close collaboration between operators and the system engineers responsible for the 1.0 and 1.2 systems. The Joint Interoperability Test Command is tasked with verification of interoperability of ABIS 1.2 and testing is scheduled to be conducted from November 3 – 14, 2014.
- During the ATEC customer test performed in February and March 2014, ABIS 1.2 operated throughout the period with no significant system disruptions. The customer test was conducted in a non-operational environment in which data submissions were made using previously recorded submission data whose flow can be controlled by the system under test. The system processed all of the submitted transactions and ingested all those transactions, satisfying the processing specifications. Although there were some initial problems with some configuration settings, the Watchdesk operators, who handle customer requests and monitor submissions and

responses, or system administrators were able to correct issues such as account and/or computer settings. In order to properly receive responses to submissions from the users, correct message templates are required. During the customer test, some discrepancies were noted in selected responses that required changes to certain message templates for the responses to be properly received as expected.

- During Phase 1 of the IOT&E, the following problems were observed:
  - Discrepancies between ABIS 1.0 and ABIS 1.2 watchlist hits. ABIS 1.0 and ABIS 1.2 were not fully consistent in identifying individuals on the watchlist. Correctly matching individuals to the watchlist is a critical ABIS function. Review of 107 watchlist hits during Phase 1 found 17 watchlist hit discrepancies. Further analysis of the discrepancies attributed the discrepancies to timing of ingestion of daily watchlists between DOD ABIS 1.2 and DOD ABIS 1.0 and differences between the contents of the daily watchlists.
  - Discrepancies in the number of identities contained in the Custom Biometrically Enabled Watchlists (BEWLs) generated by ABIS 1.0 and ABIS 1.2. Custom BEWLs are smaller subsets of the full set of identities contained in BEWL, which are used in the field to determine the course of action when a person of interest is detained. Custom BEWLs generated after Phase 1 were reviewed and all identities provided for the Custom BEWL were present.
  - Phase 1 also demonstrated ABIS 1.2 problems that (1) negatively affected successful completion of Latent and Biometric examination workflows, (2) prevented a significant amount of data sharing with the Federal Bureau of Investigation upon deployment, and (3) affected the ability of the Watchdesk and Examiners from effectively completing some tasks. During Phase 2, the software patches and changes in standard operating procedures resolved the problems noted in these areas during Phase 1.

Recommendations

- Status of Previous Recommendations. The PMO has not adequately addressed all of the previous recommendations. The PMO still needs to:
  1. Conduct a baseline assessment, to include the definition of external interfaces to the current system and customers.
  2. Institutionalize a formal standards conformance program, listing external systems that have been independently verified to be interoperable with the biometrics enterprise.
- FY14 Recommendation.
  1. The Army should resolve cybersecurity findings from the IOT&E Red Team assessment and complete an adversarial assessment of ABIS 1.2 during FOT&E.