Director, Operational Test and Evaluation

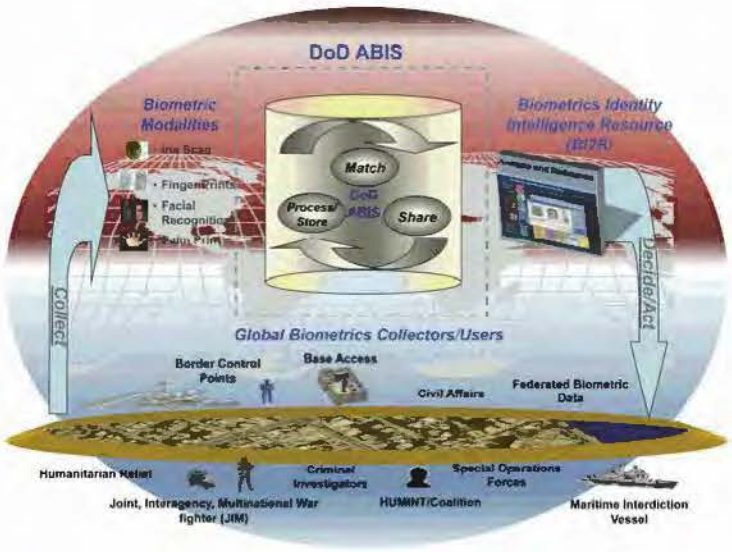
Department of Defense (DOD) Automated Biometric Identification System (ABIS) Version 1.2

Initial Operational Test and Evaluation Report

May 2015

This report on the Department of Defense (DOD) Automated Biometric Identification System (ABIS) Release 1.2 fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability of DOD ABIS.

J. Michael Gilmore
Director



Department of Defense (DOD) Automated Biometric Identification System (ABIS)

Executive Summary

This report provides the Director, Operational Test and Evaluation (DOT&E) assessment on the operational effectiveness, operational suitability, and cybersecurity of the Department of Defense (DOD) Automated Biometric Identification System (ABIS) version 1.2 (v1.2). This evaluation is based upon data from the Initial Operational Test and Evaluation (IOT&E) that the Army Test and Evaluation Command (ATEC) conducted in two phases in August and October 2014 at the Biometrics Identification Management Activity (BIMA) in Clarkshurg, West Virginia. ABIS v1.2 is operationally effective, not operationally suitable, and not survivable.

ABIS v1.2 is operationally effective. ABIS v1.2 successfully processed approximately 130,000 biometric and latent fingerprint submissions during the two-phase test.[1] The received and processed multi-modal biometric and latent submissions, stored in standardized formats, matched submissions against stored records, shared match responses in accordance with mission timeliness requirements while complying with national and international sharing agreements, and issued alerts whenever incoming submissions successfully matched against an identity on the DOD master watchlist.[2] A key improvement of ABIS v1.2 compared to the previously fielded version (ABIS version 1.0) is a reduction in the number of biometric submissions requiring review by specially trained examiner personnel, which is attributable to an enhanced matching algoritbm. However, improperly formatted responses affected biometric information sbaring with the Department of Homeland Security (DHS) and the United Kingdom.

ABIS v1.2 is not operationally suitable. The system experienced 17 essential function failures (EFFs) that required system administrator support during the test, leading to a mean time between essential function failure (MTBEFF) of only 39 hours. While there is no specified MTBEFF requirement, the prevalence of EFFs during tbe IOT&E substantively contributed to the assessment of not operationally suitable. Additionally, users in surveys expressed concerns in the areas of training, usability, and supportability, and immature help desk processes hindered the accurate accounting of trouble tickets and resolution times. ABIS v1.2 did not experience any system aborts or failures exceeding 15 minutes duration during the 27 days of record test in the IOT&E; hence, tbe system demonstrated its mean time between failures requirement of 1,140 hours with 44 percent statistical confidence.

ABIS v1.2 is not survivable against unsophisticated cyber threats. Cooperative vulnerability scans conducted from March 2014 to May 2014 discovered 102 unique Category I

---

[1] ABIS stores biometrics that includes fingerprints, irises, facial images, and palm prints. Latent fingerprints ("latents") are residual prints left on a surface that was touched by an individual. Latents can link individuals to criminal activities. Forensic labs collect and process latents and upload them to ABIS for storage and subsequent matching against new biometric submissions.

[2] The DOD master watchlist is a controlled list of "most-wanted" individuals managed by the U.S. Army National Ground Intelligence Center. The watchlist is the means by which soldiers in theater are able to apprehend dangerous persons.

vulnerabilities.[3] The system does not meet DOD redundancy requirements and would be out of service in the event of a natural or man-made disaster. Backup, restore, and recovery procedures are deferred to the Follow-on Operational Test and Evaluation (FOT&E). Additional cybersecurity details are contained in the classified annex.

System Description and Mission

DoD ABIS is the result of a Joint Urgent Operational Need request for a United States-based DOD authoritative biometrics collection, storage, and matching system. The IOT&E was requested by US Special Operations Command (USSOCOM) at the Biometrics Executive Committee meetings and by memorandum from US Central Command (CENTCOM) prior to the redeployment of ABIS 1.2. ABIS consists of information technology components and biometric examiner experts that (i) receive, process, and store biometrics from collection assets across the globe, (ii) match new biometrics against previously stored assets, and (iii) update stored records with new biometrics and contextual data to positively identify and verify actual or potential adversaries. ABIS interfaces with collection systems, intelligence systems, and other biometric repositories across the federal government. ABIS was modeled after the Next Generation Identification (NGI) program that formerly was known as the Integrated Automated Fingerprint Identification System. NGI is the criminal history database for the Federal Bureau of Investigation (FBI). NGI, which contains over 100 million subjects, began operations in 1999. Like NGI, the primary matching method of ABIS is ten print identifications whereby comparison of incoming fingerprint images to previously enrolled records allows subjects to be linked across different encounters.

ABIS v1.2 enhancements include scalable storage, support for increased transactions per day, upgrades to biometric matching algorithms, and support for mandated biometric standards. ABIS v1.2 operates at BIMA in Clarksburg, West Virginia, under the leadership of the Defense Forensics and Biometrics Agency (DFBA) – a field-operating agency under the Army's Office of the Provost Marshal General. DFBA's mission is to lead, consolidate, and coordinate forensics and biometrics activities and operations for the DOD in support of identity operations.

Test Adequacy

The operational testing of ABIS v1.2 was adequate to support an evaluation of system operational effectiveness and operational suitability. The cybersecurity evaluation was adequate to determine the system's security posture.

In August 2014, the Army Test and Evaluation Command began a two-phased operational test on ABIS version 1.2. The first phase was conducted August 7–28, 2014, and the second phase was conducted October 17–22, 2014. Because the test used the authoritative system supporting live operations, data collectors had limited opportunity to observe specific

[3] Category I cybersecurity vulnerabilities are those that if exploited will directly and immediately result in loss of confidentiality, availability, or integrity

tasks other than those required by the daily workloads at each site.[4] This was to ensure that testing would not affect real world operations.

The IOT&E consisted of two phases. During Phase 1, ABIS v1.0 and ABIS v1.2 were operating in parallel with ABIS v1.0 retaining the role as the authoritative source for submission responses received by end users. For Phase 1, BIMA operators archived ABIS v1.2 response files for comparison to responses generated by ABIS v1.0. During Phase 2 of the IOT&E, ABIS v1.2 was the single authoritative source for sharing responses with end users. The purpose of the two-phase test was to mitigate the risks of deploying ABIS v1.2 as the authoritative source for sharing responses to the field. The results of phase 1 supported the decision to proceed to Phase 2 of the operational test.

During the test, ATEC personnel collected data by direct observation of BIMA operator actions that spanned the range of ABIS capabilities. ATEC collected system metrics used to assess throughput and response times, and ATEC collected survey data to assess system usability. The supportability evaluation primarily used Help Desk data. ATEC used data from the independent cybersecurity tests to assess system security.

The test limitations for Phases 1 and 2 differed due to test and operational architecture differences, which affected the overall evaluation. Because the IOT&E took place during normal operations, data collectors had limited ability to observe specific tasks beyond those tasks required by the daily workloads. The impact of this limitation was minimal, however, as most operations were exercised during the 26 days of testing. Another test limitation was that the cybersecurity adversarial assessment took place when ABIS v1.0 was the authoritative source. Nonetheless, the cybersecurity assessment provided valuable insights into inherent vulnerabilities of the ABIS v1.2 system. For a complete cybersecurity assessment, DOT&E recommends that the Army conduct a follow-on adversarial assessment after addressing the critical cybersecurity vulnerabilities found during the Phase 1 adversarial assessment.

Finally, the interoperability assessment, conducted by the Joint Interoperability Test Command (JITC) after the ABIS v1.2 system became the authoritative source, was able to examine only 17 of 22 external interfaces because five interfaces did not send any submissions during the test window. These five interfaces included the Navy identity operations centers and a DOD terrorist explosive device analytical center that sends latent fingerprints to BIMA.

---

[4] DOD ABIS is the official, complete, accurate repository of biometric data of potential terrorists or other persons of interest for the DOD. ABIS has 22 documented interfaces with external collection sources. As ABIS receives repeat encounters as submissions, the submissions are placed into the ABIS. Daily tasks revolve around handling submissions in accordance with mission priority. Missions and submission rates continuously evolve based on wartime events outside the control of the test. During the test window, the full set of interfaces was not exercised. As discussed later, The Joint Interoperability Test Command certified 16 of the 22 interfaces as interoperable with ABIS.

Operational Effectiveness

ABIS v1.2 is operationally effective. The effectiveness evaluation included five major task areas: (i) receive and process biometric and latent submissions, (ii) store biometrics, latents, and associated contextual information, (iii) match incoming biometrics against existing records, (iv) share match responses across the DOD, the FBI, DHS, and international partners, and (v) support decision-making through watchlisting alerts during search and enrollment operations. The test team observed BIMA operators performing day-to-day operations in support of the five capabilities. During the IOT&E, successful demonstration of each of these capabilities led to the determination that ABIS v1.2 is operationally effective.

ABIS v1.2 interoperated with the external interfaces to exchange information during the test. The United Kingdom Defense Exploitation Facility reported response formatting issues during the IOT&E that have since been resolved.

The majority of BIMA operators surveyed (25 out of 34) agreed or were neutral when asked if their productivity was higher with ABIS v1.2 compared to ABIS v1.0. Survey results also recorded that real-time facial matching capabilities and palm print searching continue to have problems in ABIS v1.2, as was the case in ABIS v1.0.

JITC conducted an interoperability assessment from November 3-14, 2014, when ABIS v1.2 was the authoritative source for sharing biometric responses to the field; this test assessed 17 of the 22 external interfaces. A full interoperability assessment is required to verify the total number of active interfaces and to identify interfaces that do not meet minimum standards requirements.

Operational Suitability

ABIS v1.2 is not operationally suitable. Deficiencies exist in the areas of training, usability, and Help Desk operations. Although no system aborts were recorded during the 27 days of record test, 17 Essential Function Failures (EFF) required system administrator support.[5] These EFFs affected operational workflows. The automated cross-domain service (CDS), which is used to transfer high priority submissions from the Secret Internet Protocol Router Network (SIPRNet) to the Non-secure Internet Protocol Router Network (NIPRNet) (the network on which ABIS resides), was a particularly unreliable component and required substantial system administrator support during the IOT&E. The relatively low submission volumes over the SIPRNet during the test allowed the system operators to use workarounds allowing ABIS v1.2 to meet response time requirements. However, stability problems with the CDS could result in delays when processing higher submission volumes.

---

[5] An EFF is a failure of one or more of the system's essential functions that does not require the immediate removal of the system. The system can still operate and provide partial usefulness, but the failure requires repair at the earliest opportunity. There are six essential functions: receive, process, store, match, share, and manage. Examples of EFFs include system lock-ups due to problems with workstation configurations and failures to ingest the daily watchlist.

ABIS v1.2 training, training aids, and system documentation did not prepare operators to use the system. Operators need more training on ABIS v1.2 tools and new system administrators need greater understanding of the BIMA mission tactics, techniques, and procedures in order to provide Tier 1 support.[6] During the IOT&E, the system administrators had difficulty understanding the problems raised by the biometric and latent examiners. Additionally, a backlog of routine metrics reporting occurred during the IOT&E because of differences between ABIS v1.0 and ABIS v1.2; BIMA metrics personnel were unfamiliar with the latter. This reporting is essential for DOD decision-makers to evaluate the capability of ABIS v1.2 in support of national security missions.

Usability concerns lengthened the times for completion of examiner workflows. BIMA operators expressed the need for longer durations of inactivity before the main user portal timed out. Other problems included examiners' workstation settings not being saved between sessions, cumbersome user interfaces for generating reports, problems navigating between key identification fields in the Portal, lack of audible beeps when actions are required, inadequate tools for palm searching, lack of a single identifying number to link transactions associated with the same individual, and problems with latent examiner workflows.

The ABIS Help Desk support mechanisms were inadequate to support BIMA operators during the IOT&E. A centralized ABIS Help Desk support structure is required that supports both the BIMA operators and the external submitters. The Watchdesk (a separate support system within BIMA that does not overlap with the PMO-provided Help Desk) provided support to external submitters and did not systematically report issues to the PMO Help Desk system. Without a centralized Help Desk concept of operations, problems experienced by external submitters may escape notice and remain unresolved.

BIMA operators submitted 560 trouble tickets to the Tier 1, on-site trouble ticketing system during the IOT&E, of which 220 were still marked "assigned" rather than "closed" at the end of the IOT&E. BIMA operators cannot review existing tickets or status using this system, which may have caused the generation of duplicate tickets. Random entry of tickets, with poor descriptions, no prioritization, and no grouping by categories made sorting, interpreting, and managing of the tickets more difficult. The Help Desk Tiers 2 and 3 within the PMO use a different trouble ticket system – a proprietary tool maintained at the contractor development site.[7] At the end of the IOT&E, the PMO provided the testers a list of 29 trouble tickets from this system, of which 10 were marked "open." There was no cross-correlation between the PMO system and the Tier 1 trouble ticket system. Testers observed that when the Tier 2 system integrators worked closely together with the BIMA operators, problems encountered during the test were more quickly resolved.

---

[6] Tier 1 is the initial support level responsible for basic operator issues and is available 24/7.

[7] Tier 2 Help Desk support provides more in-depth technical support than Tier 1 requiring experienced engineers familiar with the particular product or service. Tier 3 is the highest level of support requiring expert level troubleshooting and analysis methods.

Cybersecurity

ABIS v1.2 is not secure from a cybersecurity perspective. The cybersecurity evaluation examined the security posture of server components hosted at the Criminal Justice Information Services division in Bridgeport, West Virginia, and the user-facing components at BIMA. The evaluation used four criteria: the ability to protect against unauthorized penetration of the ABIS; the ability to detect when intrusions and exploits occur; the existence of adequate and appropriate system and personnel reaction to intrusion attempts; and the ability to restore normal system operations after a disruption.

ATEC conducted an initial cybersecurity assessment of ABIS v1.2 in May 2014, which discovered 102 vulnerabilities. In August 2014, The Army Threat System Management Office conducted a 5-day adversarial assessment with objectives that included attempts to deceive, deny access, disrupt operations, eavesdrop, evade detection, mislead or influence administrators through misinformation, and illicitly control and manipulate system components and users. Specific findings are in the classified annex.

Recommendations

DOT&E recommends that the Army address the following issues prior to FOT&E:

Operational Effectiveness

- Complete a full interoperability certification for all interfaces.
- Verify that custom biometrically-enabled watchlist consumers can use ABIS to support missions requiring local watchlisting.
- Finalize and document standard operating procedures for correcting identity crosslinks.
- Assess the ability to repair non-standard submissions during the FOT&E, including evaluating time to repair submissions, the adequacy of tools and procedures, and the relative proportions of submissions requiring repair.

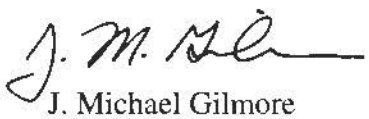
Operational Suitability

- Maintain the continuous evaluation process to monitor reliability, availability and maintainability (RAM) through full deployment.
- Assess whether sufficient numbers of trained system administrators, metrics personnel, and personnel for other critical support functions are available to support daily operations.
- Resolve stability problems with the CDS while ensuring that the CDS remains capable of preventing cyber-attacks across the NIPRNET/SIPRNET gateway boundary.
- Improve the quality of training, training aids, and other system documentation for the users.

- Develop a system for cataloging, sorting, searching, and monitoring trouble tickets that is accessible to all users and reduces redundancy in tracking and reporting of deficiencies.

Survivability

- Verify correction of vulnerabilities identified in the IOT&E.
- Complete a cooperative cybersecurity assessment of the ABIS v1.2 system before the FOT&E and an adversarial cybersecurity assessment during FOT&E.
- Address the additional recommendations regarding cybersecurity detailed in the classified annex.



J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview 1
Test Adequacy 5
Operational Effectiveness 7
Operational Suitability 19
Survivability 27
Recommendations 29
Classified Annex: Cybersecurity Testing ..... Separate Cover

This page intentionally left blank.

Section One
System Overview

This report provides the Director, Operational Test and Evaluation (DOT&E) assessment on the operational effectiveness, operational suitability, and cybersecurity of the Department of Defense (DOD) Automated Biometric Identification System (ABIS) version 1.2 (v1.2). This evaluation is based on data from the Initial Operational Test and Evaluation (IOT&E) that the Army Test and Evaluation Command (ATEC) conducted in two phases from August 8-28, 2014 and then from October 17-22, 2014 at the Biometric Identification Management Activity (BIMA) in Clarksburg, West Virginia.

Mission Description and Concept of Employment

DOD ABIS is the result of a Joint Urgent Operational Need request for a United States-based DOD authoritative biometrics source. The IOT&E was requested by US Special Operations Command (USSOCOM) at the Biometrics Executive Committee meetings and by memorandum from US Central Command (CENTCOM) prior to the redeployment of ABIS 1.2. ABIS consists of information technology components and biometric examiner experts that (i) receive, process, and store biometrics from collection assets across the globe, (ii) match new biometrics against previously stored assets, and (iii) update stored records with new biometrics and contextual data to positively identify and verify actual or potential adversaries. The system interfaces with collection systems, intelligence systems, and other biometric repositories across the federal government.

ABIS v1.2 enhancements include scalable storage, support for increased transactions per day, upgrades to underlying commercial products to include matching algorithms, and support for mandated biometric standards. DoD ABIS operates at BIMA in Clarksburg, West Virginia, under the leadership of the Defense Forensics and Biometrics Agency (DFBA) – a field-operating agency under the Army's Office of the Provost Marshal General. DFBA's mission is to lead, consolidate, and coordinate forensics and biometrics activities and operations for the DOD in support of identity operations.

System Description

BIMA operators use ABIS to help accomplish the larger DOD Biometrics mission, employing ABIS to enroll new subjects, search for matches against existing identity records, share responses with partners within and outside DOD, and issue alerts whenever watchlisted individuals are encountered.

The operational concept, which displays the major functionality of ABIS, is contained in Figure 1-1 below.

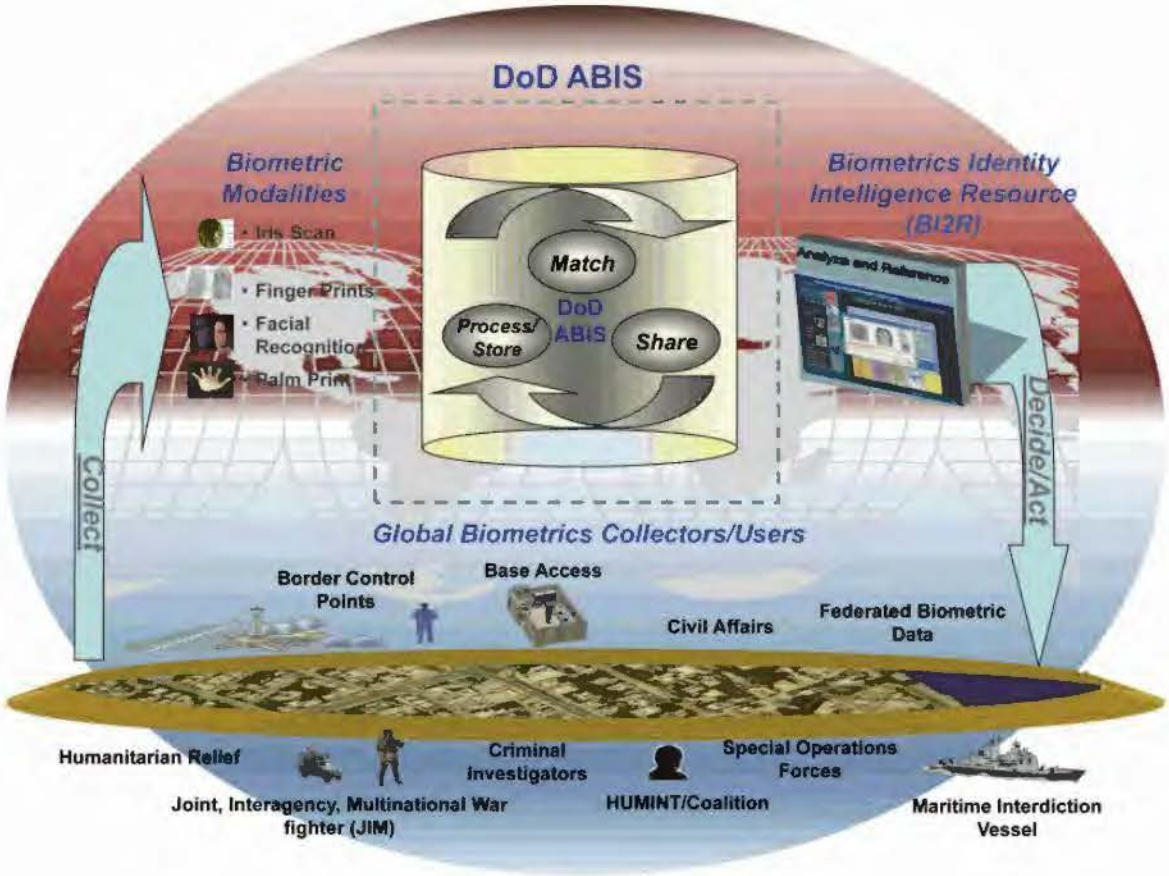


Figure 1-1. ABIS Operational Concept

- Receive/Process
  - Supports the ingestion of multi-modal biometric and latent data from globally distributed collection assets.
  - Supports the processing of biometric and latent data based on DOD Electronic Biometric Transmission Specification (EBTS)/Electronic Fingerprint Transmission Specifications standards.
- Store
  - Supports the enrollment, update, and maintenance of biometric and latent files to make standardized, current biometric information of individuals available when and where required.
- Match
  - Supports the accurate identification or verification of an individual by comparing a standardized biometric file to an existing source of standardized biometrics data and scoring the level of confidence of the match.

- Share
  - Supports the exchange of standardized biometric files and match results among approved DOD, Interagency, and Multinational partners, in accordance with applicable laws and policy.
- Decide/Act
  - Allows users to make decisions and take appropriate actions (e.g., detain, question, etc.) based on alerts received when biometric match results align with watchlisted individuals on the DOD Biometrically Enabled Watchlist (BEWL).

This page intentionally left blank.

Section Two
Test Adequacy

The ABIS version 1.2 (v1.2) Initial Operational Test and Evaluation (IOT&E) was adequate to support an evaluation of system operational effectiveness and operational suitability. A cybersecurity test identified vulnerabilities in the ABIS v1.2 security posture.

Operational Testing

The IOT&E consisted of two phases. Phase 1 took place August 8-28, 2014, and involved 28 Biometrics Identification Management Activity (BIMA) operators performing typical daily tasks. Phase 2 took place October 17-22, 2014, and involved all 56 operators engaged in daily operations. During Phase 1, ABIS v1.0 and ABIS v1.2 were operating in parallel with ABIS v1.0 retaining the role as the authoritative source for all responses to external users. BIMA operators archived ABIS v1.2 response files for comparison to responses generated by ABIS v1.0. Conversely, during Phase 2 of the IOT&E, ABIS v1.2 was the single authoritative source for sharing responses. The purpose of the two-phase test was to mitigate the risks of deploying ABIS v1.2 as the authoritative source for sharing responses to the field.

The Army Test and Evaluation Command (ATEC) performed various forms of data collection during the test. ATEC personnel collected data by direct observation of BIMA operator actions that spanned the range of ABIS capabilities. Another source of information was automatically produced system metrics used to assess throughput and response times. ATEC also collected survey data to assess system usability. Help Desk data were leveraged to evaluate supportability. ATEC leveraged cybersecurity data collected from the independent adversarial tests to assess system security.

Test Limitations

Because of the limited test duration, ATEC could not assess system reliability at the 80 percent confidence level. A total of 77 days was required; however, the two-phase test lasted only 26 days. Because the IOT&E took place during normal operations, data collectors had limited ability to observe specific tasks beyond those tasks required by the daily workloads. The impact of this limitation was minimal, however, because most operations were exercised during the 26 days of testing. Another test limitation involved the cybersecurity adversarial assessment of ABIS v1.2. Because the assessment took place when ABIS v1.0 was the authoritative source and because the ABIS v1.2 system administrators were not in place to defend the ABIS v1.2 system against cyber threats, a complete cybersecurity assessment of ABIS v1.2 could not be performed. This limitation primarily affected the assessment of the cyber defender personnel's ability to detect, react, and recover from realistic cybersecurity penetration attempts. Nonetheless, the cybersecurity assessment provided valuable insights into inherent vulnerabilities of the ABIS v1.2 system.

Finally, the test was limited because the interoperability assessment, conducted by the Joint Interoperability Test Command (JITC) after the ABIS v1.2 system became the authoritative

source, was able to examine only 17 of 22 external interfaces because five external sources did not submit any requests during the test window. These five interfaces included Navy identity operations centers and a DOD terrorist explosive device analytical center that sends latent fingerprints to BIMA. A full interoperability assessment is required to verify the total number of active interfaces and to identify interfaces that do not meet minimum standards requirements.

Section Three
Operational Effectiveness

ABIS v1.2 is operationally effective. Users accomplished all necessary tasks with only minor errors. The operational effectiveness evaluation considered five major capabilities that ABIS must be capable of performing to support mission operations: Receive/Process, Store, Match, Share, and Decide/Act.

Receive/Process

Assessment of the Receive/Process operation examined the ability of ABIS v1.2 to meet submission demands of current DOD and non-DOD submitters. Receive/Process examined three subcategories: throughput, performance, and support for non-standard submissions.

The design of Phase 1 of the IOT&E examined whether ABIS v1.2 could handle the daily throughput levels experienced during real-world submissions by employing parallel operations architecture with ABIS v1.0 as the authoritative system. The systematic copying of contents from the ABIS v1.0 receiving folders into the analogous ABIS v1.2 folders allowed sharing of incoming submissions by both systems. To mitigate mission risk, external sharing of match/no-match responses relied only on ABIS v1.0 outputs. By quarantining match/no-match response files generated by ABIS v1.2, Biometrics Identification Management Activity (BIMA) operators were able to compare responses for the same submission in ABIS v1.0. Real-world mission constraints caused some differences in the submissions entering the two systems. For example, approximately 20 percent of submissions received by ABIS v1.2 were bulk fingerprint scans from U.S. European Command (USEUCOM) that ABIS v1.0 did not process, likely because of inadequate numbers of operators. After accounting for these discrepancies, analyses confirmed that more than 72,000 submissions had matching response files between the two systems.

The threshold throughput requirement for ABIS is 8,000 submissions per day; ABIS v1.2 daily throughputs exceeded this number on four separate days during the test window. ABIS experienced a peak of approximately 15,000 daily submissions on August 12, 2014. The average daily submissions were approximately 5,000 and the median number of submission was just over 4,300. Data submission rates of real-world events did not allow demonstration of the objective requirement of 45,000 daily submissions during the IOT&E.

Maximum allowed response time for generating a match response per priority level of the original request is the basis for most of the ABIS performance requirements. Analysis of submission performance reports gathered during Phase 2 confirmed that ABIS v1.2 match/no-match response times met requirements by a wide margin with statistical confidence in all of the 31,000 submissions.[8] Tables 3-1 and 3-2 show the results by priority of the incoming biometric

[8] All available representative personnel were supporting Phase 2 operations using ABIS v1.2 since it was servicing the end-users. Performance results from this Phase are more operationally relevant.

submissions that were analyzed. Submission priorities represent the maximum length of time a response is required by the submitter.

Table 3-1. Evaluation of ABIS v1.2 Response Times for Biometric Matching during Phase 2

Submission Priority	Total Samples	Automated Response Time (minutes)		Median Automated Response Time (minutes)	Manual Response Time (minutes)		Median Manual Response Time (minutes)	Required Threshold (minutes) (auto/manual)
		Mean	80% CI		Mean	80% CI		
1	1,251	0.94 (1,240)	[0.924, 0.956]	0.75 (1,240)	2.4 (11)	[1.975, 2.731]	2.2 (11)	15/30
2	7,523	0.84 (7,507)	[0.829, 0.845]	0.68 (7,507)	5.3 (16)	[4.382, 6.236]	5.0 (16)	30/120
3	19,587	0.97 (19,232)	[0.965, 0.978]	0.79 (19,232)	41.1 (355)	[36.101, 43.689]	23.9 (355)	60/1,440
4	2,565	0.63 (2,508)	[0.628, 0.641]	0.5 (2,508)	28.1 (397)	[20.254, 36.004]	4.2 (397)	240/2,880

(Numbers in parentheses are the number of submissions)

Table 3-2. Evaluation of ABIS v1.2 Response Times for Latent Matching during Phase 2

Submission Priority	Total Samples	Manual Response Time (minutes)		Median Manual Response Time (minutes)	Required Latent Threshold (minutes)
		Mean	80% CI		
1	6	9.8	[5.194, 14.396]	8.7	120
2	17	6.1	[4.688, 7.432]	4.4	1,440
3	343	163.8	[130.147, 197.443]	50.1	7,200
4	9	63.9	[29.866, 98.010]	29.8	N/A

ABIS v1.2 is designed to meet the DOD Electronic Biometric Transmission Specification (EBTS) v1.2. The DOD EBTS specifies requirements for the interface between DOD systems that capture biometric data and those that store or match it. Not all submissions received at BIMA meet minimum EBTS v1.2 standards. ABIS moves submissions that are not compliant with EBTS v1.2 from secure File Transfer Protocol (sFTP) destination folders, email, or media to a location where specially trained personnel can repair them before being entered into the automated receive/process queues. The time to repair, the types of repair, and the percentage of submissions requiring repair cannot be determined from the system performance reports. Table 3-3 lists the types and numbers of errors automatically captured and reported during Phase 2. Duplicate submissions were relatively frequent and highlighted in the table. Duplicate

submissions occur when users in the field inadvertently submit the same biometric data more than once. Approximately 32 percent of these submissions were bulk fingerprint scans from USEUCOM. The Department of Homeland Security (DHS) accounted for 54 percent of the duplicate submissions. Watchdesk personnel in interviews stated that duplicate submissions are a normal occurrence and do not degrade operations.

Table 3-3. Submission Ingest Errors

Error	Phase 1 Count (% of 104,170 total submissions)	Phase 2 Count (% of 31,298 total submissions)
Authentication Failure	1,079 (1.0%)	22 (0.1%)
Authorization Failure	23 (0%)	13 (0%)
Corrupt Submission	253 (0.2%)	13 (0%)
Duplicate Submission	18,239 (17.5%)	3,276 (10.5%)
Invalid TCN	371 (0.4%)	0
Invalid Watchlist	114	7
No Biometrics Present	5 (0%)	0
Unsatisfied Link	277 (0.3%)	1 (0%)
US Citizen Not Allowed	1,388 (1.3%)	108 (0.4%)
Storage Error	18 (0%)	2 (0%)
Total Errors	21,767 (20.3%)	3,442 (11%)

The Joint Interoperability Test Command (JITC) conducted an interoperability assessment November 3-14, 2014, after Phase 2 of the IOT&E. Due to test limitations noted previously, JITC was able to assess only 17 of 22 external interfaces. DOT&E recommends that JITC perform a full interoperability assessment prior to the FOT&E. However, the interoperability assessment will require clear definition of all active and current interfaces and associated Service-level agreements. JITC should confirm that ABIS is consistently meeting Service-level agreements and that mechanisms exist to flag violations or interruptions of these agreements. The assessment should identify those interfaces that do not meet minimum EBTS requirements. BIMA and PM Biometrics should issue recommendations to enable submitters to meet minimum standards requirements and evolve to the DOD-mandated EBTS 3.0. To enable compliance with mandated standards, the Army should broadcast awareness of commonly occurring interoperability problems to DOD Biometrics stakeholders and notify submitters who are sending a substantial number of poor quality submissions.

The Cross Domain Solution (CDS), which allows for the expedited transfer of classified submissions into the unclassified ABIS v1.2 database, was unstable during the IOT&E. As a workaround, the Watchdesk operator frequently had to manually post high-priority submissions to the U.S. Special Operations Command (USSOCOM)-shared portal and alert the submitter by email of the file posting to the portal.

Store

Assessment of the Store capability examined the ability for ABIS v1.2 to securely store and retrieve submissions containing biometric data, latent prints, and associated contextual and biographical information in support of current and emerging missions. The evaluation of Store is divided into four subcategories: capacity, history, integrity, and standards compliance.

- Capacity is the ability for ABIS to store more records without degrading performance.
- History refers to the ability to search and retrieve all information relevant to a single person, including all the submission records that the system has linked to that same identity.
- Integrity is the measure of accuracy and consistency of the stored data over its life cycle.
- Standards compliance is the ability to store and retrieve data in accordance with the currently adopted EBTS v1.2 specification.

Capacity examines the ability of ABIS to store more records. At present, ABIS v1.2 contains more than 15 million biometric submission records, exceeding the threshold requirement of 2 million records, but not the objective requirement of 30 million records. During the IOT&E, the system accrued approximately 330,000 submissions. Review of Phase 2 data showed that average file size was approximately 800 KB, with file sizes ranging from 200 KB to 2 MB. The 31,000 submissions in Phase 2 added approximately 24 GB to the database. The Biometric database has a capacity of 2.6 TB, of which 1.6 TB are used. Automated search and retrieval of stored records during the IOT&E was faster in ABIS v1.2 than in ABIS v1.0.

History examines the ability of ABIS v1.2 to link all encounters that map to the same identity. Identity linking occurs via automated tenprint-to-tenprint matches that score above a specified threshold, via examiner decision in the processing of queues, and via examiner decision through the portal. During the IOT&E, BIMA operators could review identity histories without problems. Examiners manually link or unlink biometric records within an identity as part of their normal standard operating procedures. Examiners unlink identities when they encounter erroneously linked identities. Crosslink files can be one source of erroneous linking when one file incorrectly contains biometrics from multiple individuals. Standard operating procedures for correcting crosslinks have been developed and institutionalized.

Integrity measures the ability of the system to accurately store data over its life cycle. The upgrade to ABIS v1.2 required "re-templating" all raw biometric images into new templates for subsequent matching. PM Biometrics reported that as of July 21, 2014, 2,687 of 12,358,114 (0.02 percent) submission records could not be migrated because of duplicate, corrupted, or invalid data in the EBTS records. BIMA accepts this discrepancy and agrees that it does not affect operations.

Standards Compliance examines the ability for ABIS v1.2 to store and retrieve records according to the mandated EBTS standard. ABIS v1.2 is using an older version of the standard

to support the needs of the majority of external submitters. DOD policy requires the submitters to begin implementing the EBTS v3.0 standard, but development of devices and procedures are required to meet the standard.

Match

The Match capability examines the ability of the system to determine whether an incoming submission matches one or more existing records within prescribed time requirements. The analysis of Match has two subcategories: consistency with ABIS v1.0 and adequacy of Examiner software. ABIS v1.2 and ABIS v1.0 are "consistent" when the same submission returns the same result during parallel operations. In a live system, match accuracy is difficult to measure because ground truth (whether the subject is or is not the matched identity) is unobtainable. The IOT&E used consistency of matches between the two systems and manual review of selected matches by human operators to evaluate Match capability.

Adequacy of Examiner software focuses on whether the tools used by Biometric and Latent Examiners meet expectations. This assessment relies on Examiner subject matter expertise in ensuring match accuracy.[9]

The test assessed automated and manual matches for consistency. Because the system is multi-modal, one or more biometrics may be involved in the decision-making process. The system must match incoming fingerprints to both existing fingerprints (index-to-index finger or other combinations may be employed) and to existing unsolved latent prints (all available fingerprints may he used). Iris images are templated and searched against the iris gallery, and compares facial images to the entirety of the face gallery. If the fingerprints or the irises score high enough to trigger an auto-identification, a response is generated and sent to the submitter. Due to the version of search core software used by ABIS v1.2, the face algorithm employed in ABIS v1.2 is unahle to auto-identify by face only. Due to this limitation, a separate face-matching capability compares face-only submissions. If ABIS v1.2 is not capable of achieving a match on any of the unilateral biometric modalities, a proprietary fusion algorithm engages to leverage all modalities to increase the incidence of auto-identifications. The fusion capability further reduces the number of biometric submissions that require human examiner review.[10] Verifying consistency for both automated and manual match/no-match determinations took advantage of data from Phase 1 testing because of its longer duration and allocation of sufficient personnel to operate both systems.[11] Table 3-4 shows the Phase 1 submissions (approximately

---

[9] In identification systems, accuracy is defined by two error rates: false-positive error rate and false-negative error rate. The system can be adjusted to reduce one error rate at the expense of the other based on knowledge of the quality of the incoming and existing submissions. Such optimizations are performed offline by subject matter experts, and can take time. Periodic adjustment is required to keep pace with changes in the breadth and quality of submissions and changes in search algorithms. Interviews with several BIMA and Biometrics Program Management Office personnel indicate such an update is overdue. Changes in the thresholds can affect the match accuracy results.

[10] Yellow resolves are search responses that do not automatically provide conclusive match results but instead provide a list of candidate identities. Biometric and latent examiners use special software to resolve such cases.

[11] Fewer personnel were available to support ABIS v1.0 operations during Phase 2.

66,000) and level of match consistency between the two systems.[12] Since 98 percent of these submissions contain fingerprints, it is likely that the match decision leveraged fingerprint matching more than the other modalities.[13]

Table 3-4. Evaluation of ABIS v1.2/ABIS v1.0 Match Consistency during Phase 1

		ABIS v1.0	
		Match	No-Match
ABIS v1.2	Match	59,238	185
	No-Match	30	6,505

These results indicate a 99.7 percent consistency between the two systems, and are a positive indicator that ABIS v1.2 matching was as good as ABIS v1.0. During Phase 2, approximately 34 percent of submissions resulted in a positive match. The rate of "yellow resolves" that require manual review by examiners was approximately 1 percent. The ABIS v1.2 system demonstrated a 10 percent reduction in manual review rate (from 11 percent to 1 percent) without loss of consistency with ABIS v1.0. That is, ABIS v1.2 achieved equivalent results with fewer manual reviews.

Latent examiners reported anomalies with the unidentified latent match (ULM) capabilities. The ULM tools send incoming fingerprints to a repository of latent fingerprints that are yet unlinked to any individual in the database. The concern was that the rate of ULM matches dropped significantly relative to when ABIS v1.0 was the authoritative source, without a plausible explanation.[14] Upon completion of the IOT&E, there were 88 problems pertaining to the Latent Examiner Workstation in the BIMA Event Tracker, a BIMA trouble ticket system.

Share

Sharing timely match responses with operational users to support DOD priority missions is the primary purpose of ABIS. Since the deployment of ABIS v1.0, BIMA has developed sharing agreements with numerous groups within the DOD, DHS, FBI, and international

---

[12] Missing fields and differences in response formats prevented a one-to-one comparison of all submissions.

[13] The ability for multi-modal biometrics to increase identification of potential adversaries has not been independently assessed. Based on the data provided, there were no records for positive facial identification. BIMA uses an off-line suite for facial matching. Facial match results from this suite are not available within the match response time requirements. Approximately 9,000 positive matches were made by iris matching during Phase 1 but only about 500 of those were not already resolved through fingerprint matching. There were 158 cases in which the iris disposition conflicted with the fingerprint disposition. The latter was used to confirm the match result.

[14] Latent examiners stated that they had expected to see approximately 10 matches per day, but were seeing no more than one or two. ATEC did not collect latent hit rates during the test.

partners. This assessment examined sharing success across the three types of partners: DOD partners, federal partners (FBI and DHS), and international ABIS partners. First, the assessment considered the relative proportions of submissions across these partners. Next, the assessment described the ABIS sharing agreements that clearly and correctly defined and coded in the system. Submissions from partners are processed and responses received by the intended recipients. Finally, the assessment focused on a subset of submissions during Phase 2 to validate successful sharing of responses for those submissions.

Figures 3-1 and 3-2 show the relative proportions of submissions sent by DOD Components, DHS, and the FBI during the two phases of the test. These proportions change as missions evolve. DHS shared a large proportion of submissions during both phases to support its Customs and Border Protection division. Although these are included in the submission count, these submissions are not retained by ABIS under current sharing agreements. U.S. Central Command was a large DOD submitter, with the National Ground Intelligence Center (NGIC) managing those submissions. During Phase 1, USEUCOM sent nearly 40,000 submissions consisting largely of low priority, bulk submission of fingerprint scans from DOD missions spanning their area of responsibility.

Federal partners have a three-fold relationship with ABIS. First, having large biometric repositories themselves, the DHS and FBI share certain large collections based on mutually beneficial agreements. The FBI shares collections obtained in foreign countries where U.S. law enforcement works together with the U.S. military to register criminals from other countries who may pose a national threat. DHS shares collections from refugee missions so that DOD can maintain local copies of these records to satisfy mutually relevant missions. Second, the DHS and FBI can send individual submissions to merge match results that can enhance identity awareness within their own repositories. For example, DHS sends large numbers of submissions obtained at Customs and Border Protection sites to ABIS to help prevent potential adversaries from entering the U.S. ABIS does not retain these submissions because these persons are generally not suspicious persons. Third, certain DOD submitters send individual submissions to be searched against the FBI and DHS collections to broaden DOD's awareness of known criminals or persons of interest.

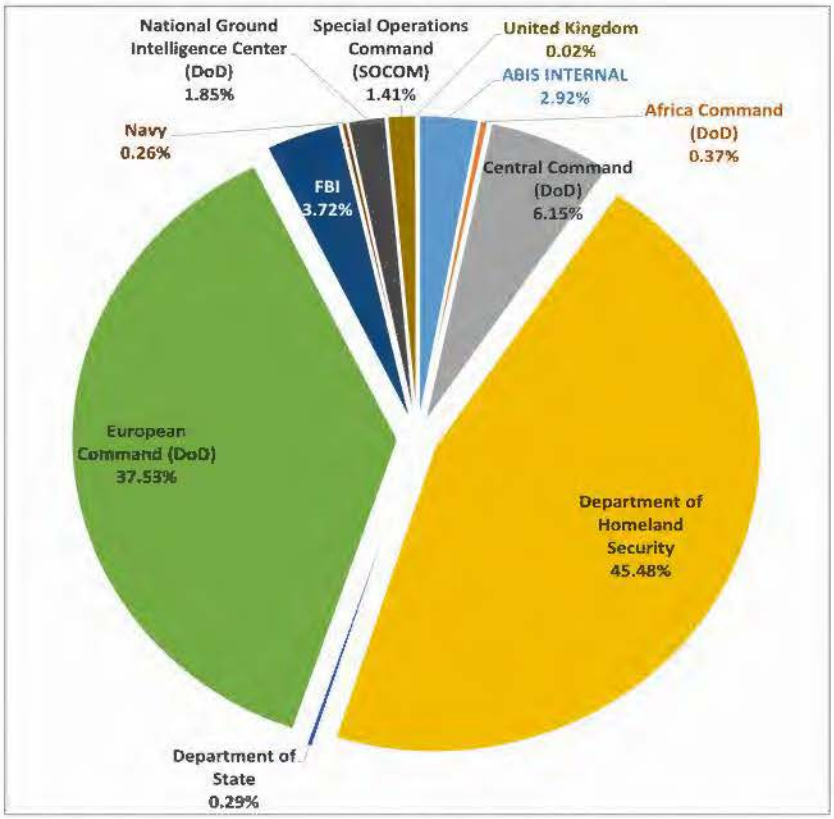


Figure 3-1. ABIS v1.2 Phase 1 Submissions (Total: Approximately 104,000)

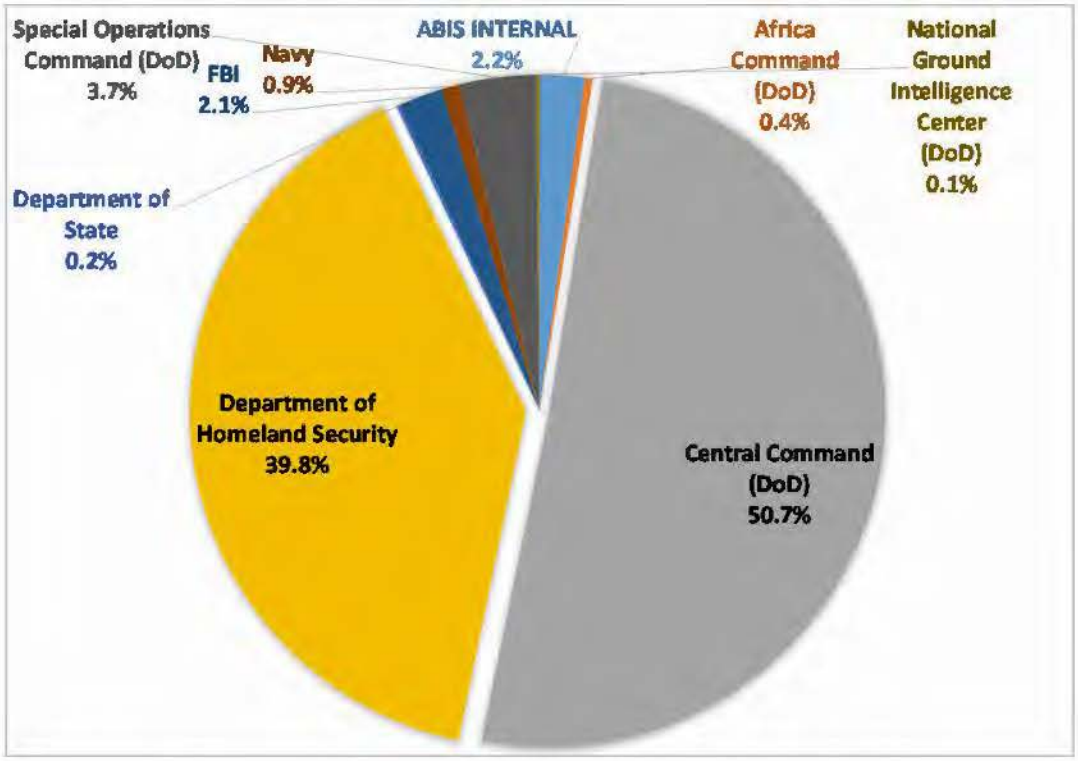


Figure 3-2. ABIS v1.2 Phase 2 Submissions (total: ~ 31,000)

With tens of thousands of incoming submissions and many more outgoing responses (each response can go to multiple recipients), a manageable strategy for assessing Share was required. Sharing agreements define special handling instructions for submissions and responses.[15] In order for each response to process successfully, these instructions must he accurate correctly processed by the system. Each interface agreement has a unique configuration file, denoted as an originating agency identifier (ORI) configuration. ORI configurations are continually evolving to meet changing mission requirements (e.g., need for new modalities), email address updates (e.g., from personnel turnover), and new requests to search other repositories (e.g., DHS and FBI). Each partner has many ORIs with distinct rules for handling different groups of submissions. Currently, ORIs do not have an expiration date. As a result, more than 8,000 ORIs exist, but many are inactive.[16] BIMA is reviewing the ORIs to validate the active ORI set.

ABIS and its consumers continuously coordinate interface changes, monitor interfaces, and fix errors to ensure that information exchanges are accurate, complete, understandable, and timely. Inaccurate ORIs lead to errors in responses, including incorrect handling of submissions and incorrect output file formats. Such problems result in help desk tickets that the Watchdesk must investigate and resolve. A previous deployment attempt in August 2013 failed in part because of outdated and misconfigured ORIs that resulted in incorrect output file formats. Given the volume of daily submissions, the IOT&E targeted five high-volume ORIs per day from each major DOD submitter group. Points of contact at each of these groups confirmed whether expected responses were received during each day of Phase 2. Additionally, ATEC surveyed Watchdesk personnel to capture their impression of sharing problems.

ABIS v1.2 successfully shared responses with DOD partners, with only minor problems. Table 3-5 shows the reported number of submissions and issues experienced for submissions from the most frequently encountered ORIs.

Table 3-5. Evaluation of ABIS v1.2 Responses for DOD Partners during Phase 2

DOD Component	Submissions	Issues
U.S. Special Operations Command	865	2
U.S. Africa Command	94	0
National Ground Intelligence Center	2,511	0
U.S. Navy	87	0

USSOCOM submitted two trouble tickets to the Watchdesk, both of which were resolved. USSOCOM also noted that ABIS v1.2 responses from the FBI repository took up to 6

[15] For example, agreements typically include email addresses for sending alerts. Agreements with foreign partners may require that submissions are not retained in ABIS after search results are returned. Certain missions may require that all enrolled individuals are "encounter protected" such that their biometrics are searchable only by stakeholders of that particular mission.

[16] This number is a rough estimate provided by emails from BIMA operators.

hours; however, the response times met the specified requirements for the FBI, and were attributed to problems within the FBI infrastructure. USSOCOM encountered no ABIS v1.2 problems that affected their operations. Post-test analysis discovered that USSOCOM handheld devices did not receive a yellow-flash notification message for submissions that went to yellow resolve. All response times were under 3 minutes, and the reason for the lack of a yellow-flash notification is unknown. Since the end of test, USSOCOM has received yellow-flash notifications.

During Phase 2, ABIS v1.2 sent 2,046 submissions to the FBI, but the FBI received 2,439 submissions. Without a point of contact at the FBI, it was not possible to ascertain the reason for this discrepancy. DHS sent 807 responses during Phase 2, likely in response to USSOCOM requests. Because of privacy concerns, DHS does not reply to all DOD match requests.

Only one foreign partner reported problems during the test. The United Kingdom reported problems to the Watchdesk regarding improperly formatted responses. These problems have since been resolved.

Interviews with Watchdesk personnel indicated that external agencies did not experience significant problems during the IOT&E.

Decide/Act

The Decide/Act capability examines the ability of ABIS v1.2 to provide timely responses that can influence appropriate actions when warfighters encounter persons of interest. The watchlist identifies Persons of interest including known or suspected terrorists. The Biometrically Enabled Watchlist (BEWL) is created by ABIS when the watchlist and biometrics are matched. The BEWL is an intelligence product developed and maintained by the National Ground Intelligence Center (NGIC). Decide/Act has three subcategories: daily ingest of the DOD Biometrically Enabled Watchlist (BEWL), BEWL "hit" alerts generated and sent to all designated recipients, and period processing of Custom BEWLs.[17]

During both Phase 1 and Phase 2, ABIS v1.2 successfully processed daily BEWLs.[18] The process of creating a BEWL starts with searching through a list of unique transaction numbers (submissions coming into ABIS and NGIC are marked as soon as they enter the system with a number that includes the time of receipt), finding all identities that match to the incoming snbmissions, and tagging them as "watchlist" hits. Enhancements to the interface between NGIC and BIMA improved the daily BEWL ingestion process, with Watchdesk procedures now

---

[17] The BEWL is an intelligence product developed and maintained by the National Ground Intelligence Center (NGIC). The Watchdesk receives daily updates of the BEWL. ABIS ingests this update. When submissions entering ABIS match against existing records, they are also compared to the BEWL to verify whether the individual is someone that the DOD is tracking, for whatever reason. ABIS outputs BEWL "hits" in addition to match/no-match results. DOD military personnel must receive appropriately formatted alerts (to include actions they must take) when individuals they encounter are on the BEWL.

[18] The original goal was to compare the number of watchlist hits from ABIS v1.0 and ABIS v1.2. However, this was later determined to be a moot comparison because of test architecture limitations preventing simultaneous processing and because of differences in the watchlists used on each system.

requiring minutes instead of hours to process the daily BEWL. ABIS processed all valid watchlist files during phase 2. However, ABIS received four corrupted files during phase 2. ABIS successfully processed updates for the corrupted files with no adverse effects on the mission. However, NGIC reports that the new interface with ABIS v1.2 precludes the proper exchange of error messages when match reports fail to process through ABIS.

When biometric submissions to ABIS return a match, ABIS compares the identity to the watchlist to determine if a watchlist hit occurred. The associated match response file must include the hit details, including the actions to execute when an encounter with the matched individual takes place. During the IOT&E, approximately 10 percent of the matches made by ABIS resulted in a watchlist hit. The accurate format of the response files allowed an assessment of watchlist processing accuracy. A review of the trouble tickets pertaining to watchlist hits did not find any tickets regarding non-receipt of watchlist hits by intended recipients.

Custom BEWLs are a subset of identities extracted from the daily master DOD BEWL based on categories of interest to distinct groups of ABIS consumers. Consumers within USSOCOM will have different interests than consumers within the United Kingdom, for example. The BIMA Watchdesk ingests the subset of identities, generates output files, and places these files in folders where designated administrators at the consumer sites retrieve them. USSOCOM receives a custom BEWL approximately twice a month and uploads the information to handheld devices to allow local watchlisting without the need to reach back to ABIS. Processing the customized scripts required working closely with the customer representatives within BIMA, the Watchdesk, and the System Integrator. Customer representatives within BIMA have confirmed that generated Custom BEWLs are accurate. External consumers were not able to confirm that the BEWLs are meeting their mission requirements due to formatting issues that were still being resolved during and after the IOT&E.

This page intentionally left blank...

Section Four
Operational Suitability

ABIS v1.2 is not operationally suitable, with deficiencies in the areas of training, usability, and Help Desk operations. ABIS v1.2 did not experience any failures during the IOT&E that were countable against the Mean Time between Failures (MTBF). Failures that count against MTBF are termed system aborts. Essential Function Failures (EFF) that are at least 15 minutes in duration as termed system aborts, however, EFFs of less than 15 minutes are not. Although no system aborts were recorded during the 27 days of record test, 17 essential function failures (EFFs) during Phase 1 required system administrator support.[19] Mean time between EFF (MTBEFF) was 39 hours, with an 80 percent statistical confidence interval of 28 hours to 55 hours. The test recorded 132 additional Reliability, Availability and Maintainability (RAM) events classified as "minor" during the IOT&E (117 during Phase 1 and 15 during Phase 2). Users opened 560 tickets using a separate trouble ticket system, with 220 of these tickets still marked as unresolved at the end of the IOT&E. BIMA and the PMO maintained two separate trouble ticket systems during the IOT&E. No common identifier links these two systems. Furthermore, tbe trouble tickets are not rated by priority or mission impact.

During the IOT&E, the test team observed users performing routine tasks during normal operations, and recorded observations of mission successes and failures. The system must maintain availability of 95 percent or higher and a 90 percent probability of completing a 120-hour mission.[20] RAM data collectors reported no system aborts during the 27 days of record test. The system demonstrated that it met the mean time between failures (MTBF) threshold requirement of 1,140 hours between failures with a 44 percent statistical confidence level, no reported EFFs lasted at least fifteen minutes resulting in none being scored as system aborts during the test. DOT&E considers the 17 EFFs as chargeable failures that would affect the overall reliability of the mission because of the need for system administrator support. With 17 chargeable failures during 664 hours of RAM monitoring, the demonstrated MTBEFFs is 39 hours. During the IOT&E, Table 4-1 describes the 151 temporary RAM events that did not affect reliability of the mission. Examples of temporary events included the cross-domain service being down, unexplained system lock-ups, and inability to access biometric files.

RAM failures were categorized using a seven-point severity level scale in accordance with the failure definitions and scoring criteria developed by the Army. Table 4-1 contains the failure definitions and failure occurrences during both phases. No EFFs and only one rapid

---

[19] An essential function failure is a failure of one of six essential functions that nonetheless does not require the removal of the system from service. If the system is unable to receive, process, store, match, and manage submissions for longer than 15 minutes, however, the essential function failure is scored as a system abort.

[20] Establishing a sufficient statistical confidence of 80 percent requires 77 days of testing (with no failures) in which all likely operational functions are executing on operationally representative hardware and software. Since the total reliability test time spanned a period of only 27 days, achieving sufficient statistical confidence was not possible.

recovery event occurred during Phase 2. However, Phase 2 was only 5 days long while Phase 1 was 21 days.

Table 4-1. Failure Definitions and Scored Incidents

Failure	Definition	Incidents	
		Phase 1	Phase 2
System Abort	An event that renders the system unable to enter service or causes the immediate removal from service.	0	0
Essential Function Failure	A failure that allows partial system usefulness but must be fixed at earliest opportunity. EFFs include: 1) Inability to receive, process, store, match fingerprints, and generate a watchlist alert for a period greater than 15 minutes. 2) Inability to share responses within 8 hours. 3) Failure of Examiner workstations for a period greater than 15 minutes.	17	0
Non-Essential Function Failure	A failure that allows partial system usefulness and can be repaired at the next scheduled maintenance opportunity.	37	13
Rapid Recovery Event	A failure that can be corrected within established time constraints through the execution of prescribed maintenance procedures using authorized tools and parts available on-site.	22	1
Other Failure Event	Incidents that are not officially part of the system under test (e.g., equipment modification, test peculiar, performance limitation, information) and have no applicability to reliability or maintainability	49	0
Maintainability Failure	Incidents that are not reliability failures but do affect maintainability. Examples include preventative and scheduled maintenance, routine operating procedures such as replacing batteries or printer components.	11	1
Dependent Failure	A failure that is caused by another near-simultaneous failure.	0	0
Total		136	15

In surveys, BIMA operators reported difficulties in learning the new workflows in ABIS v1.2. Latent examiners reported the most problems. BIMA operators submitted 560 trouble tickets into their local ABIS trouble ticket (ABIS Event Tracker) system. Although the system integrator worked on-site as Tier 1 help support to address the problems when reported, the parties did not have a mutual understanding of problems. To improve usability, the PM Biometrics and BIMA should review the biometric and latent examiner service tactics, techniques, and procedures to ensure that they accurately reflect the existing workflow processes. Biometric examiners also need more training on the new tools and features available in ABIS v1.2. Operator comments identified the need for a longer duration of inactivity before the main user portal times out from inactivity. In addition, operators need examiner workstation settings saved between work sessions, improvements to reporting, improved navigation between key identification fields in the portal, audible beeps when actions are required, and improvements to palm searching. Latent examiners need a single identifying number with which to link

transactions associated with the same individual. The Watchdesk needs improvements to the reliability and usability of the cross-domain service. Finally, PM Biometrics needs to address problems with the latent examiner workflows.

Measuring the time to resolve help desk tickets has been problematic. To complicate matters there are two separate trouble ticket systems, one allows direct entry input by BIMA operators and the other is a proprietary issue-tracking product (JIRA) with input only by system integrator personnel and the DOD Biometrics Program Office. No common identifiers link the two systems. More than 200 problems in the BIMA-operated system remain open whereas the PM Biometrics considers all high priority tickets from the IOT&E closed. Neither trouble ticket system prioritizes tickets according to mission impact. The configuration control board does not systematically address the status of open tickets, expected resolution date, or regression test plans and procedures. In both systems, verification of tickets marked "closed" through regression testing with BIMA operators present is unclear. Furthermore, tickets were not grouped by functional area or by the affected system component. DOT&E recommends that BIMA work with the PM Biometrics to develop a system for cataloging, sorting, searching, and monitoring trouble tickets that is accessible to all users and reduces redundancy in tracking and reporting of deficiencies. For example, if tenprint examiner workstation problems were grouped separately, it would be simpler for operators to determine whether a problem they are observing has already been reported and is being addressed. The problem should be traceable between the two trouble ticket systems.

System supportability concerns include insufficiently trained system administrators whose responsibilities are integral to examiner tactics, techniques, and procedures. Additionally, new roles and responsibilities require appropriate training and timely subject matter assistance. For example, the Watchdesk is now responsible for creating custom BEWLs. During the IOT&E, the Watchdesk needed more training and subject matter expert assistance to generate custom BEWLs. Finally, metrics personnel require more training to generate match statistics reports for external customers. The backlog of customer requests for these match reports is growing. Access to customized match statistics reports is important to DOD decision-makers who must relay the contributions ABIS v1.2 is making towards national security missions within and outside the DOD.

Reliability, Availability, and Maintainability (RAM)

This evaluation of RAM divided it into four subareas: Reliability, Availability, Maintainability, and Incident Maintainability. The last item examined the closure rate of trouble tickets that BIMA opened against the ABIS v1.2 during Phases 1 and 2.

During the IOT&E, no system aborts were scored during the IOT&E. While many EFFs occurred during the test, none caused ABIS to be down for more than 15 minutes because of unplanned downtime; there were 7.5 hours of planned downtime during the test. Phase 1 recorded 17 EFFs requiring system administrator support, but none of these prevented the system from processing requests for more than 15 minutes. Phase 2 had no system aborts or EFFs. While an EFF is not scored against MTBF if it is less than 15 minutes, a system problem that is

left unresolved would result in a mission failure or loss of an essential function and result in a critical failure.[21] Accounting for EFFs in the availability analysis, 11.62 hours of total downtime occurred during the test. This results in an overall worst-case availability point estimate of 97.2 percent with an 80 percent confidence interval of 97.2 percent to 98.8 percent. ABIS v1.2 met its operational availability requirement of 95 percent.

The root cause for the 7 minutes of unplanned downtime during Phase 1 was determined to be the main user portal being down. All BIMA operators use the Portal to access core functions. Both portals required a reboot, which fixed the problem. The point estimate for MTBEFF is 39 hours with an 80 percent confidence interval of 28 hours to 55 hours. ATEC should maintain the continuous evaluation process that is in place to monitor RAM through full deployment to ensure system stability would support the ABIS mission.

During normal operations, BIMA operators submit trouble tickets to a locally accessible trouble ticket tracker (ABIS Event Tracker) for direct input of problems as they experience them. During the test, System Administrators on-site at BIMA collaborated with BIMA operators to attempt to understand the problems, close the trouble tickets if possible, and open their own tickets using their proprietary tracker maintained at their Fairmont, West Virginia developmental facility.[22] The BIMA operators have no visibility into tickets after they enter them into the ABIS Event Tracker, and thus no way to identify similar tickets or to verify status of tickets. The Watchdesk previously was the Tier 1 support, and Examiners are adjusting to the new process of reporting their tickets to the System Administrator personnel.[23] The ABIS v1.2 System Administrators did not receive full training on BIMA daily tactics, techniques, and procedures prior to the IOT&E. Observations during the IOT&E indicate that biometric examiner problems were often misinterpreted.

Usability

The user responses to survey questions administered in person by a member of the ATEC test team is the primary basis for the usability assessment. Two sets of respondents were included in the surveys. The first set comprised ABIS Watchdesk operators responsible for managing the submission queues and interfacing with the external submitters. The second set comprised biometric and latent examiners responsible for manual biometric and latent match determinations and latent print processing. Experience levels of latent examiners ranged from 2 months to 9 years. Of 20 latent examiner respondents, the average years of experience at BIMA was 3 years while the median years of experience at BIMA was 2.5 years. Experience levels of biometric examiners ranged from 5 months to 8 years. Of eight biometric examiners surveyed,

---

[21] An EFF that is not resolved within 15 minutes is scored as a system abort.

[22] These system integrators acted as Tier 1 help support for BIMA Examiners. The Watchdesk was the official Tier 1 help desk for external customers. There is no single help desk structure describing ABIS v1.2 operations.

[23] For ABIS v1.0, BIMA provided system administrator support. For ABIS v1.2, the System Integrator under contract by the PMO provided system administration support. During the IOT&E, these personnel were still getting acclimated to daily BIMA operations.

the average years of experience at BIMA was 2.5 years while the median years of experience was 1.7 years.

The evaluation of overall usability looked at four subareas: training, documentation, user satisfaction with system operation, and Help Desk adequacy.

Table 4-2 shows the user responses for survey questions addressing overall usability using a 5-point Likert-like scale. Many respondents felt that more training would have been beneficial. PM Biometrics provided Watchdesk and Examiner training before Phase 1, at which time there were more BIMA personnel to respond. Between Phase 1 and Phase 2, Defense Forensics and Biometrics Agency laid off approximately 60 percent of the Examination staff. Therefore, there are fewer total responses after Phase 2, as shown in Table 4-3.

Only three of the eight Watchdesk personnel responded, so the results from the survey are not statistically meaningful. Watchdesk personnel were neutral to negative in their responses to surveys. Results in Table 4-3 suggest that the personnel believed that ABIS v1.2 provided less functionality than ABIS v1.0. Interviews with these personnel indicate apathy and low morale from the severe staff reductions and the length of time and effort taken to transition from ABIS v1.0 to ABIS v1.2. The Watchdesk has assumed new responsibilities in ABIS v1.2 including processing custom BEWLs. Watchdesk personnel need updated standard operating procedures to perform these new responsibilities.

Table 4-2. Usability Survey Results (Training) (Phase 1)

Question	Watchdesk		Examiners	
	Total	Percent Agree	Total	Percent Agree
Did the training meet expectations?	3	**33**	30	**40**
Did the depth of training material meet training needs?	3	**33**	30	**40**
Would additional training be beneficial?	3	**33**	30	**63**

In addition to the survey results shown in Table 4-2, system ease of use and the degree to which BIMA operators felt they could easily use the system to perform their tasks was assessed. Table 4-3 demonstrates that the Web Portal, used by both the Watchdesk and the Examiners was easy to navigate. However, the examiners did not find the overall usability of ABIS v1.2 to meet expectations. Table 4-4 focuses on those tools used only by Examiners. Examiners expressed less confidence in the ability for ABIS v1.2 to meet their needs and are concerned about lost functionality.

Table 4-3. Usability Survey Results (Ease of Use) (Phase 2)

Question	Watchdesk		Examiners	
	Total	Percent Agree	Total	Percent Agree
Was the web Portal easy to navigate?	3	**66**	8	**50**
Did the web Portal meet your expectations?	3	**66**	8	**50**
Did the DoD ABIS v1.2 web portal provide no loss in functionality when compared to DoD ABIS v1.0?	3	**33**	8	**38**
Are you confident in the results provided by DoD ABIS v1.2?	3	**66**	8	**25**
Does DoD ABIS v1.2 improve your daily productivity?	3	**66**	8	**38**

Table 4-4. Usability Survey Results (Ease of Use for Examiner Tools) (Phase 2)

Question	Number of Responses					Summary	
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean Response	Median Response
Was the Tenprint examiner Workstation(TEW) easy to navigate?	0	0	2	4	1	Neutral	Agree
Did the TEW meet your expectiations?	0	0	2	4	1	Neutral	Agree
Did the DoD ABIS 1.2 TEW provide no loss in functionality when compared to DoD ABIS 1.0?	0	1	3	3	0	Neutral	Neutral
Was the Latent Examiner Workstation(LEW) easy to navigate?	0	2	0	4	1	Neutral	Agree
Did the LEW meet your expectiations?	0	2	0	4	0	Neutral	Agree
Did the DoD ABIS 1.2 LEW provide no loss in functionality when compared to DoD ABIS 1.0?	0	1	2	3	0	Neutral	Neutral
Was the Facial Examiner Workstation(FEW) easy to navigate?	0	0	1	3	1	Neutral	Agree
Did the FEW meet your expectiations?	0	0	2	2	1	Neutral	Agree
Did the DoD ABIS 1.2 FEW provide no loss in functionality when compared to DoD ABIS 1.0?	0	1	2	2	0	Neutral	Neutral

Help Desk

This evaluation looked at two Help Desk areas. The first area is help desk support for external customers; the second area is help desk support for BIMA operators, including the Watchdesk and examiners.

BIMA operators expressed concerns that their problems are not accurately logged in the PMO trouble ticket system. The PM Biometrics should ensure that adequate training for the System Administrators in daily BIMA tactics, techniques, and procedures. This would better prepare the System Administrators to accurately capture problems and raise them according to urgency to higher Tiers for fixes. BIMA should assess whether sufficient numbers of trained System Administrators are available to support daily operations. Additionally, PM Biometrics should provide a better tracking mechanism between the two trouble ticket systems so that operator problems are resolved transparently.

This page intentionally left blank.

Section Five
Survivability

ABIS v1.2 is not secure from a cybersecurity perspective. The cybersecurity evaluation examined the security posture of server components hosted at the Criminal Justice Information Services division in Bridgeport, West Virginia, and the user-facing components at BIMA. The evaluation examined four criteria: the ability to protect against unauthorized penetration of the ABIS, the ability to detect when intrusions and exploits occur, the existence of adequate and appropriate system and personnel reaction to intrusion attempts, and the ability to restore normal system operations after a disruption.

A total of 102 Category I cybersecurity vulnerabilities were discovered the cooperative assessments from March 2014 to May 2014. In August 2014, the Army Threat System Management Office conducted a 5-day adversarial assessment with threat-representative objectives that included attempts to deceive, deny access, disrupt operations, eavesdrop, evade detection, mislead or influence administrators through misinformation, and illicitly control and manipulate system components and users. Specific findings are in the classified annex.

This page intentionally left blank

Section Six
Recommendations

DOT&E recommends that the Army address the following issues prior to FOT&E:

Operational Effectiveness

- Complete a full interoperability certification for all interfaces.
- Verify that custom biometrically-enabled watchlist consumers can use ABIS to support missions requiring local watchlisting.
- Finalize and document standard operating procedures for correcting identity crosslinks.
- Assess the ability to repair non-standard submissions during the FOT&E, including evaluating time to repair submissions, the adequacy of tools and procedures, and the relative proportions of submissions requiring repair.

Operational Suitability

- Maintain the continuous evaluation process to monitor RAM through full deployment.
- Assess whether sufficient numbers of trained system administrators, metrics personnel, and personnel for other critical support functions are available to support daily operations.
- Resolve stability problems with the CDS while ensuring that the CDS remains capable of preventing cyber-attacks across the NIPRNET/SIPRNET gateway boundary.
- Improve the quality of training, training aids, and other system documentation for the users.
- Develop a system for cataloging, sorting, searching, and monitoring trouble tickets that is accessible to all users and reduces redundancy in tracking and reporting of deficiencies.

Survivability

- Verify correction of vulnerabilities identified in the IOT&E.
- Complete a cooperative cybersecurity assessment of the ABIS v1.2 system before the FOT&E and an adversarial cybersecurity assessment during FOT&E.
- Address the additional recommendations regarding cybersecurity detailed in the classified annex.