

Event Report compiled and published by the Biometrics Identity Management Agency
March 2011

Table of Contents

Introduction	3
Purpose of the Event	3
Event Recap	3
2011 Biometrics Collaboration Forum Agenda	4-5
Session Summaries	6
International Biometrics Data Sharing	6-8
DoD Biometrics Enterprise Architecture: As-Is and To-Be	8-10
Biometrics on the Border	10-11
USMC Identity Operations Strategy	11-13
Marine Corps Afghanistan Handheld Biometrics Field User Evaluation	13-16
Biometrics Training Update	16-17
DoD Biometrics Capstone Training Strategy	17-18
DoD Biometrics CONOPs Revisited: The COCOM Perspective	18-20
DoD ABIS Present and Future	21
Operational Metrics	22-23
The Road from a Quick Reaction Capability to a Program of Record	23
Leveraging Biometrics to Create Business Efficiencies, Effectiveness, and Accuracy	23-24
Biometric Equities for the Identity & Privilege Management Working Group (IPvMWG) Roadmap	24-25
Credentials Part I & II	25-26
National Institute of Standards and Technology Identity Program Update	26-27
Biometrics Enterprise Requirements Strategy	27
DoD Identity Resolution Collection Management	28-30
Intelligence Requirements for NATO Standardization Agreement (STANAG)	30-31
DoD Biometrically-Enabled Watch List Discussion	31-32
Biometrics Collaboration Forum Attendee List	33-42
Acronym List	43-45

Introduction

Purpose:

The purpose of the 2011 Biometrics Collaboration Forum (BCF) was to integrate the community of biometrics users within the Department of Defense (DoD) and affiliated agencies. The event was not designed as a series of lectures or updates, but as a collaborative event designed to further biometrics in the DoD.

Forum Objectives included:

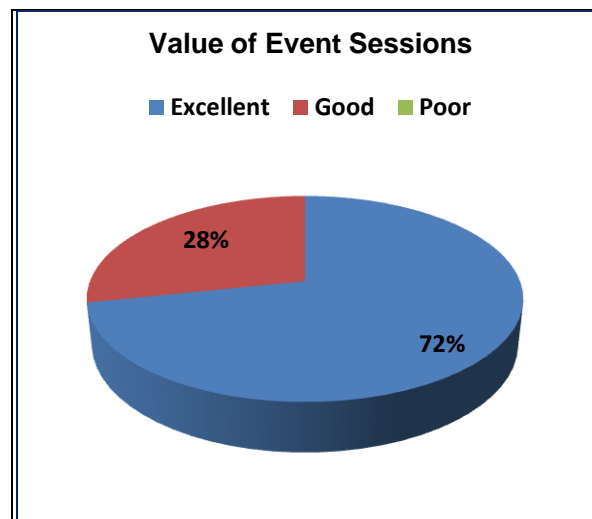
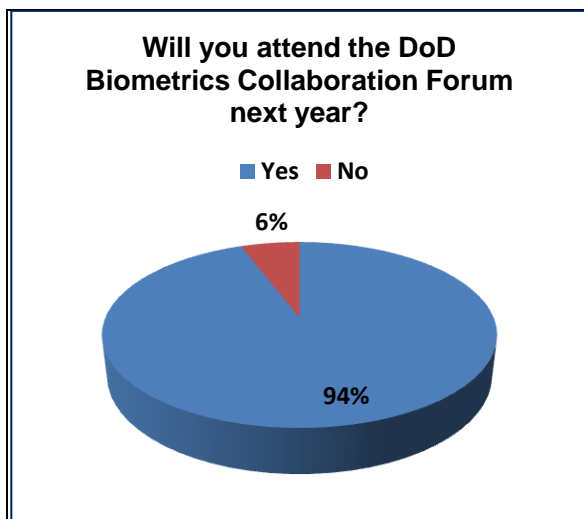
- ▶ Discussing the status of biometrics endeavors across the DoD
- ▶ Collaborating to identify the highest priority issues in the various elements of biometrics initiatives
- ▶ Integrating members of the DoD biometrics community to help solve these issues

This Forum Report is the summation of the progress made toward those objectives and provides the way ahead for continued collaboration.

Event Recap:

Over 290 participants attended the 2011 Biometrics Collaboration Forum, representing more than 140 organizations from throughout the DoD, Federal Government, Multinational and Industry Partners, and Academic communities.

Feedback from forum participants was overwhelmingly positive, with 94% expressing their desire to participate in next year's event. Topic relevancy, presentation method and delivery, and the overall value of the sessions were also highly rated.



Participant Commentary:

- ▶ "One of the better events I have attended. Keep the momentum. Keep things actionable and inform stake holders of process on action items."
- ▶ "Great content, learned a lot, very valuable. Was able to network and make valuable contacts for home station training support."
- ▶ "Outstanding, informative, engaging general and breakout sessions. Enjoyed it a lot."

2011 Biometrics Collaboration Forum Agenda

Date / Time	Plenary Session - Charlotte Mecklenburg Hall				
25 JAN 9:00-9:15	Welcome and Introduction of the BIMA Director Opening Remarks - Dr. Thomas Killion				
9:15-9:45	Keynote Address - MG Bennet S. Sacolick, Commanding General U.S. Army John F. Kennedy Special Warfare Center and School				
9:45-10:00	Session Break				
Date / Time	Strategic and Capabilities Integration Ardwell Room	Biometrics Training, Metrics, and Operations South Carolina Hall	Combatant Command Support North Carolina Hall	Friendly Biometrics Graves Hall	Classified Sessions Duke Energy Building
10:00-12:00		Biometrics Training Update	DoD Biometrics CONOPs Revisited: The COCOM Perspective	Friendly Biometrics Track Introduction Leveraging Biometrics to Create Business Functions Efficiencies, Effectiveness, and Accuracy	
12:00-1:00	Lunch				
1:00-3:00	DoD Biometrics Enterprise Architecture: As-Is and To-Be	DoD ABIS - Present and Future		Biometrics Equities for the Identity & Privilege Management Working Group (IPvMWG) Roadmap	Intelligence Considerations for DoD Biometrics CONOPs
3:00-3:15	Session Break				
3:15-5:30	Biometrics on the Border	<i>Continuation Session</i> DoD ABIS -Present and Future		Friendly Biometrics Credentials Part I	DoD Identity Resolution Collection Management

Date / Time	Strategic and Capabilities Integration <i>Ardwell Room</i>	Biometrics Training, Metrics, and Operations <i>South Carolina Hall</i>	Combatant Command Support <i>North Carolina Hall</i>	Friendly Biometrics <i>Graves Hall</i>	Classified Sessions <i>Duke Energy Building</i>
26 JAN 8:30-10:00	International Biometrics Data Sharing	USMC Identity Operations Strategy	DoD Stakeholder Requirements	National Institute of Standards and Technology (NIST) Identity Program Update	
10:00-10:15	Session Break				
10:15-12:00	<i>Continuation Session</i> DoD Biometrics Enterprise Architecture: As-Is and To-Be	Developing an Operational Metrics Capability	<i>Continuation Session</i> Biometrics Stakeholder Requirements	Friendly Biometrics Credentials Part II	NATO Standardization Agreements (STANAG) Discussion
12:00-1:00	Lunch				
1:00-3:00	<i>Continuation Session</i> Biometrics on the Border	DoD Biometrics Capstone Training Strategy	The Road from a Quick Reaction Capability to a Program of Record	Biometrics Enterprise Requirements Strategy	Biometrically - Enabled Watch List (BEWL) Standard Review
3:00-3:15	Session Break				
3:15-5:30	Marine Corps Afghanistan Handheld Biometrics Field User Evaluation	<i>Continuation Session</i> DoD Biometrics Capstone Training Strategy	<i>Continuation Session</i> The Road from a Quick Reaction Capability to a Program of Record		<i>Continuation Session</i> Biometrics Enabled Watch List (BEWL) Standard Review
27 JAN 9:00-11:00	Topic Closeout - Plenary Session				
11:00-11:15	Session Break				
11:15-12:00	Closing Remarks - Dr. Thomas Killion				

Session Summaries

International Biometrics Data Sharing

Session Leads:

Mr. Tony Demestihias, Biometrics Identity Management Agency (BIMA) Policy Branch
Mr. Mark Singer, BIMA Policy Branch

Session Objectives/Issues:

The session objective was to provide an overview of current international biometric data sharing efforts. International biometric data sharing programs within the DoD are still in their infancy as the United States, its allies, and partner nations continue to fully appreciate the power of biometrics and how sharing such data can protect not only men and women in uniform, but also our homelands. As such, this session focused on providing an overview of international data sharing efforts as well as future initiatives.

The main constraint with international data sharing efforts is the technical challenges that prevent full interoperability between the respective countries. This session provided the opportunity to update the current status of developing the technical interfaces and caveats required to embark upon international biometric data sharing efforts. Finally, the session provided an overview of the role the Executive Agent (EA) has in shaping international biometrics data sharing agreements as well as the technical support provided by the EA.

Topic Summary:

Due to the technical challenges associated with international biometric data sharing, much of the discussion focused on the technical feasibility of international biometric data sharing and what needs to be done to obtain the necessary interoperability between the United States and its partner nations. The current status of the development and approval of a caveat, to ensure partner nation biometric data is not inadvertently shared with non-approved entities, was thoroughly discussed, including the possible standardization of such a caveat.

With the expected increase in sharing of biometric data with foreign partners, as well as domestic, concerns were raised regarding the size and capability of DoD ABIS to handle a large capacity of transactions as well as storing an increased amount of biometric files. These concerns were discussed and flowed into the larger requirements discussion which spanned across several sessions at the forum.

Finally, the session discussed policy and organizational impediments to sharing international biometric data, particularly through the COCOMs. Some COCOMs commented regarding the lack of support from COCOM leadership while others attributed sharing difficulties with policy impediments or gaps.

Findings and Insights:

Throughout the discussion, several findings and insights appeared that will shape the subsequent recommendations and way ahead. It became apparent that there is a need for a single point of contact for COCOM engagement when it comes to international biometric data sharing efforts. It was recommended that an office or individual be designated as the point of contact for COCOMs to engage with during efforts to develop and implement international sharing initiatives, regardless of whether that office or individual resides within the Office of the Under Secretary of Defense for Policy (OUSD(P)), the Principal Staff Assistant for Biometrics

(PSA), or the EA. Additionally, it is apparent that based upon differing host nation cultures, laws, norms, policies, etc. that special handling instructions will be imperative for each subsequent international data sharing agreement. One solution will not fit all partner nations and DoD components and BIMA must have the flexibility to adapt to data sharing requests from different partner nations. Finally, the group came to the consensus that there is no direction or overarching strategy guiding international data sharing efforts. While Combatant Commands have the authority to enter into sharing agreements with those partner nations within their area of responsibility, OUSD(P) also has commenced data sharing efforts with partner nations. A plan of action or even greater coordination between the COCOMs and OUSD(P) is needed to ensure there is no overlap or redundancy, and synchronize efforts.

Next Steps and Timeline:

The BIMA Policy Branch will continue its ongoing efforts to help identify, analyze, and close COCOM policy gaps that limit the collection, storing, and sharing of biometric data with partner nations within their area of operations. Another ongoing step needed to address the issues raised by the session attendees is to educate COCOM leadership regarding the benefits derived from deploying biometric technologies and the subsequent identification tools within their area of operations. Any efforts made to educate COCOM leadership on the benefits of biometrics will likely pay dividends in future support for the use of biometrics.

Another step that emerged from the session is to work with the BIMA Requirements Branch / Biometrics Requirements Working Group and the COCOMs to articulate future requirements to initiate and support international biometric data sharing efforts. In the next 90 days, working through the BRWG, the BIMA Requirements Branch can fully vet and analyze COCOM needs, thus developing a well articulated and valid requirement to help spur sharing agreements with partner nations.

A need highlighted during the session was a repository or matrix that captures current international data sharing agreements throughout the United States Government. This was requested as a means to determine what agreements are already in place, prevent duplication of effort, and identify opportunities to expand current agreements to include biometric data. A repository or matrix can also capture the unique norms, policies, laws, and cultures encountered when working with a partner nation during the development of a sharing agreement. This will provide any office developing an agreement with a better understanding of partner nation constraints before negotiation. The BIMA Policy Branch hopes to develop such a tool within the next 180 days.

Finally, it was determined that a survey distributed to the COCOMs and Biometrics Enterprise Stakeholders to capture current policy gaps is needed. This will allow those DoD components engaged with biometrics to highlight the areas of difficulty that require a policy to close a gap. The BIMA Policy Branch expects to develop and distribute a survey within the next 30 days.

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Solicit COCOM input on international biometric data sharing needs and work to turn these needs into	Biometrics Requirements Working Group	30/60 days	BIMA Requirements Branch BIMA Policy Branch	

requirements that are well articulated				
Development of a matrix that captures current international biometric data sharing agreements throughout the United States Government		180 days	BIMA Policy Branch	
Distribution of a Biometrics Policy Survey to the COCOMs and other stakeholders to capture concerns / issues / needs / perspectives	Biometrics Policy Working Group	30 days	PSA OUSD(P) BIMA Policy Branch	

DoD Biometrics Enterprise Architecture: As-Is and To-Be

Session Leads:

Mr. Giovanni Demonte, BIMA Architecture Branch
 LTC Kevin Woods, BIMA Architecture Branch
 Ms. Vanitha Khetan, BIMA Architecture Branch
 Mr. Adam Pannone, BIMA Architecture Branch
 Ms. Sarah Rose, BIMA Architecture Branch

Session Objectives/Issues:

The overall objectives of the sessions were to discover, connect and align to other biometric architectures within the DoD, Federal Agencies and other relevant partners. Specific areas of discussion included classified architectures, friendly biometric architectures, Cross-Domain Issues, 2025 Biometrics Enterprise Architecture, decision support, and future focus of the enterprise.

Topic Summary:

Discussion Points -

The first session centered on the topics of architectures created by the BIMA Architecture Branch and their progress for Army / DoD approval. The second session was targeted as a structured information gathering session on topics that influence the Biometrics Enterprise Architectures. The discussion points were as follows:

- ▶ Improving coordination among the BIMA Capabilities Integration Division branches: A CENTCOM rep noted their input into architecture direction can be gleaned from the requirements they submitted. He relayed that many of the requirements submitted have not been implemented; they don't have visibility for the status of the requirement, how it has progressed and what the adjudication was. Others spoke up, echoing the CENTCOM representative's comments.
- ▶ Governance driven compliance for biometric capability within DoD:

There was a discussion surrounding the regulatory authority that BIMA should possess and doesn't currently. BIMA endorsed standards should be regulated for compliance through DoD policies. This will allow us to achieve the elusive "seamless interoperability" between agencies that has been an objective for the enterprise. Policies and effective governance structures are lacking for enforcing standards. Architecture can be used to describe the necessary governance framework based off of DoD models.

- ▶ Biometrics is intrinsically related to Operations Security (OPSEC) and Information Assurance (IA), however this alignment is not clearly defined. Members of the session raised the issue of the OPSEC dependencies in the process of approving biometric capabilities.
- ▶ The DoD Biometrics Enterprise will change focus from primarily being a 'Wartime' need to 'Peacetime' activities. The use and application of biometrics during wartime was limited to supporting the war-fighting mission area. With the expectation of war activities declining in the future, the scope of biometric use and application will expand to other mission areas especially into the business mission area. The need for using DoD's biometric capability to support friendly business mission areas, such as identity and privilege management will be a large shift in focus. Friendly biometrics is not clearly defined for biometric scope. The enterprise should capture friendly definition / categories and the application of biometrics to support friendly activities.

Findings and Insights:

- ▶ There exists a need for a high-side Biometrics Enterprise Architecture. The architecture description is limited in depth of coverage in the interest of keeping the architecture unclassified. But much is lost, and there will be more lost in the future as the focus of enterprise becomes more far-reaching and not restricted to DoD. Therefore the need to develop a classified EA to depict the necessary information to support strategic decision making and analysis is emerging. The INSCOM EA development could directly contribute to the classified Biometrics Enterprise Architecture.
- ▶ Lack of community consensus on existing data-sharing efforts. There is still a need to continue socializing and representing the biometric architecture capability at biometric communities.
- ▶ Need for improved Biometrics for personnel recovery operations.

Next Steps and Timeline:

Next Steps -
Working Group Meetings

- ▶ Increase stakeholder involvement for Quarterly Meetings.
- ▶ Component architecture feedback.
- ▶ DBEKS replacement plan.

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Integrate Requirements into As-Is EA	BIMA Collaboration	60 days	BIMA Architecture Branch and Requirements Branch	
Validate As-Is	Remote	90 days	BIMA Architecture	CENTCOM

Architecture with CENTCOM	Collaboration		Branch	
Validate As-Is Architecture with SOCOM	Remote Collaboration	90 days	BIMA Architecture Branch	SOCOM
Capture Biometric capability for Coast Guard and Border Patrol operations	Remote Collaboration	60 days	BIMA Architecture Branch	Customs and Border Protection
Biometrics Glossary CR submission	Remote Collaboration	10 days	BIMA Architecture Branch	

Biometrics on the Border

Session Leads:

Mr. William Vickers, OUSD(I) / TCA
Mr. Antonio Trindade, Associate Chief Border Patrol
LTC Joe Lopez, USNORTHCOM J34

Session Objectives/Issues:

This session leveraged lessons learned from operational areas and applied them to current border security issues, examining the political, social, technology, operations and data movement and analysis to provide a practical collaborative solution.

Topic Summary:

Discussion Points

- ▶ The DoD has broad experience in using biometrics and other sensors to contribute to secure borders, Ports of Entry and cities. The DoD Biometrics community including BIMA, OUSD (P), and SOCOM has previously partnered with DHS and CBP to look at how biometrics can enhance border security.
- ▶ Day one:
 - Highlighted the seriousness of the Southwest border problem set along with briefs of previous and ongoing programs.
 - Discussed pilots and articulated the need for a limited operational demonstration of current technology to gather metrics and lessons learned to determine scope of problem to determine requirements.
- ▶ Day two:
 - Presented a conceptual architecture and two scenarios.
 - ▶ Fixed site – with supporting infrastructure.
 - ▶ Austere/remote area – lack of infrastructure.
 - Discussed business rules within DoD and interagency partners.
 - Discussed technology transfer from DoD to CBP.

Findings and Insights:

- ▶ Concurrence of Operational Objectives.
- ▶ Challenges with interagency coordination.
- ▶ Clearly defining baseline and understanding of the DoD perspective / objectives.
- ▶ Incremental expansion of existing technology baseline and concepts.
- ▶ Maintaining strong coalitions and resource commitments.
- ▶ Senior leadership buy-in.

Next Steps and Timeline:

- ▶ Meet/coordinate with Stakeholders.
- ▶ Draft timeline.
- ▶ Identify authorities.
- ▶ Identify legal review.
- ▶ Develop CONOP.
- ▶ Identify Resource Requirements.
- ▶ Present to leadership / leadership buy-in.
- ▶ Execute operation / Tech Demo.

USMC Identity Operations Strategy

Session Lead:

Maj Frank Sanchez, HQ USMC

Session Objectives/Issues:

- ▶ The USMC lacks a coordinated and synchronized expeditionary Identity Operations (IdOps) capability to support identity dominance across the full Range of Military Operations (ROMO).
- ▶ The solution to this problem is a concept which leverages joint and organic capabilities, enabling the Marine Corps to fully integrate value added identity operations into all aspects of USMC operations and missions, to the maximum extent possible.
- ▶ The purpose of the USMC Identity Operations Strategy is the following:
 - Describes using IdOps to support Marine Corps operating concepts.
 - Provides a structure to integrate traditional and emerging DoD identity operations enablers.
- ▶ Drives identity dominance planning and guides resourcing to train and equip Marines to employ IdOps across the full ROMO.
- ▶ Illustrates potential gaps between current capabilities and the desired end state - attain and maintain identity dominance over the nation's adversaries while contributing to the national intelligence enterprise and ultimately homeland defense.

Topic Summary:

Discussion Points

- ▶ Operations Enduring Freedom and Iraqi Freedom
 - A largely anonymous enemy often hidden indistinguishable from the civilian population.

- ▶ Urgent operational requirements.
 - “Supplemental Funding” vs. “Base Budget.”
 - Moving from “ad hoc” to Programs of Record.
- ▶ Identity Operations
 - Emerging USMC Capability.
 - Biometrics + Forensics + Identity management.
- ▶ “[IDOPS is] a mission enabler for law enforcement, intelligence, force protection, counterinsurgency operations, humanitarian operations, site exploitation, physical security, and other mission sets.” (IdOps OIPT 011842Z Oct 10).

Findings and Insights:

To-Be USMC IdOps:

- ▶ Institutionalize Identity Operations in the Marine Corps.
 - Portfolio and Program Management.
- ▶ Planning, Programming, Budgeting and Execution System (PPBES).
 - Guidance and Doctrine.
- ▶ Unity of effort through Joint and Interagency collaboration.
 - Lean, lethal, agile expeditionary force.
 - Reduce duplication of effort and avoid unnecessary resource expenditure or utilization.
 - Enhance mission success.
- ▶ Integrate identity operations into Marine Corps operations and missions.
 - Denying anonymity to the adversary.
 - Protecting our assets, facilities and forces.
 - Contributing to the successful completion of Service and Joint missions.
- ▶ Robust and integrated use of IdOps across the full Range of Military Operations missions would significantly enhance safety, situational awareness and mission accomplishment.

Next Steps and Timeline:

Action	Forum	Deadline or Timeline	Lead Organization(s)	Comments
IdOps Strategy – Action Officer Staffing	USMC IdOps OIPT	02-04 November 2010	HQ USMC	Action Complete
O-6/GS-15 Level Staffing	Marine Corps Action Tracking System (MCATS)	Entered Staffing 21 December 2010	HQ USMC	Receiving Staff Comments
GO/SES Level Staffing	MCATS	TBD	HQ USMC	
Assistant Commandant of the		TBD	HQ USMC	

Marine Corps (ACMC) Signature				
IdOps Strategy Implementation Plan - Commence coordination/staffing	USMC IdOps OIPT	08-10 March 2011	HQ USMC	
O-6/GS-15 Staffing	MCATS	Late March 2011	HQ USMC	
GO/SES Staffing	MCATS	Early April 2011	HQ USMC	
ACMC Signature		TBD	HQ USMC	

USMC Biometrics Pilot

Session Lead:

MAJ Frank Sanchez, HQ USMC

Session Objectives/Issues:

To lean forward in providing a tactical biometric capability that supports Marines in Afghanistan and future Marine Air-Ground Task Force (MAGTF) Operations.

Topic Summary:

Situation

- ▶ Current biometric devices used (BAT/HIIDE) do not meet requirements for a tactical collection device.
- ▶ Multiple Urgent Universal Needs Statement (UUNS) / Joint Urgent Operational Needs Statement (JUONS) have been submitted over several years requesting an advanced device.
- ▶ JUONS requiring solution to BAT replication and data latency issues.
- ▶ J-8 Directed BIMA to develop solution to address these issues using existing technology/capabilities, and demonstrate for fielding approval.
- ▶ A Joint Analysis of Alternatives concluded the Secure Electronic Enrollment Kit (SEEK) is the best current device to meet requirements.
- ▶ BIMA/PP&O proposed pilot program was briefed to Marine Forces, Central Command (MARCENT).
- ▶ Commander, United States Marine Forces, Central Command (COMUSMARCENT) directs G-3 to go forward with program.
- ▶ LtGen Dunford – “This is the most promising development on biometrics in a long time.”

USMC / BIMA Methodology

- ▶ Leverage currently fielded COTS/GOTS solutions to deliver the required tactical biometric capability and responsive architecture **now**.
 - Work within DoD to leverage existing efforts (SOCOM, NCIS, Navy, NGIC, PM, etc.)
- ▶ Field a solution that will meet the majority of UUNS/JUONS requirements now while developing the long term solution.
 - 80% solution now is better than zero now.
 - Don’t sacrifice the entire capability awaiting the full capability.

- Support both battlefield and national security biometric efforts.
- ▶ Field a solution and enhanced architecture that allows information to be ingested in BAT, expands searchable records, provides feedback to the end user, and simultaneously reduces match time against DoD and interagency databases to support both battlefield and national security goals.

BAT/SEEK Bridge

- ▶ Capacity of ingesting 1,400 records into BAT per day (new encounters/tactical enrollments only).
 - Once ingested into BAT, same replication times apply as a direct BAT submission.
 - Mass enrollment operations would still utilize the BAT and not create an additional strain on the bridge.
 - Current capability could support 42,000 new enrollments per month.
 - Estimated only 2250-3000 SOCOM enrollments per month.
- ▶ Enrollments to be collected by the SEEK and ingested through the bridge are enrollments we are not receiving and sharing now.
 - Marines are not sufficiently enrolling individuals on patrol due to the lack of a tactical enrollment device that meets standards.
 - Currently, every encounter is a missed opportunity for enrollment.
- ▶ “The Databridge 1.0 was found to provide an acceptable confidence of meeting operational needs for ingestion of Combined Security Transition Command - Afghanistan (CSTC-A) and SEEK files.” (Source: PM DoD Biometrics Databridge Report March 2010).

Watchlist

- ▶ BIMA-WV is currently generating a Biometrically-enabled Watch List (BEWL) for the SEEK devices for SOCOM.
 - Signed IDS CDD contains the requirement for BIMA to provide the same service to the DoN.
- ▶ Currently Tier 1 & 2 only – updated every two weeks (~ 500 records).
 - Marine Corps would require Tiers 1, 2 & 4 updated weekly (~20,500 records).
 - ▶ BIMA will support this requirement.
- ▶ Watch list nominations originate in Afghanistan and are maintained by NGIC.
 - NGIC forwards the watch list to BIMA-WV for flagging in ABIS.
 - ABIS records are parsed to generate SEEK templates and posted on a BIMA server for updates to devices.
 - Watch list in ABIS is the same as in BAT.
- ▶ SEEK files submitted through the portal will always check against the latest DoD and FBI watch lists.
- ▶ Watch list currency will be equal to that of HIIDE.

Implementation

- ▶ USMC will get 10 SEEK II devices.
 - CENTCOM / II MEF's involvement in Pilot Program does not constitute the USMC's preferred replacement for the HIIDE. DOD PM Biometrics will go through normal procurement process in FY11 to replace HIIDE.
- ▶ Portal software.
 - GOTS software provided at no cost by SOCOM.
 - BISA Architecture and satellites provided by BIMA (including 1yr bandwidth).
 - SEEK and VSAT provided by USMC.
- ▶ Server to run web-based portal – can be installed and operated anywhere.
 - Requires operational support.
- ▶ As with any system, training will be required.
 - Mobile training teams provided by SOCOM, train-the-trainer.
 - NCIS training support at Camp Leatherneck.
 - Existing Biometric System Administrators (BSA)**.
- ▶ Identify personnel to upload files and perform watch list maintenance.
 - Leverage BSAs currently updating Pier, HIIDE watch lists.

Advantages

- ▶ Provides Marines the tactical handheld they've required for years - now.
- ▶ Eliminates classification issues of plugging UNCLAS handhelds into BAT.
- ▶ Follows established DoD Directives, guidance, and standards.
- ▶ Allows matches against watchlists, DoD, FBI, and DHS biometric databases.
- ▶ Information collected will be ingested into BAT for analysis/matching.
- ▶ Open architecture will allow for notification of match/no-match to Intel Community (IC) and user within 5-22 minutes using existing networks (NIPR).
 - Current architecture latency issues result in delayed notification to IC.
 - Architecture will allow for auditing of records to ensure submission.
 - Avoids current BAT replication issues resulting in lost records.
- ▶ Architecture can support any future biometric device that conforms to standards.
- ▶ Supports senior leadership guidance to maximize the use of current capabilities and reduce the impact of legacy systems shortcomings.
- ▶ Supports senior leadership direction to increase biometric enrollments in Afghanistan.

Findings and Insights:

Current Status of Pilot

- ▶ Oct 2010- A Co. 1/8 Marines took custody of (10) SEEK II Handhelds.
- ▶ Immediate need for FSR/FSA to support equipment, ingest into portal, watchlist downloads, software issues.
 - Limited FSA/FSR knowledge of SEEK system.
- ▶ Once up and running approx 40 enrollments submitted during first operation with a few Tier hits.
 - As of o/a 15Jan11- 460 enrollments through SOCOM Portal.

- ▶ Capabilities of handheld for outside the wire transmission has been limited.
 - Currently shipping BGAN for use of downloading outside FOB to evaluate capability to transmit and confirm within 5-22 minutes.
- ▶ 30 day assessment-Issues with training, FSR support, BAT Bridge.
- ▶ Awaiting Marine Corps Operational Test and Evaluation Activity (MCOTEA) official assessment.
- ▶ 3/2 to replace 1/8. Moving forward with training during pre-deployment training, Soldier as an FSE course attendance; SEEK equipment to use prior to deploying.
 - Unit gain confidence in gear and integrate into modus operandi-.
- ▶ As of Dec10, PP&O (POE) Expeditionary Branch requested support for Marine Expeditionary Units (MEUs) deploying and in need of a tactical biometrics device.
 - Specifically requested SEEK device.
- ▶ PPO IdOps agreed to support MEUs / Special Operations Training Groups (SOTGs) with SEEK devices in order to evaluate tactical capabilities/limitations across expeditionary mission.
 - Use during Visit, Board, Search, and Seizure (VBSS) missions, other MEU missions-will help support USMC IdOps Strategy 2020 assumptions/capabilities/limitations.
- ▶ MEUs to request MCOTEA official evaluation of SEEK devices in support of missions.
 - Formal, impartial evaluation by Marine Corps Center for Lessons Learned (MCCLL).

Next Steps and Timeline:

- ▶ Continue to evaluate the pilot-its capabilities and limitations and help mold/advocate the current and future need for tactical biometrics ISO Marine Corps expeditionary missions.
- ▶ Field user evaluation will be conducted to identify areas for potential enhancement in future phases.

Biometrics Training Update

Session Leads:

LtCol Tom Pratt – BIMA Military Operations Branch
Mr. Mike Kershner – BIMA Military Operations Branch
Mr. Dennis Branson – BIMA Military Operations Branch
Mr. Nick DiPiazza – BIMA Military Operations Branch
Mr. Chris Melton – NSTID, USAICoE
Mr. David Tyler – TCM-BF

Session Objectives/Issues:

Update the biometrics training community of interest on training developments since the last Biometrics Training Working Group meeting (October 10, 2010) and identify future actions required to improve biometrics training of the force.

Topic Summary:

Discussion Points -

- ▶ The appointment of a proponent (USAICoE) for biometrics is a positive step.
- ▶ Much remains to be done, especially in the realm of leader training.

Findings and Insights:

- ▶ The proponent should assume the lead for Army biometrics training.
- ▶ BIMA should transition current training efforts to the Army proponent and shift to a support role in biometrics training.
- ▶ BIMA should move forward on joint training and senior leader education.
- ▶ Recommendations.
 - That BIMA continue to provide training leadership at the joint level.
 - That BIMA continue to try to educate senior leaders on biometrics.

Next Steps and Timeline:

Next Steps -

- ▶ Next Biometrics Training Working Group meeting will be at Fort Huachuca 22-24 March to facilitate the transition of training efforts to the proponent (USAICoE).
- ▶ The Commander's Guide to Biometrics in Afghanistan should be followed by a guide oriented to general application around the world.

Timeline – Transition of Army training efforts to the proponent should be complete by 1 July.

DoD Biometrics Capstone Training Strategy

Session Leads:

Mr. Joseph Dunleavy, BIMA Requirements Management Branch
Mr. Raymond Jones, BIMA Requirements Management Branch
Mr. Michael Bishop, BIMA Requirements Management Branch

Session Objectives/Issues:

Present a recommended path forward for developing standardized biometrics doctrine and institutional training at all levels across the Services and Department of Defense for users / operators and junior and senior leaders.

Topic Summary:

- ▶ Discussed the draft DoDI 8521.TT which identifies and specifies key roles and responsibilities for a Single Manager for Military Biometrics Training.
- ▶ Discussed the primary focus of the draft DoDI; that of formalizing requirements for a capstone level DoD Biometrics Training Working Group.
- ▶ Reviewed a draft or straw man charter for the working group.

Next Steps and Timeline:

- ▶ Internally staff the draft DoDI 8521.TT, Single management responsibilities for Military Biometrics Training.
- ▶ Staff the draft DoDI with the services, via a DoD Staffing form/mechanism.
- ▶ Hold the first working group meeting to flush out and formalize the group's charter.

Timeline:

- ▶ Complete internal staffing of DoDI by EOM February.
- ▶ Submit draft DoDI for DoD/Joint Staff/Service staffing in mid March.
- ▶ Convene working group by EOM February – flush out charter and members.
- ▶ Convene first working group session to develop way ahead and address issues.

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Internal DoDI 8521.TT Staffing	BIMA Staff	Complete internal staffing by end of February 2011	BIMA Requirements Management Branch	All BIMA Divisions and Branches
Service and DoD staffing of DoDI8521.TT	Staffing throughout and across DoD	Start Department staffing by Mid-March 2011	BIMA Requirements Management Branch	All BIMA Divisions and Branches
Establish the DoD Biometrics Training Working Group per draft DoDI	DoD Biometrics Community	Mid to late February 2011	BIMA Requirements Management Branch	All BIMA Divisions and Branches

DoD Biometrics CONOPS Revisited: The COCOM Perspective

Session Leads:

Mr. Bill Phillips, Acting Chief, BIMA Plans Branch
Mr. Benji Hutchinson, OUSD(I) Biometric, Forensic and Identity Intelligence

Session Objectives/Issues:

The Capstone Concept of Operations for DoD Biometrics was published in November 2006 with the dual intent of establishing the Biometrics Process and providing a framework for operators and administrators to incorporate biometrics into their operational plans and business processes. As the DoD Biometrics Enterprise continues to evolve in terms of both the development and employment of biometrics capabilities, it is necessary to review, validate and update the CONOPS.

The intent of this session was threefold:

- ▶ Receive input from COCOMs on their employment of biometrics capabilities.
- ▶ Compile best practices and lessons learned to update vignettes contained in the CONOPs and allow COCOMs to learn from one another.
- ▶ Discuss specific recommendations for updating the CONOPS.

Topic Summary:

This session was conducted as a panel discussion with representatives from seven COCOMs as panel members (USSOCOM, USPACOM, USSOUTHCOM, USNORTHCOM, USAFRICOM, USEUCOM and USCENTCOM). Prior to the BCF all panel members were provided with a template to use in preparing their briefs, and each COCOM was allocated 15 minutes during the

session to brief their slides and field questions from the audience. While each COCOM had their unique perspectives and concerns, there were several common themes that emerged.

Common Themes:

- ▶ There was a general recognition that as operations in the CENTCOM AOR draw down, we need to change the way in which we currently view biometrics collections. The permissive environment will shrink considerably, and the future will be largely “by, with and through” partner nations.
- ▶ Central to the “by, with and through” philosophy will be building partner nations’ capabilities in order to facilitate the sharing of biometric data. In some areas there is a rapidly closing window of opportunity as other nations are making a push to offer the same capabilities.
- ▶ In order to institutionalize biometrics as an enduring capability, there must be a focused effort to educate senior leaders on the benefits of employing biometrics capabilities. Specifically, leaders need to understand biometrics beyond what they’ve been exposed to in the CENTCOM AOR.
- ▶ Related to a need for senior leader education, COCOMs would appreciate more specific guidance in terms of where biometrics should sit in their commands (J-2, J-3, J-8), and on specific authorities they have in terms of building partner nation capacity and entering into data sharing agreements.
- ▶ The DoD cannot do it alone; there needs to be emphasis placed on developing, maintaining and leveraging interagency relationships and partnerships.
- ▶ There exists hesitancy among partner nations to share biometrics data out of concerns about who the U.S. will turn around and share this data with.
- ▶ Need to establish programs of record to ensure funds don’t go away as OCO dollars dry up. Right now SOCOM has the only program of record.

COCOM Discussion Points –

- ▶ USSOCOM
 - USSOCOM succeeds by working “by, with and through” others (partner nations and geographic COCOMs).
 - USSOCOM biometrically enrolls and vets all foreign nationals who are receiving training on SOF TTPs. There is currently no programs in place outside of SOCOM to track who is receiving other U.S. funded training (SOCOM recommended that this be emphasized in the CONOPS).
 - Raised issue of need to store data that might be sensitive due to the nature of its collection (specifically regarding operations in USAFRICOM).
- ▶ USPACOM
 - PACOM conducts very few collections on their own – majority done through host nation entities (specifically law enforcement organizations, but some customs and immigration).
 - Currently have a massive amount of paper cards (800,000 from the Philippines alone) that need to be digitized and stored in a searchable format. Other nations (China, Japan) are offering to help develop this capability, so if we don’t do it, they will.
- ▶ USSOUTHCOM
 - SOUTHCOM is not fighting a war – focus is on building partnerships with host nations and interagency partners.
 - Success stories (Dominican Republic, Columbia).

- SOUTHCOM Biometrics CONOPS is in draft status – should be out for coordination by the end of February 2011.
- ▶ USNORTHCOM
 - Biometrics currently sits in the J-34.
 - NORTHCOM owns a lot of terrain, but no troops.
 - Focus was on access control, but has shifted significantly to the Southwest border.
 - Waiting for Mexico to request our assistance in developing their biometrics capabilities.
- ▶ USAFRICOM
 - Largely focused on nation building – highly political environment.
 - Attempting to use SOCOM as a model to biometrically enroll / vet all foreign nationals receiving U.S. funded/sponsored training.
 - View Biometrics / Forensics / DOMEX as three components of a single discipline.
- ▶ USEUCOM
 - Lot of emphasis on counter network operations (Counter Narcotics, Human Trafficking, Arms Proliferation).
 - Strategy of active security – enabling the first line of defense for the homeland through engagements to promote regional security and stability.
 - Would like to see a holistic approach to biometrics / BEI / Identity.
- ▶ USCENTCOM
 - Provided a brief on the Last Tactical Mile.
 - Discussed the need to move at the speed of warfare in developing capabilities.

Findings and Insights:

The primary insights that came out of this session are addressed in the “common themes” section above. These are issues and concerns that were shared across the COCOMs, and will serve as points of focus in drafting the updated CONOPS.

The final recommendation is that an update of the DoD Capstone CONOPS for biometrics is warranted.

Next Steps and Timeline:

Next Steps -

- ▶ Reach out to all session participants and audience members to collect notes and thoughts from the session that may not have been present.
- ▶ Conduct the “kick-off” meeting to develop scope of the DoD Biometrics CONOPS.
- ▶ Working Group to develop timeline for writing the DoD Biometrics CONOPS strawman.

Timeline –

- ▶ TBD: Develop DoD Biometrics CONOPS draft and staff across the Biometrics Enterprise.

DoD ABIS Present and Future

Session Leads:

Mr. Sam Aloï, Chief, BIMA Biometric Operations Branch
Mr. Neal Gieselman, BIMA Lead Systems Engineer
Ms. Lauren Cooney, BIMA Examinations Services Lead

Session Objectives/Issues:

The session objectives / issues were presented in a two hour block consisting of three sections followed by a two hour block consisting of a question and answer session with the biometric community of interest. The first section discussed DoD ABIS current and future considerations including the Afghan 1000, DHS Memorandum of Agreement, Afghan ABIS, etc. The second section focused on card scanning tools, forensic workbench tool, the Biometrically Enabled Watch List, and accuracy across the modalities. The third section provided an update of our latent backlog mitigation plan as well as latent processing with regards to forward latent matching.

Topic Summary:

Discussion Points - The focus of DoD ABIS current and future considerations is reliant on system sizing issues. This is currently being addressed in coordination with PM DoD Biometrics. The tools discussed during the second section are aimed at increasing the quality of data received from our customers for ingestion into DoD ABIS. The latent backlog mitigation plan has resulted in an increase of 13 latent print examiners resulting in stabilization of the backlog. The latent processing for forward latent matching completed the initial test phase and server issues were identified. A regression test effort is tentatively scheduled for 21-25 February 2011.

Findings and Insights:

While the focus of our user community is on both capacity and throughput, we must ensure DoD ABIS is evolved to consider the effect of system sizing on the accuracy and integrity of the database. The BIMA Biometrics Operations Branch recommended a user session be added to next year's collaboration forum and ask for increased participation in the Biometric Requirements Working Group (BRWG), et al.

Next Steps and Timeline:

Next Steps – Attendance in Biometric Working Groups (i.e. BRWG, BSWG, etc.)

Product development – enhancements to card scanning, forensic workbench, and other tools

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
System Sizing - Tmi - Identix 6.5.1	DoD ABIS CCB Working Groups	Phased Approach 3QFY11	BIMA PM Biometrics	COCOMS

Operational Metrics

Session Lead:

Mr. Russ Wilson, BIMA Metrics and Evaluation Branch

Session Objectives/Issues:

- ▶ Report current status of operational metrics; partners, efforts and reporting mechanisms.
- ▶ Collaborate high-level strategic effort; 5 year operational focus.
- ▶ Socialize Biometric Enterprise Strategic Plan (BESP) efforts.
- ▶ Categorize key aspects into four measurement domains.
- ▶ Discuss/define end user needs; focus on SMEs involvement across enterprise.
- ▶ Present types of operational metrics; static versus dynamic.
- ▶ Facilitate open forum discussion.

Topic Summary:

- ▶ Levels of metrics; focus on operational needs of end users.
- ▶ Ensure metrics align with BESP efforts; build on identified metrics for success.
- ▶ Involve subject matter experts (SMEs) from Biometrics Community of Interest (BCOI) to analyze data and ensure understanding of the variables involved during operations.
- ▶ Identify tradeoffs; improve activities while maintaining high quality.
- ▶ Define metrics, collect, analyze and report metrics that support the operational needs.

Findings and Insights:

- ▶ Operational metrics present a special challenge.
- ▶ Varying end-user needs and requirements for operational metrics.
- ▶ Operational metrics are in high demand across the end-user.
- ▶ Improvement is needed in operational areas while high quality is maintained.

Next Steps and Timeline:

- ▶ Meet with IDA to identify technical way ahead for Biodash transition - Mar 2011.
- ▶ Identify/involve targeted SMEs from BCOI – Mar-April 2011.
- ▶ Capture concerns of Commanders and Decision-Makers that metrics can support – May 2011.
- ▶ Institute a “Tiger Team”; conduct regular meetings and report efforts – May-June 2011.
- ▶ Transition and maintain the IDA dashboard to BIMA Central – July 2011.
- ▶ Define metrics on all four domains to support biometric operations – Aug 2011.
- ▶ Collect, analyze and report operational metrics – Oct 2011.

Timeline:

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Meet with IDA to identify technical way ahead for Biodash transition	Meeting	15 Mar 2011	BIMA	IDA
Identify/involve targeted SMEs from BCOI	Analysis of SLAs and customer agreements to identify	15 April 2011	BIMA	COCOMS/PM Biometrics/BCOI

Capture concerns of Commanders and Decision-Makers	SVTCs and meetings	~May 2011	BIMA	Theater – End-users
Institute a “Tiger Team”; develop charter; conduct regular meetings and report progress and findings	Working sessions involving operational participates	~June 2011	BIMA	Theater – End-users
Transition and maintain IDA Biodash Dashboard	Sessions with IDA/BOB/to transition, update and maintain database	~August 2011	BIMA	IDA

The Road from a Quick Reaction Capability to a Program of Record

Session Lead:

COL Theodore Jennings, PM DoD Biometrics

Please contact the session lead directly for additional information.

Friendly Biometrics Track

Leveraging Biometrics to Create Business Efficiencies, Effectiveness & Accuracy

Session Leads:

Mr. Brian Hunt, Chief, BIMA Business Functions Branch

Mr. Chris Miller, BIMA Business Functions Branch

LTC Joseph Baird, US Army Accessions Command (USAAC)

Mr. Dale Ostrowski, Deputy Director, J3/Operations for US Military Entrance Processing Command (MEPCOM)

Ms. Eroica Johnson, SPAWAR System Center Atlantic supporting Navy Installations Command (CNIC)

Mr. Mike Tyner, US Strategic Command (USSTRATCOM)

Mr. Roger Roehr, Pentagon Force Protection Agency (PFPA)

Session Objectives/Issues:

The focus of the session was to highlight ongoing biometric activities and create opportunities to share lessons learned and best practices.

Topic Summary:

- ▶ **USAAC / USAREC** - LTC Baird
 - Provided update on the use of biometrics to enable suitability checks earlier in the recruiting process for increased effectiveness & efficiencies.
- ▶ **MEPCOM** - Mr. Dale Ostrowski
 - Provided update on the use of biometrics to fix identities in the recruiting process to eliminate fraud and streamline the business process execution.

- ▶ **SPAWAR System Center – Atlantic / CNIC** - Ms. Eroica Johnson
 - Provided an update on the use of biometrics to enable ship borne personnel accountability.
- ▶ **STRATCOM** - Mr. Mike Tyner
 - Provided update on current outlook and initiatives associated to biometrics.
- ▶ **PFPA** – Mr. Roger Roehr
 - Provided an update on the status of the PFPA initiative and an August 2011 pilot at the Mark Center in Alexandria, Virginia.

Next Steps and Timeline:

Next Steps are simply staying abreast of these initiatives as they progress through their milestones. No other actions are required.

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Repurpose case studies into the IPM Conference Sessions	Working Groups	<120	BIMA Business Functions branch	Various partners

Biometric Equities for the Identity & Privilege Management Working Group (IPvMWG) Roadmap

Session Leads:

Mr. Thomas Mathis, BIMA Business Functions Branch
Mr. Pete Joukov, DoD CIO

Session Objectives/Issues:

Update community on IPvM Roadmap activities; review and establish consensus on Biometric Equities.

Topic Summary:

Discussion Points -

- ▶ The Identity Management and Protection Senior Coordinating Group (IPMSCG) has existing authorities to advance friendly biometrics in DoD.
- ▶ The IPvM Roadmap is an opportunity to formally define the role of biometrics DoD-wide and help define the framework to mature friendly biometric capabilities.

Findings and Insights -

- ▶ The IPvM analysis revealed significant interest in biometrics-enabled watch-lists for hiring and access control (part of the Full Spectrum Biometrics concept).
- ▶ The IPvM analysis also highlighted value of federating biometrics-enabled identity information to support a wide array of mission sets.

Next Steps and Timeline:

Next Steps

- ▶ Invited participants to contact DoD CIO office and participate in IPvMWG
- ▶ Continue participation in IPvMWG Meetings

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Develop a CONOPs	Identity & Privilege Management Working Group	CONOPs <30	BIMA Business Functions Branch, with Plans Branch, Policy Branch, Requirements Branch and Architecture Branch reps	OSD-NII IPvM Workgroup Members
Develop a Roadmap	IPvM Workgroups	Roadmap <120	BIMA Business Functions Branch, with Plans Branch, Policy Branch, Requirements Branch and Architecture Branch reps	IPvM Workgroup Members

Credentials Part I & II

Session Leads:

Mr. Brian Hunt, Chief, BIMA Business Functions Branch
Mr. Thomas Mathis, BIMA Business Functions Branch

Session Objectives/Issues:

- ▶ Inform IPMSCG Quick Look Friendly Biometrics Transition Plan for IPMSCG.
- ▶ IPMSCG requested BIMA lead helping the DoD Community develop guidance on the diversity of biometric modalities and applications for access control occurring today.
- ▶ Identify baseline terminology to enable a constructive dialogue, including a high-level explanation of authentication as part of the authorization process.
- ▶ Review illustrative Use Cases that detail the various roles biometrics can have in the authentication process.
- ▶ Discuss challenging issues.
- ▶ Biometrics The Good, The Bad, and the Ugly, i.e., what are accepted and validated benefits (Good), known issues that need understanding (Bad), and challenging issues that required future studies and research (Ugly).
- ▶ Provide an update on the efforts of the Defense Installation Access Control (DIAC) Working Group.

Topic Summary:

Discussion Points -

- ▶ Agreed that there are significant language challenges that hamper communications when discussing Identity and Privilege Management.

- ▶ Reviewed and established consensus on differing roles of biometrics with authentication.
- ▶ DIAC is kicking off a Biometrics Analysis Study to determine where/how to use biometrics in PACS to enhance Force Protection. This aligns with the IPMSCG Quick Look Team for Friendly Force Biometrics recommendations, regarding biometrics and physical access.

Findings and Insights:

- ▶ Agreed that there is a lack of a solid science foundation for the different biometric modalities to enable drafting uniform policy and criteria.
- ▶ Agreed that commercial standards for DoD biometrics systems are required to enable the proliferation of biometrics applications in DoD.

Next Steps and Timeline:

Next Steps -

- ▶ Engage IPvMWG to put a roadmap initiative to organize and advance the science of biometrics to enable drafting of more mature policy & guidance.
- ▶ Follow up with NIST and review status of biometrics research & studies and work out a way ahead.
- ▶ Conduct a review within BIMA to establish priorities on Friendly Biometrics initiatives.

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
NIST recap	Working Group	<30	BIMA Business Functions Branch Some BIMA Standards Branch role TBD.	OSD-NII & NIST
Identity Protection and Management Session	IPM	<90	BIMA Business Functions Branch Some BIMA Standards Branch role TBD.	

National Institute of Standards and Technology (NIST) Identity Program Update

Session Lead:

Ms. Donna Dodson, Chief, Computer Security Division, Information Technology Laboratory, NIST

Session Objectives/Issues:

Provide updates on NIST Identity Programs, NIST 800-63, PIV and provide community opportunity for question and answer.

Topic Summary:

- ▶ Highlighted the NIST SP 800-63 E-Authentication is the implementation of OMB 04-04 and is applicable to remote access only.
- ▶ 2005-2007 NIST Supported Biometrics Study on E-Authentication was a great initiative; recommend we use it as a foundation for the biometrics community to strengthen the language in NIST SP 800-63.
- ▶ Supported earlier assertion of a need to improve the biometrics technology science foundation and commercial standards for biometrics systems within DoD.

Next Steps and Timeline:

- ▶ BIMA will follow up with NIST to get a broader understanding of the scope of their Biometrics Activities.

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Learn more about NIST Biometrics activities	Various	<30	BIMA Business Functions Branch	OSD-NII
Support studies and SP 800-63 rewrite				

Biometrics Enterprise Requirements Strategy

Session Lead:

Mr. Robbie Mosley, BIMA Requirements Management Branch

Session Objectives/Issues:

Established understanding and consensus on the need for Friendly Forces Analysis of Alternatives (AoA)

Topic Summary:

- ▶ Recognize the criticality of identifying stakeholders of all mission areas to enable the AoA.

Next Steps and Timeline:

- ▶ Obtain Director BIMA guidance to begin planning for Friendly AoA.
- ▶ Conduct Planning with Requirements Management Branch on Friendly AoA.
- ▶ Coordinate with Resource Management & Director to program funding for AoA.

Timeline –

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Identify timeline for AoA	NA	<30	BIMA Business Functions Branch	BIMA Requirements Management Branch, DAMO-CI

DoD Identity Resolution Collection Management

Session Lead:

Mr. Avi Isaacson, US Army Intelligence and Security Command

Session Objectives/Issues:

The objective of this session is to discuss the development of Collection Management (CM) requirements. The integration of biometrics as a non-traditional Intelligence, Surveillance, and Reconnaissance (ISR) asset into the CM process was discussed, as well as topical issues relating to covert / clandestine and cyber capabilities.

This session covered the following topics:

- ▶ Collection Management Doctrine / Policy.
- ▶ Converting Intelligence Requirements into CM Requirements.
- ▶ Establishing Priorities for Collection.
- ▶ Tasking Mechanisms for Biometrics Collection.
- ▶ Feedback / Retasking of Biometrics Collectors.
- ▶ Ability for the Biometrics Community to Task Specialized Collection Assets.
- ▶ Retaining Data of Non-traditional Sources (Classified US Persons, and US/Host Nation Laws).
- ▶ Searching/Matching of Non-traditional Sources.
- ▶ Biometrics and HUMINT.

Topic Summary:

OUSD(I), COCOM, and Army Military Intelligence were present during the topic discussions.

Discussion Points –

Topic #1: Collection Management Doctrine/Policy. Discussion centered on whether our existing doctrine/policy was sufficient with regard to biometrics CM requirements. Actions:

- ▶ COCOMs – Develop ways to improve theater-level policy and oversight.
- ▶ Services – Capture TTPs, Best Practices.
- ▶ TCM BF – Revise Army FMs.
- ▶ DIA – Revise UJTL.

Topic #2: Converting Intelligence Requirements into CM Requirements. Discussion focused on answering whether our existing national-level CM requirements are sufficient to accomplish our goals. Additionally, we tried to answer whether the current biometrics intelligence products were sufficient in their support to the Warfighter. Actions:

- ▶ COCOMs – Scope CM requirements to capture a better understanding of human intentions and serve as tip-offs for other “INTs”.
- ▶ Services – Integrate biometrics into CM courses.
- ▶ COCOMs – Develop a target-centric approach.
- ▶ All – Increase access to databases.

Topic #3: Establishing Priorities for Collection. Discussion focused on answering whether sufficient mechanisms were in place to prioritize collections. Actions:

- ▶ OUSD(I) – Develop National CM Strategy.
- ▶ COCOMs – Publish COCOM priorities and assign resources to collect on them.
- ▶ TCM BF - Advocate integration of Soldiers at Brigade Combat Teams (BCTs).

- ▶ All – Increase the efficiency of existing resources.

Topic #4: Tasking Mechanisms for Biometrics Collection. Discussion sought to answer whether sufficient mechanisms are in place to task specific collection assets. Additionally, discussion sought to answer whether sufficient mechanisms are in place to ensure that efficiency of collection across multiple platforms (i.e. assign multiple Identity Resolution collection platforms on a single site at a single time). Actions:

- ▶ Services - Improve training.
- ▶ COCOMs / Services – Decentralization of CM resources as far forward as possible is critical.
- ▶ All – Increase the efficiency of existing resources.

Topic #5: Feedback/Retasking of Biometrics Collectors. Discussion centered on how effective our feedback mechanisms were to the CM generator. Actions:

- ▶ COCOMs – Improve feedback to MI assets supporting BEI.

Topic #6: Ability for the Biometrics Community to Task Specialized Collection Assets. Discussion focused on how to get the “right people” involved, gaining access to “raw” data, and ensuring that the right authorities are in place to collect. There were no actions resulting from this topic.

Topic #7: Retaining Data of Non-traditional Sources (Classified, US Persons, and US/Host Nation Laws). Discussion focused on ensuring the a common interpretation of Intelligence Oversight and ensuring that, when appropriate, we develop shareable systems that satisfy US and Host Nation laws. Actions:

- ▶ Army / OUSD(I) – Develop Intelligence Oversight Policy.
- ▶ COCOMs / OUSD(I) – Develop policy to address US / Host Nation laws.

Topic #8: Searching/Matching of Non-traditional Sources. Discussion focused on matching of non-traditional sources. Actions:

- ▶ COCOMs – Improve the process of acquiring data.
- ▶ BIMA (DISR) / OUSD(I) (ICSR) - Develop DoD and international standards.
- ▶ DIA – Develop batch processing of non-standardized file formats.

Topic #9: Biometrics and HUMINT. Discussion was classified.

Findings and Insights -

Much work remains to develop, staff, and coordinate collection management in the biometrics community. This CM must be fully integrated into a National CM strategy and utilize existing CM processes, be decentralized down to at least the BCT level, and fully leverage the entire Identity Resolution capability. As we transition to non-permissive environments, we must seek to do business overtly with friendly nations, while embracing alternative measures when appropriate, in order to develop focused, rich datasets of Identity Resolution data useful throughout the continuum of operations.

Next Steps and Timeline:

Next Steps -

USD(I), Services, and COCOMs address CM in appropriate forums

Timeline – All actions are listed above, and the respective timelines and forums are event-based pending the development of policy, DoD CONOPs, doctrine, and personnel/equipment fielding. Further, these will be COCOM-specific forums.

Intelligence Requirements for NATO Standardization Agreement (STANAG) Study 4715

Session Lead:

Mr. Benji Hutchinson, OUSD(I) SETA Advisor on Biometric, Forensic, and Identity Intelligence

Session Objectives/Issues:

The purpose of this session was to discuss and develop biometric and forensic enabled intelligence (BEI and FEI) technical requirements for NATO Study 4715. This study, when published, will become the STANAG for Biometrics Data, Interchange, Watch Listing, and Reporting Standard within NATO. The goals of this session were to develop an outline and begin generating content for a technical contribution that will be submitted to NATO for consideration for inclusion in Study 4715. The specific pieces of Study 4715 that pertain to intelligence activities are the standardized match results, watchlisting, and reporting of intelligence derived from biometric samples and forensic information. The group also began identifying roles and responsibilities of the contributing agencies over the next 30 days to prepare intelligence input for the technical contribution.

Topic Summary:

Discussion Points -

- ▶ The current and future biometrics and BEI technical standards requirements emanating from the intelligence community. Specifically, standards for NATO BEI reporting formats, match results, and a standard for a NATO BEWL.
- ▶ The current format of the Biometric Identification Analysis Report (BIAR) may or may not be sufficient for submission to NATO as a contribution. A deeper examination of the format is needed.
- ▶ The group discussed the utility of a tier based watchlist and the challenges and benefits of proposing a category based watch list.
- ▶ NATO classification codes may not be sufficient.

Findings and Insights -

- ▶ U.S. Defense Intelligence community must decide upon a standard CONOPs for the DoD BEWL before making a recommendation for the study.
- ▶ The group agreed to meet at a later date to discuss at length the sufficiency of the BIAR format and the data elements within that format. Additional data will be needed for a NATO standard reporting format.
- ▶ The group agreed, based on input from an Australian participant, the U.S. must decide upon either a tier based or a categorical BEWL before recommended an approach to NATO. If the U.S. decides to modify US BEWL operations, it needs to be consistent and aligned with the future NATO standard.
- ▶ Wider documentation (Intelligence Community specific standards for reporting, as an example) is needed to capture technical requirements from the NATO, DoD Biometrics and Defense Intelligence communities.
- ▶ More deliberate sessions on developing the US contributions are needed across all sections of the Study.
- ▶ The STANAG may need to contain security classification markings for partner countries engaged NATO biometrics and BEI enabled operations.

Next Steps and Timeline:

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
Develop intelligence requirements for standards to be submitted in a U.S. technical contribution for the STANAG. Specific content for reporting and the BEWL are needed.	Identity Intelligence Working Group (I2WG) – Proposed Focus Group on BEI Data Issues	<p>30 days: Develop all U.S. technical content.</p> <p>60 days: Consolidate all U.S. input and submit to appropriate NATO groups.</p> <p>90 days: Coordinate with NATO partners to review all NATO national contributions to the STANAG.</p>	BIMA and OUSD(I)	INSCOM, National Ground Intelligence Center

DoD Biometrically-Enabled Watch List Discussion

Session Leads:

Mr. Matthew Young, BIMA Standards Branch
Mr. Paul Moruza, National Ground Intelligence Center
Mr. Kevin White, National Ground Intelligence Center

Session Objectives/Issues:

The purpose of this session was to review the BEWL Transmission Specification progress, discuss BEWL CONOPs and develop a clear way ahead for both the Transmission Specification and CONOPs.

Topic Summary:

Discussion Points -

The BEWL has a large amount of stakeholders, including interagency partners and others National Security entities. There exists a rather large delta between as-is and to-be BEWL, which will result in

Findings and Insights:

Communication of Top Hits across DoD and IC entities needs to be improved to place emphasis on why the BEWL is so important. Ultimately, the BEWL is the point which translates all the biometric data collection into something that is useful, and is the means by which the soldiers in theater are able to apprehend dangerous persons. There was significant COCOM and Services input on warfighter needs during the session which help keep everyone focused on the importance of delivering the best data to the warfighter. During the second half of the session, a

BEWL CONOPs drafting session took place in which valuable input and alignment was provided to the appropriate sections needed to fulfill the mission.

Next Steps and Timeline:

Recommendations:

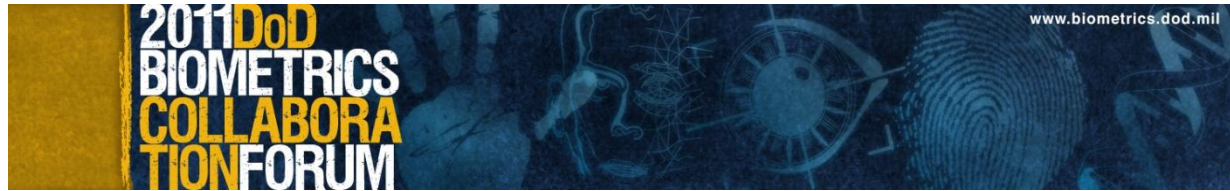
- ▶ Continue collaboration between operators, users and stakeholders.
- ▶ NGIC to create BEWL COI (a recommendation made during the session, will require granted authority from OUSDI and DIA to perform these actions).

Timeline:

- ▶ Version 0.2 of BEWL Transmission Specification to be delivered in March.
- ▶ Draft of CONOPS available in March – April.

Action	Forum	Deadline or Timeline	Lead Organization(s)	Support Organization(s)
BIMA to finalize development team for Transmission Specification	BIMA	90 Days	BIMA Standards Branch	NGIC, BIMA Data Team, DHS, FBI and NTSC
BIMA to assess impact on ABIS	BIMA	90 Days	BIMA Biometric Operations Branch	BIMA Standards Branch, Requirements Branch, Architecture Branch
NGIC to lead CONOPs development	NGIC	90 Days	NGIC BEWL Operations	BIMA Biometric Operations Branch, Standards Branch, OUSD(I)
NGIC to crosswalk CONOPs with CCD for BEC and JPI	NGIC	30 Days	NGIC BEWL Operations	BIMA Biometric Operations Branch, Standards Branch, OUSD(I), BIMA Requirements Branch

Attendee List



LAST NAME	FIRST NAME	ORGANIZATION	EMAIL
Abe	Brian	Mitre	bcabe@mitre.org
Adams	Desmond	CIO - G6	karen.cauraugh@us.army.mil
Albers	James	L-1 Identity Solutions	jalbers@l1id.com
Alexander	Danielle	Applied Research Associates	dalexander@ara.com
Alexander	Gregory	OSD	gregory.alexander.ctr@osd.mil
Aloi	Sam	BIMA Biometrics Operations Branch	sam.aloi@biometrics.dod.mil
Anderson	Delia	US-VISIT/National Protection & Programs Directorate	delia.anderson@dhs.gov
Andrews	Michael	BIMA Plans Branch	andrews_michael@aol.com
Archer	Craig	USSOCOM	craig.archer@socom.mil
Arp	Jim	K3 Enterprises	jim.arp@k3-enterprises.com
Augustyn	Joyce	BIMA Enterprise Engagement Branch	joyce.augustyn@us.army.mil
Baird	Joseph	US Army Accessions Command	joseph.baird@us.army.mil
Baker	Thomas	I MEF ATFP	thomas.j.baker@usmc.mil
Balut	Brian	Asymmetric Warfare Group	brian.balut@us.army.mil
Bazzett	Ronald	Army Intel	ronald.bazzett@mi.army.mil
Beaver	Gary		gary.beaver@us.army.mil
Becker	Karyn	DHS/US-VISIT Program	karyn.i.becker@dhs.gov
Bello	Ilich	USMC	ilich.bello@usmc.mil
Besco	Michael	Navy SPAWAR	michael.besco@navy.mil
Bishop	Michael	BIMA Requirements Management Branch	michael.bishop@us.army.mil
Bishop	David	National Maritime Intelligence Center	dmbishop@nmic.navy.mil
Bittenbender	Harrison	BIMA Requirements Management Branch	harrison.bittenbender@us.army.mil
Blakeley	Brian	ColorID, LLC	brian@colorid.com
Blakely	Jeff	OUSD P&R	jeff.blakely.ctr@osd.pentagon.mil
Blakemore	Bryan	Mount Airey Group	bblakemore@mountaireygroup.com
Blanton	Jennifer	SOCOM	blantonj@jdi.socom.mil

Boag	Terry	Charlotte-Mecklenburg Police Department	terry.dana.boag@us.army.mil
Boardman	Jill	USSOCOM	jill.boardman@socom.mil
Boesdorfer	Todd	Booz Allen Hamilton	boesdorfer_todd@bah.com
Bommelje	Britt	NDIA	bbommelje@ndia.org
Borhauer	Rachel	BIMA Requirements Management Branch	rachel-borhauer@us.army.mil
Bowman	William	Six3 Systems	william.bowman@six3systems.com
Boyd	Heidi	DHRA	heidi.boyd@osd.pentagon.mil
Boyd	John	The Patuxent Partnership	john.boyd82@gmail.com
Brandt	Josh	USCG	josh.d.brandt@uscg.mil
Branson	Dennis	Camber Corporation	dennis.branson@gmail.com
Brauner	Scott	Anser	scott.brauner@anser.org
Brian	Likens	PM Biometrics	Brian.Likens@biometrics.dod.mil
Brown	Karen	Biometrics Identity Management Agency (BIMA)	karen.brown@biometrics.dod.mil
Buckel	Karla	BIMA Metrics and Evaluation Branch	karla.buckel@biometrics.dod.mil
Buhrow	William	Biometrics Identity Management Agency (BIMA)	bill.buhrow@cox.net
Bui	Quang	Biometrics Identity Management Agency (BIMA)	quang.bui@us.army.mil
Burrow	Adolphus	SPAWAR Atlantic	burrowa@infosec.navy.mil
Bussian	Robert	OSD	robert.bussian@osd.mil
Bustamante	Tammie	USCG	tammie.l.bustamante@uscg.mil
Butler	John	Joint Personnel Recovery Agency (JPRA)	john.butler@axad.belvoir.army.mil
Campbell	Larry	Oberon Associates	lcampbell@oberonassociates.com
Carper	Eric	NGIC BIP	eric.carper@biometrics.dod.mil
Carter	Alex	TRADOC - USAREC	alexander.carter@us.army.mil
Castleman	Erin	Booz Allen Hamilton	castleman_erin@bah.com
Cave	Chris	Bode Technology Group	chris.cave@bodetech.com
Ceravolo	Christopher		christopher.ceravolo@us.army.mil
Charles	Tench	BTA	charles.tench@bta.mil
Chedister	Bradley	USSOCOM HQ	bradley.chedister.ctr@socom.mil
Chong	Min	STOPSO	min.chong@stopso.com
Chris	Moyd	JIB/JSOR	cmoyd26@yahoo.com
Christensen	John	Northrop Grumman	john.d.christensen@ngc.com
Citrenbaum	Keith		keith.citrenbaum@us.army.mil

Clancey	Patrick	BIMA Enterprise Engagement Branch	patrick.clancey@us.army.mil
Clark	Brian	UNISYS	brian.clark@unisys.com
Clarke	Garrett		garrett.clarke@us.army.mil
Collins	Timothy	Navy CAC PMO	timothy.j.collins2.ctr@navy.mil
Comer	Randy	Anser supporting USMC	randy.comer@anser.org
Conner	Cathy	C3I	caconner@comcast.net
Connolly	Wally	Army G-2	wally.connolly@us.army.mil
Conrad	John	Signaltel supporting DOJ	johnsc@signaltel.net
Cooney	Lauren	BIMA Biometrics Operations Branch	lauren.cooney@biometrics.dod.mil
Costello	Mike		mcostello@gloconeng.com
Courtney	Marc	COMUSMARCENT	marc.courtney@marcent.usmc.mil
Curry	Kevin	NORTHCOM J84	kevin.curry@northcom.mil
D'Agostino	Tom	BIMA Standards Branch	thomas.dagostino@us.army.mil
Defabritis	Michael	II MEF, USMC	michael.defabritis@iimeffwd.usmc.mil
Demestihias	Anthony	BIMA Policy Branch	anthony.w.demestihias@us.army.mil
DeMonte	Giovanni	BIMA Architecture Branch	giovanni.demonte@us.army.mil
DENT	Magruder	Aware, Inc.	mdent@aware.com
DeWolfe	Sam	Northrop Grumman	samuel.dewolfe@ngc.com
Dipiazza	Nicholas	BIMA Military Operations Branch	nicholas.dipiazza@us.army.mil
Dodson	Donna	NIST	ddodson@nist.gov
Doray	Edmund	NORTHCOM	edmund.doray@northcom.mil
Dossett	Charles	US Army Recruiting Command (HQUSAREC)	charles.dossett@usarec.army.mil
Duggal	Sanjeev	DHS - CBP - OIT - OBP	sanjeev.duggal@associates.dhs.gov
Dunleavy	Joseph	BIMA Requirements Management Branch	joseph.dunleavy@us.army.mil
Dunn	Jeffrey	NSA	jsdunn@alpha.ncsc.mil
Earhart	Michael	USD(I)	michael.earhart@osd.mil
Edmund	McCarthy	USASOC	edmund.mccarthy@us.army.mil
Ehlert	Craig	TRADOC Capabilities Manager Biometrics and Forensics	craig.ehlert@us.army.mil
Elder	Kenneth	BIMA Concepts and Technologies Branch	kenneth.elder@biometrics.dod.mil
Eric	Taylor	USASOC	Taylorcm.ctr@jdi.socom.mil
Eric	Hildre	BIMA	eric.hildre@conus.army.mil

Esposito	Renee	Booz Allen Hamilton	esposito_renee@bah.com
Fisher	David	CardSmart	dfisher@yourcardsolution.com
Fisher	Todd	PEO-EIS	todd.g.fisher@us.army.mil
Flores	Carmen	Business Transformation Agency	carmen.flores@bta.mil
Ford	Billy	Air Force	billy.ford.ctr@hanscom.af.mil
Fossa	James	Prospective Chief of Biometrics Iraq	fossaj@bolles.org
Fowlkes	Aaron	NGIC	aaron.fowlkes@us.army.mil
Fox	Gary	USARCENT	gary.l.fox@arcent.army.mil
Fuller	Donald	OSD	donald.fuller.ctr@osd.mil
Gabriel	Cheley	BIMA Enterprise Operations Division	cheley.gabriel@biometrics.dod.mil
Gantt	Kenneth	BIMA Deputy Director	ken.gantt@biometrics.dod.mil
Gates	Robert	Biometrics Identity Management Agency (BIMA)	robert.m.gates@us.army.mil
Gearty	Mike	TCM BF	michael.gearty@us.army.mil
Gieselman	Neal	BIMA Biometrics Operations Branch	neal.gieselman@biometrics.dod.mil
Gill	James	National Ground Intelligence Center	james.t.gill@mi.army.mil
Golden	Warren	OSD P&R IM	warren.golden@osd.pentagon.mil
Gosinski	Toni	HQ USEUCOM	gosinskt@eucom.mil
Graczyk	John	Booz Allen Hamilton	graczyk_john@bah.com
Grant	Paul	DoD CIO	joseph.callahan.ctr@osd.mil
Green	Mike	J8 Force Protection	michael.green@js.pentagon.mil
Griffith	James	Janus Research	james.griffith@janusresearch.com
Groulx	Danny		dgroulx@yourcardsolutions.com
Gustin	Peter	US Army Signal Center of Excellence	peter.gustin@conus.army.mil
Hall	Heather	JIEDDO	heather.hall@jieddo.dod.mil
Hamlin	Chad	HQMC CD&I	chad.hamlin@usmc.mil
Harmell	Mitchell	US Border Patrol	mitchell.harmell@dhs.gov
Hart	Susan		dayhiker57@gmail.com
Harzak	Donald	CENTCOM	harzak_donald@bah.com
Hatano	Toru	BIMA Business Functions Branch	toru.hatano@us.army.mil
Hayes	Jeff	Aware Inc.	jhayes@aware.com
Height	Robby	HQ USAAC G6	robby.height@usaac.army.mil
Helin	Scott	CENTCOM J2	scott.helin.ctr@centcom.mil

Helmich	Mitchell	SAIC	helmichh@saic.com
Hembree	Larry	CNIC	larryhembree@hembreeconsulting.com
Henderson	Rachelle	DHS	rachelle.henderson@dhs.gov
Herdegen	Dale	MITRE	dherdegen@mitre.org
Heuring	Terry	IDA	theuring@ida.org
Hickok	Glenn	Cross Match Technologies	glenn.hickok@crossmatch.com
Higgins	Michael	JIEDDO/MITRE	higginsm@mitre.org
Hill	Eric	Special Operations Command Pacific	eric.hill@idealinnovations.com
Hodges	Steve	Agnitio Corporation	shodges@agnitio.us
Holland	John	US Army	john.holland@us.army.mil
Hollingsworth	Mike	Signaltel supporting DOJ	michajh@signaltel.net
Howard	Brad	Navy	bradley.howard@navy.mil
Hudson	Sally	USD(I)	sally.hudson@osd.mil
Hughes	Christine	Center for Naval Analyses	hughesc@cna.org
Hunt	Brian	BIMA Business Functions Branch	brian.hunt@us.army.mil
Hurst	Christopher	Headquarters US Air Force	christopher.hurst@pentagon.af.mil
Hutchinson	Benji	OUSD(I)/Six3 Systems	benji.hutchinson@dodiis.mil
Ichikawa	Bryan	UNISYS	bryan.ichikawa@unisys.com
Isaacson	Avi	HQ, INSCOM	avram.isaacson@us.army.mil
Isola	Steven	USAICoE Doctrine	steven.isola@conus.army.mil
Jackson	Jerry	IBM	jerry.jackson@us.ibm.com
Jennings	Theodore	PM DoD Biometrics	theodore.jennings@us.army.mil
Johns	Vincent	BIMA Military Operations Branch	vincent.johns@biometrics.dod.mil
Johnson	Jennifer	BIMA Requirements Management Branch	jljohnson@me.com
Johnson	Eroica	SSC LANT CHAS	eroica.johnson@navy.mil
Jones	Valerie	BIMA Metrics and Evaluation Branch	valerie.jones@biometrics.dod.mil
Jones	Ray	BIMA Requirements Management Branch	raymond.c.jones@us.army.mil
Jones	Jeffrey	Navy/ASN E,I&E	jeffrey.r.jones2@navy.mil
Joukov	Peter	DoD CIO Identity Assurance	peter.joukov.ctr@osd.mil
Juchem	Philip	OSD / NII	philip.juchem@us.army.mil
Kasaian	Joy	International Biometric Group	jkasaian@ibgweb.com

Keipper	Kevin	Aoptix Technologies, Inc.	kkeipper@aoptix.com
Kershner	Michael	BIMA Military Operations Branch	michael.kershner@us.army.mil
Khetan	Vanitha	BIMA Architecture Branch	vanitha.khetan@us.army.mil
Killion	Thomas	Director, Biometrics Identity Management Agency	thomas.killion@biometrics.dod.mil
King	James	USCG	james.g.king@uscg.mil
Knezevic	Daniel	BIMA Policy Branch	daniel.knezevic@us.army.mil
Konieczny	Frank	SAF/A6	frank.konieczny@pentagon.af.mil
Kritz	Amy	USCG	amy.kritz@uscg.mil
Langley	Sandra	DMDC	Sandra.langley@osd.pentagon.mil
Langworthy	Peter	Northrop Grumman	peter.langworthy@ngc.com
Lawson	Christopher	BIMA Enterprise Engagement Branch	chris.lawson3@us.army.mil
Lazarevich	Aleksandr	PM DoD Biometrics	aleksandar.lazarevich@us.army.mil
Leary	Frank	SPAWAR Atlantic	frank.leary@navy.mil
Leas	Richard	FBI - TEDAC	richard.leas@ic.fbi.gov
Lecea	Julie	AFOSI	julie.lecea@ogn.af.mil
Leonard	Johnson	TTECG S-2	leonard.bjohnson@yahoo.com
Lohman	Dave	Biometrics Identity Management Agency (BIMA)	dave.lohman@biometrics.mil
Lopez	Joe	USNORTHCOM	joe.lopez@northcom.mil
MacDonald	Lisa	BIMA Strategic Integration Division	lisa.macdonald@us.army.mil
Machuga	David	Northrop Grumman	david.machuga@ngc.com
Mackness	Abby	MorphoTrak	abby.mackness@morphotrak.com
Manzo	John	FBI	john.manzo@leo.gov
Mariano	Lynn	Pentagon Force Protection Agency	Lynn.Mariano@pfpa.mil
Martin	Robert	USCG	robert.a.martin@uscg.mil
Martin	Jennifer	Booz Allen Hamilton	martin_jennifer@bah.com
Martinez	Omar	L1	omartinez@l1id.com
Mathis	Thomas	BIMA Business Functions Branch	tom.mathis1@us.army.mil
McDonald	Nerolie	HQ Joint Operations Command, Australia	nerolie.mcdonald@defence.gov.au
McDonald	Scott		scott.j.mcdonald@us.army.mil
McGuire	Douglas	TCM-BF	douglas.mcguire2@us.army.mil
McKee	Robert	SOCOM / SPAWAR	robert.mckee@navy.mil
McKee	Dave	USCENTCOM CCJ2	mckeed@centcom.mil
McKee	Robert	SPAWAR	robert.mckee@navy.mil

McKinney	Lloyd	USMEPCOM	lloyd.mckinney@mepcom.army.mil
McMurtrie	Robert	TCM-BF	robert.mcmurtrie@us.army.mil
McNally	Stephen	500th MI Brigade	stephen.mcnally@us.army.mil
McNamara	Daniel	CENTCOM	mcmamadj@centcom.mil
Melton	Christopher	NSTID, USAICoE	christopher.melton@us.army.mil
Mestemaker	Matthew	USMC	matthew.mestemaker@usmc.mil
Meyerhoff	Tim	Iris ID Systems	meyerhoff@irisid.com
Mike	Harris	SOCOM	michael.g.harris2@sor.mil
Millard	Galen	USAF	galen.millard.1@us.af.mil
Miller	Christopher	BIMA Business Functions Branch	chris.s.miller@us.army.mil
Missler	Mike	NCIS	james.m.missler@navy.mil
Montgomery	Joseph	LNO USAICoE	joseph.r.montgomery@us.army.mil
Mooney	Robert	Mitre	rmooney@mitre.org
Moore	Wendy	Design Mill, Inc	wendy_moore@designmillinc.com
Morgan	Kent	MEPCOM	kent.morgan@mepcom.army.mil
Moruza	Paul	NGIC	paul.moruza@us.army.mil
Mosley	Robbie	BIMA Requirements Management Branch	robbie.mosley@conus.army.mil
Munn	Chris	USD(I)	chris.munn@osd.mil
Murphy	Monte	Applied Research Associates	mmurphy@ara.com
Musa	Samuel	National Defense University	musas@ndu.edu
Nagy	Arturo	ITSFAC	anagy@itsfac.com
Nanavati	Samir	International Biometric Group	snavati@ibgweb.com
O'Neill	Timothy	CENTCOM	timothy.b.oneill.ctr@centcom.mil
Orozco	Oscar	SOUTHCOM	oscar.orozco@idealinnovations.com
Ortiz	John	CENTCOM J3	john.a.ortiz.ctr@centcom.mil
Ortscheid	Tim	ColorID, LLC	timothy@colorid.com
Osti	Andrew	SPAWARSYSCEN Atlantic	andrew.osti@navy.mil
Ostrowski	Dale	HQ USMEPCOM	dale.ostrowski@mepcom.army.mil
Ott	Greg	Sycamore.US, Inc.	greg.ott@sycamore.us
Oye	Craig	BIMA	craig.oye@biometrics.dod.mil
Pannone	Adam	BIMA Architecture Branch	adam.c.pannone@us.army.mil
Paterino	Kelly	HQ USMC PP&O	kelly.paterino.ctr@usmc.mil
Paul	Frasca	Max Vision	Pfrasca@maxvision.com
Pavlick	Eric	PM DoD Biometrics	eric.pavlick@us.army.mil
Perez	Carlos	USCENTCOM J2	perezc@centcom.mil

Perkerson	John	NCIS	jperkers@ncis.navy.mil
Peter	Ross	PM Biometrics	Charles.p.ross1@us.army.mil
Peyton	Richard	Crossmatch	richard.peyton@crossmatch.com
Phillips	Bill	BIMA Plans Branch	william.phillipsii@conus.army.mil
Philpitt	Nicholas	CENTCOM	nicholas.philpitt@centcom.mil
Piela	Joshua	USAFRICOM	joshua.piela@africom.mil
Plaza	Dane	Bode Technology Group	dane.plaza@bodetech.com
Pohlig	Cristin	Office of the Provost Marshal General, Forensics Branch	cristin.pohlig@us.army.mil
Polite	Damaion	USMC	damaion.polite@usmc.mil
Powers	Victor	TRADOC	victor-powers@us.army.mil
Pratt	Thomas	BIMA Military Operations Branch	pratttm@conus.army.mil
Presley	Pete	JIEDDO-ACOE	pete.presley@us.army.mil
Priester	Marquita	Navy	marquita.priester@navy.mil
Quinlan	Kevin	BIMA Policy Branch	kevin.r.quinlan@us.army.mil
Quinn	Kimberly	DIA	kimberly.quinn@dia.mil
Quintana	Karla	SOUTHCOM	karla.quintana@hq.southcom.mil
Rautanen	Wil	INSCOM Training & Doctrine Detachment	william.rautanenjr@conus.army.mil
Ray	Taylor	Office of Border Patrol	courtney.ray@dhs.gov
Raymond	Perry	BIMA	raymond.d.perry@us.army.mil
Redman	William	BIMA Plans Branch	redman_william@bah.com
Reynolds	Kathryn	BIMA Enterprise Engagement Branch	kathryn.l.reynolds@us.army.mil
Richardson	Herb	BIMA Business Operations Branch	herbert.richardson@biometrics.dod. mil
Ridge	Aaron	C2 TECOE	aaron.ridge.ctr@usmc.mil
Rivera	Andre	TCM BF LNO to CENTCOM	andreaanthonyrivera@gmail.com
Roehr	Roger	PFPA	roger.roehr.ctr@pfpa.mil
Rose	Sarah	BIMA Business Functions Branch	sarah.rose1@us.army.mil
Rossi	Randy	Asymmetric Warfare Group	randy.rossi@us.army.mil
Sanchez	Frank	HQMC	frank.l.sanchez@usmc.mil
Sanders	Eric	USARPAC	eric.j.sanders.ctr@us.army.mil
Sanders	Shane	513 MI BDE	sanders_shane@bah.com
Schaefer	Thomas	Applied Research Assoc	tom.schaefer@ara.com
Schuepp	Paul	Animetrics	pschuepp@animetrics.com
Schulenberg	Chad	AFRICOM	chad.schulenberg@idealinnovations. com

Schultz	Jean	E & M Technologies	jean.schultz@eandmtech.com
Scott	Christopher	TRADOC Capabilities Manager Biometrics	christopher.j.scott1@us.army.mil
Sexton	Eileen	IMAGEWARE SYSTEMS	esexton@iwsinc.com
Shafer	Nathan	CENTCOM	nathan.shafer.ctr@centcom.mil
Shaffer	Chris	513th MI BDE, INSCOM	chris.p.shaffer@mi.army.mil
Sherman	Eric	II MEF II MHG MP Spt Co	eric.sherman@usmc.mil
Siemasko	Zora	SAIC	siemaskoz@saic.com
Sieminski	Greg	National Ground Intelligence Center	gregory.sieminski@us.army.mil
Simon	Kedron	Cross Match	kedron.simon@crossmatch.com
Simon	Kenneth	USAREC	kenneth.simon@usarec.army.mil
Singer	Mark	BIMA Policy Branch	mark.singer1@conus.army.mil
Smith	Justin	FBI	justin.smith@ic.fbi.gov
Smithson	Joel	Six3 Systems	joel.smithson@six3systems.com
Sorenson	Karen	SPAWAR LANT	karen.sorenson@navy.mil
Spaun	Nicole	US Army Europe	nicole.spaun@us.army.mil
Stallsmith	David	ColorID, LLC	david@colorid.com
Steinhauer	Joshua	USEUCOM	josh.steinhauer@idealinnovations.com
Stevens	Andrew	NGIC	andrew.stevens@ngc.com
Stoffolano	Matt	National Park Service	matt_stoffolano@nps.gov
Storey	Gary	Biometrics Identity Management Agency (BIMA)	gary.storey@us.army.mil
Strohl	Michael	AFRICOM	michael.strohl@africom.mil
Suchma	Kathryn	FBI/TEDAC	kathryn.suchma@ic.fbi.gov
Sutton	Marcia	USCG	marcia.e.sutton@uscg.mil
Swann	Brandon	NCSC	bswann@restarea.ncsc.mil
Sweet	Thomas	IO Centric Solutions	thomas.a.sweet.ctr@navy.mil
Sykes	Rick	MorphoTrak	rsykes1226@aol.com
Taylor	Steve	BIMA Enterprise Engagement Branch	steve.s.taylor@us.army.mil
Taylor	Tracy	CIO-G6	karen.cauraugh@us.army.mil
Thorpe	Andrew		andrew.m.thorpe@kuwait.swa.army.mil
Tom	Binkley	MARCORSYSCOM	tbinkley@itsfac.com
Trindade	Antonio	U.S. Border Patrol	antonio.trindade@dhs.gov
Triplett	Ryan	BIMA Standards Branch	ryan.l.triplett@us.army.mil
Trissell	Kevin	PM DoD Biometrics	kevin.trissell@us.army.mil
Turbyfill	Bob	IO Centric Solutions Inc.	bob.turbyfill@iocentralsolutions.com

Tyler	David	CGI Federal supporting DOD PM Biometrics	david.tyler@stanleyassociates.com
Tyner	Michael	STRATCOM	tynermi@stratcom.mil
Van Laethem	George	USJFCOM J7	george.vanlaethem.ctr@jcom.mil
Van Sice	Jason	Cross Match Technologies	jason.vansice@crossmatch.com
Vermillion	Michael	NMEC	mlvermillion@cox.net
Vickers	William	OUSD(I)/TCA	william.vickers@six3systems.com
Vignaroli	Dante	Bode Technology Group	dante.vignaroli@bodetech.com
Vogel	Paul	USCG	paul.g.vogel@uscg.mil
Wagner	Jennifer	513th MI	wagner_jennifer@bah.com
Walker	Rickey	Office of Naval Intelligence	rickey.b.walker@gmail.com
Washington	Frederick	TCM-BF	fred.wash@us.army.mil
Weaver	Elizabeth	BIMA Enterprise Engagement Branch	liz.weaver@us.army.mil
Weber	Robert	U.S. Army Asymmetric Warfare Group	robert.w.weber.ctr@us.army.mil
Werner	Rodger	HSI	rodger.werner@dhs.gov
Wheeler	Donald	Marine Corps Warfighting Laboratory	donald.wheeler.ctr@usmc.mil
Whisenant	Mark	DHS CBP	mark.whisenant@cbp.dhs.gov
White	Craig	Biometrics Identity Management Agency (BIMA)	craig.white@us.army.mil
White	Kevin	NGIC/MITRE	kwhite@mitre.org
White	Chris	NSA/CTR	white_chris@bah.com
Williams	John A.	HQDA, G-3/5/7, DAMO-SSI	john.williams25@us.army.mil
Wilson	Dennis	SPAWAR LANT	wilsondr@east.infosec.navy.mil
Wilson	Russ	BIMA Technologies and Analysis Division	russ.wilson@biometrics.dod.mil
Wilson	Ryan	TRADOC	ryan.wilson12@us.army.mil
Windham	Gary	Department of Defense	gary.b.windham@ugov.gov
Woods	Kevin	BIMA Architecture Branch	kevin.b.woods@us.army.mil
Wright	Michael	BIMA Military Operations Branch	michael.j.wright@conus.army.mil
Wright	Kevin	PM DoD Biometrics	kevin.a.wright1@us.army.mil
Yeager	Meghan	SAIC	yeagerm@saic.com
Young	Matthew	BIMA Standards Branch	matthew.r.young4.ctr@us.army.mil

Acronym and Terms List

AABIS: Afghan Automated Biometric Identification System
ABIS: Automated Biometric Identification System (ABIS - D: ABIS - DNA)
ACMC: Assistant Commandant of the Marine Corps
AFRICOM: Africa Command
AoA: Analysis of Alternatives
AOR: Area of Operations
ARCENT: Army Forces Central Command
BCOI: Biometrics Community of Interest
BCT: Brigade Combat Team
BEC: Biometric Enabling Capability
BEI: Biometrics Enabled Intelligence
BEWL: Biometrically Enabled Watch List
BIARS: Biometric Intelligence Analysis Report
BRWG: Biometrics Requirements Working Group
BSWG: Biometrics Standards Working Group
CBP: Customs and Border Patrol
CCB: Change Control Board
CDD: Capabilities Development Document
CENTCOM: Central Command
CEXC: Combined Explosive Exploitation Cell
CNIC: Center Atlantic supporting Navy Installations Command
COCOM: Combatant Command
COI: Community of Interest
COMUSMARCENT: Commander, United States Marine Forces, Central Command
CONOP: Concept of Operations
DBEKS: DoD Biometrics Expert Knowledgebase System
DHS: Department of Homeland Security
DIA: Defense Intelligence Agency
DIAC: Defense Intelligence Analysis Center
DISR: Defense Information Standards Registry
DOMEX: Document and Media Exploitation
EA: Executive Agent or Enterprise Architecture

EBTS: Electronic Biometric Transmission Specification
EUCOM: European Command
FBI: Federal Bureau of Investigation
HUMINT: Human Intelligence
IA: Information Assurance
IC: Intelligence Community
IAFIS: Integrated Automated Fingerprint Identification System
IDENT: DHS Automated Biometric Identification System
INSCOM: Intelligence and Security Command
IPMSCG: Identity Protection Management Senior Coordination Group
IPvMWG: Identity Privilege Management Working Group
ISR: Intelligence, Surveillance, and Reconnaissance
JPI: Joint Personnel Identification
JUONS: Joint Urgent Operational Needs Statement
MAGTF: Marine Air-Ground Task Force
MARCENT: Marine Forces, Central Command
MCAST: Marine Corps Action Tracking System
MCCLL: Marine Corps Center for Lessons Learned
MCOTEA: Marine Corps Operational Test and Evaluation Activity
MEPCOM: Military Entrance Processing Command
MEU: Marine Expeditionary Unit
MOA: Memorandum of Agreement
NIST: National Institute of Standards and Technology
NGIC: National Ground Intelligence Center
NORTHCOM: Northern Command
NSTC: National Science and Technology Center
NSTID: New Systems Training Integration Division
OPSEC: Operational Security
OSD NII: Office of the Secretary of Defense Network and Information Integration
OUSD(I): Under Secretary of Defense for Intelligence
OUSD(P): Under Secretary of Defense for Policy
PACOM: Pacific Command
PFPA: Pentagon Force Protection Agency
PIV: Personal Identity Verification
PPBES: Planning, Programming, Budgeting and Execution System

PM: Project Manager
POR: Program of Record
PSA: Principal Staff Assistant
ROMO: Range Of Military Operations
SEEK: Secure Electronic Enrollment Kit
SME: Subject Matter Expert
SOCOM: Special Operations Command
SOTG: Special Operations Training Group
SOUTHCOM: Southern Command
STANAG: Standardization Agreement
TBD: To Be Determined
TCM-BF: TRADOC Capabilities Manager – Biometrics & Forensics
TMi: Transaction Manager Integration
TRIAD: DoD term used to depict the future interoperability between IAFIS (DOJ), ABIS (DoD), and IDENT (DHS)
TTPs: Tactics, Techniques, and Procedures
UJTL: Universal Joint Task List
USAAC: United States Army Accessions Command
USAICoE: US Army Intelligence Center of Excellence
USAREC: US Army Recruiting Command
USSTRATCOM: US Strategic Command
UUNS: Urgent Universal Needs Statement
VBSS: Visit, Board, Search, and Seizure