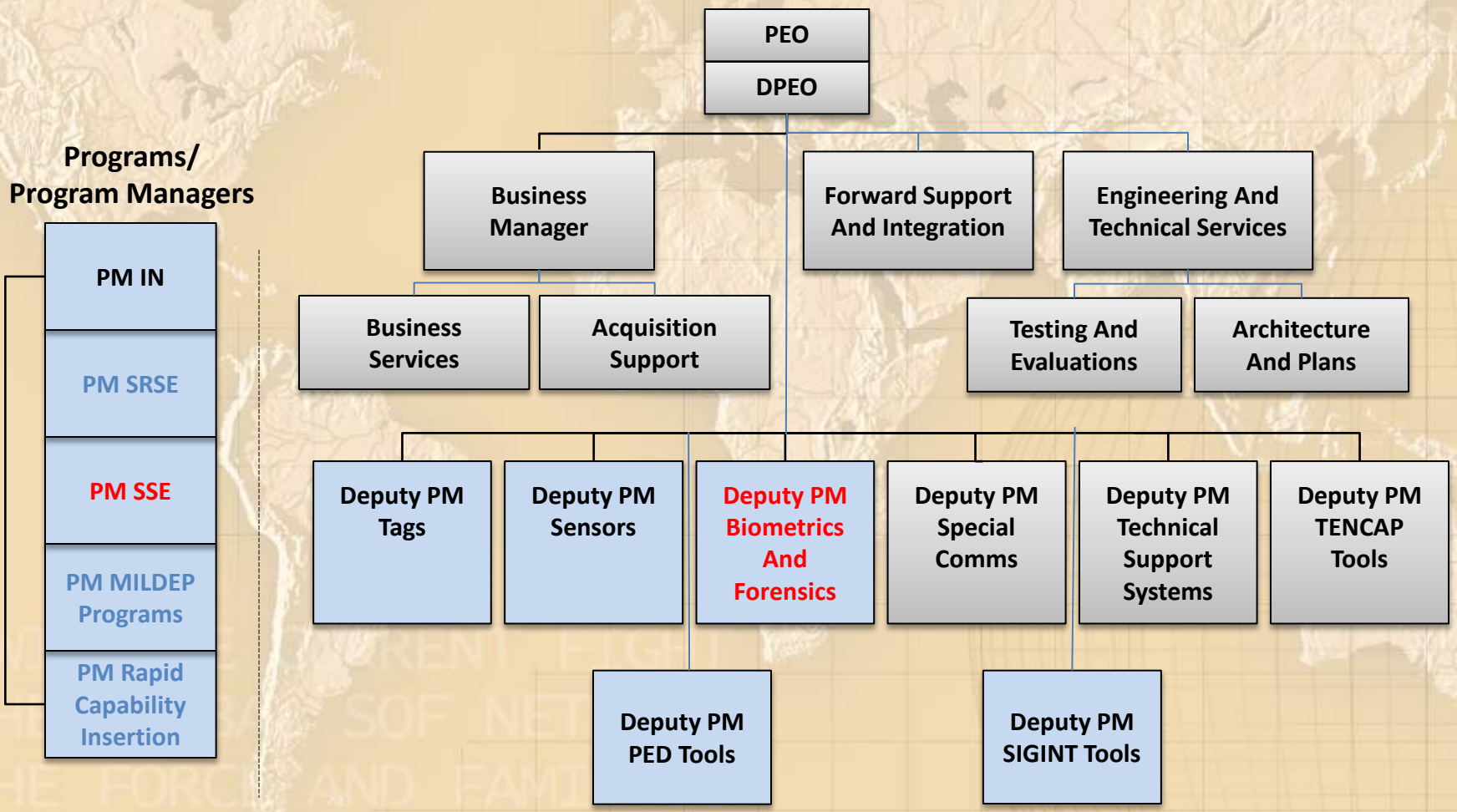
Mr. MICHAEL FITZ

Program Manager

Sensitive Site Exploitation

Operating Structure



Sensitive Site Exploitation

- Capability To Exploit Personnel, Documents, Electronic Data, And Material On A Sensitive Site/Objective
- Collects And Transmits Unique, Measurable Biometric Signatures

ACQUISITION STRATEGY	PERIOD OF PERFORMANCE	MILESTONES
Commodity Procurement Program	Annually Fields Capital Equipment Replacement And Technology Refresh To Component Kits	Fielding: Annually User Testing: Annually Commodity Procurements: Annually New Equipment Training: Continuously Fielding And Deployment: Continuously

POINT OF CONTACT	FUNDING	CURRENT CONTRACT/OEM
Michael Fitz Michael.fitz@socom.mil 813-826-7429	FY13 Procurement: $11.1M FY14 Procurement: $15.3M	Multiple

Sensitive Site Exploitation (SSE)

Cross Match SEEK II
Fingerprint & Iris Imager

Cross Match Guardian-R
Fingerprint Scanner

Enrollment (EN) Kit

Cross Match SEEK II
Fingerprint And Iris Imager

Identification (ID) Kits

Biometrics

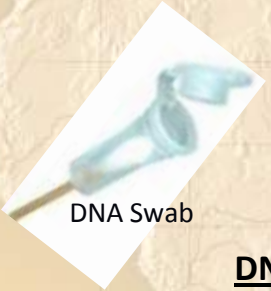
Metal Tec 1500

Metal Detector

IDEX Pens

Field Forensics EL-1003

Explosives And Trace Element Detection



DNA Swab

Latent Print Collection Kit

Forensic Lights

DNA And Latent Print Collection

3G SIMIS

XRY/XACT

CELLEX

ADF G-2

Low-Level MEDEX

USASOC Enabler Kit

Tableau TD-2 Imager

Digital Intelligence FRED-L

High-Level MEDEX

Data And Information Extraction

Tactical Site Exploitation (Forensics)

Exploitation Analysis Center (EAC)

Latent Print Copy Station

EAC Shelter
(Shown: 1 of 2 Shelters)

Griffin 460

Latent Print Fuming Chambers

AFIX Tracker
Latent Print Examiner

AHURA
First Defender

AHURA
TruDefender

Latent Print
Collection Kit

BattleLite
Forensic Lights

TracER Laser Lite

SABRE 5000

Latent Print Extraction Modalities

Trace Element Analysis Modalities

Biometrics Development Opportunities

- Non-optical Imaging Sensors For Fingerprint Capture And Matching
- Rapid DNA Matching
- Stand-off/Remote Facial Recognition And Matching
- Stand-off/Remote Iris Capture
- Dustless Latent Print Collection
- Deception Detection

Forensics Development Opportunities

- Hidden Chamber And Hidden Material Detection
- NRT Document/Cellular Phone Translation/Gisting
- Improved Presumptive Tactical Explosives/Nitrates/Narcotics Kits
- CELLEX Cable Testing
- Portable Radio Frequency/Cell Phone Detection
- Hand-Held Metal Detector With Adjustable Sensitivity
- SIM Card Detector
- Portable, Automated 3-D Room/Building Mapping Device
- Portable X-Ray Device To Safe Cell Phones/Computers

In-House Broad Agency Announcement (BAA)

- FY2011-2012 SORDAC Consolidated BAA (HG9222-10-BAA-SORDAC-KI)
  - Efficient Contract For Relevant RDT&E Efforts
  - Updated Annually Within Special Reconnaissance, Surveillance, And Exploitation (SRSE) Areas Of Technological And Scientific Importance
  - Valid Through 2014

Tactical Biometrics Evaluation 2012 (TBE-12) Summary Report

Background

- DoD increasingly relies on tactical biometric devices for identity management
- Vendors do not have a well documented set of operational requirements
  - Operating procedures vary and data format standards are often ignored
  - Quality of collected data varies widely
- Influx of new tactical biometric devices on the market
  - Each claims 'best' performance
- USSOCOM posted a call for devices in FedBizOps in October 2012
  - Vendors provided devices and training in November
  - Testing was conducted in December

Key Question

"Which devices are capable of collecting high-quality, matchable data and maintaining that collection standard across tactical environments?"

TBE-12 Devices Tested

Vendor **Model** *Type*	**L-1** **HIIDE 4** *Baseline*	**Cross Match** **SEEK II** *Baseline*	**Cross Match** **Avenger** *New*	**Wyle** **DCS** *New*	**RaptorID** **RaptorPad** *New*	**AOptix** **Stratus** *New*
Image						
Dimensions (inches)	5 x 8 x 3	8.7 x 5.5 x 3.5	9.5 x 6.2 x 1.8	6.9 x 3.7 x 1.1	5.5 x 9.7 x 1.8	6 x 3 x 1.4
Weight (lbs)	2.18	3.6	3.2	0.79	2.6	0.89 (including iPhone)
Iris Collection	• 640x480 (VGA) camera • Single-iris capture	• Dual-iris capture • Shielded iris sensor to block ambient illumination	Simultaneous dual-iris capture using two iris cameras	• Dual-wavelength IR LEDs • Simultaneous dual-iris capture	Single-iris capture	Dual-iris capture
Fingerprint Collection	• Capacitive 500dpi sensor • Single-print capture	• Optical sensor • Dual-print capture	• Active capacitance sensor • Dual-print capture	Three capacitive sensors capture three prints simultaneously	• Active capacitance sensor • Dual-print capture	• Capacitive sensor • Single-print capture
Face Collection	640x480 (VGA)	1.3 MP camera	5 MP camera	UV illumination	• Rear: 5MP camera / LED Flash (SAP 42) • Front: 1.3MP camera	Through native iPhone camera
Notes	Fielded in conflict zones around the world	Fielded in conflict zones around the world	User interface identical to Cross Match SEEK II	Android-based	• Software provided by Incadence. • Android-based • Runs MARS client.	• iPhone based • Sleeve holds iris, fingerprint sensors

Test Scenario 1: STERILE

Sterile (STER)

- Environment in which biometric devices are traditionally tested
- Not representative of an operational environment
- Subject is seated and fully cooperative
- Indoors with controlled lighting and a stationary platform (table top)
- Operator is unencumbered by other tactical equipment

Test Scenario 2: COOPERATIVE

Tactical-Cooperative (COOP)

- Represents a tactical access control scenario
- Subject is cooperative
- Operator faces challenges with the environment
- Collection is outdoors
- Operator is wearing an urban tactical kit, which may include shooting gloves, helmet, vest and a rifle

Test Scenario 3: UNCOOPERATIVE

Tactical Uncooperative (UNCO)

- Represents a hostile post-objective scenario
- Subjects actively impede collection of biometric data by clenching their fists, closing their eyes, and generally resisting operator instructions
- Subject is handcuffed, irritated, and combative
- Collection is outdoors
- Operator is wearing an urban tactical kit and may be carrying additional equipment




Test Scenario 4: NIGHTTIME

Night Tactical-Uncooperative (NIGHT)

- Represents a hostile nighttime post-objective scenario
- Subjects actively attempt to impede collection of their biometric data by clenching their fists, closing their eyes and generally resisting operator instructions
- Subject is handcuffed and irritated/combative
- Operator is wearing urban tactical kit, a headlight, and may be carrying additional equipment

Test Scenario 5: EKIA

Enemy Killed in Action (EKIA)

- Represents a post-objective scenario at night when operator encounters a deceased enemy combatant
- Operator is instructed to maintain light discipline while performing the biometric collection




Morgue Testing

- Prior to TBE-12, five of the six collection devices were used by experienced operators to collect fingerprint and iris images from cadavers.
  - Assess device utility to collect and match iris images from deceased individuals
  - Confirm the ability of the active capacitance sensor to collect fingerprint images from deceased individuals.

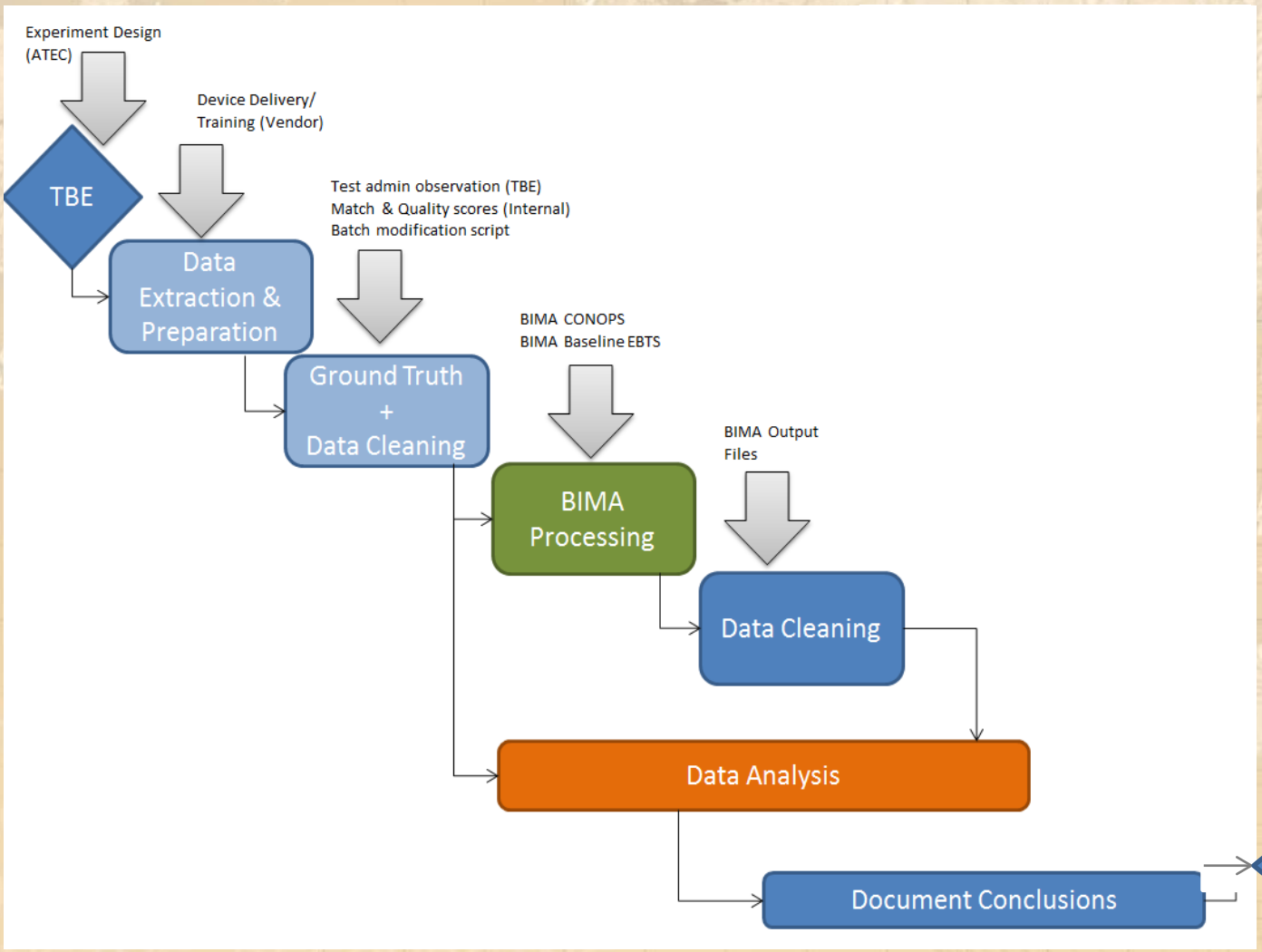
Test Resources

- Leadership: Southern Methodist University
- Design of Experiments (DOE) collection: ATEC
- Devices and training by vendors
- Participants selected
  - 12 Military operators
  - 12 Arabic role players
  - 6 Test administrators
- Five Test scenarios

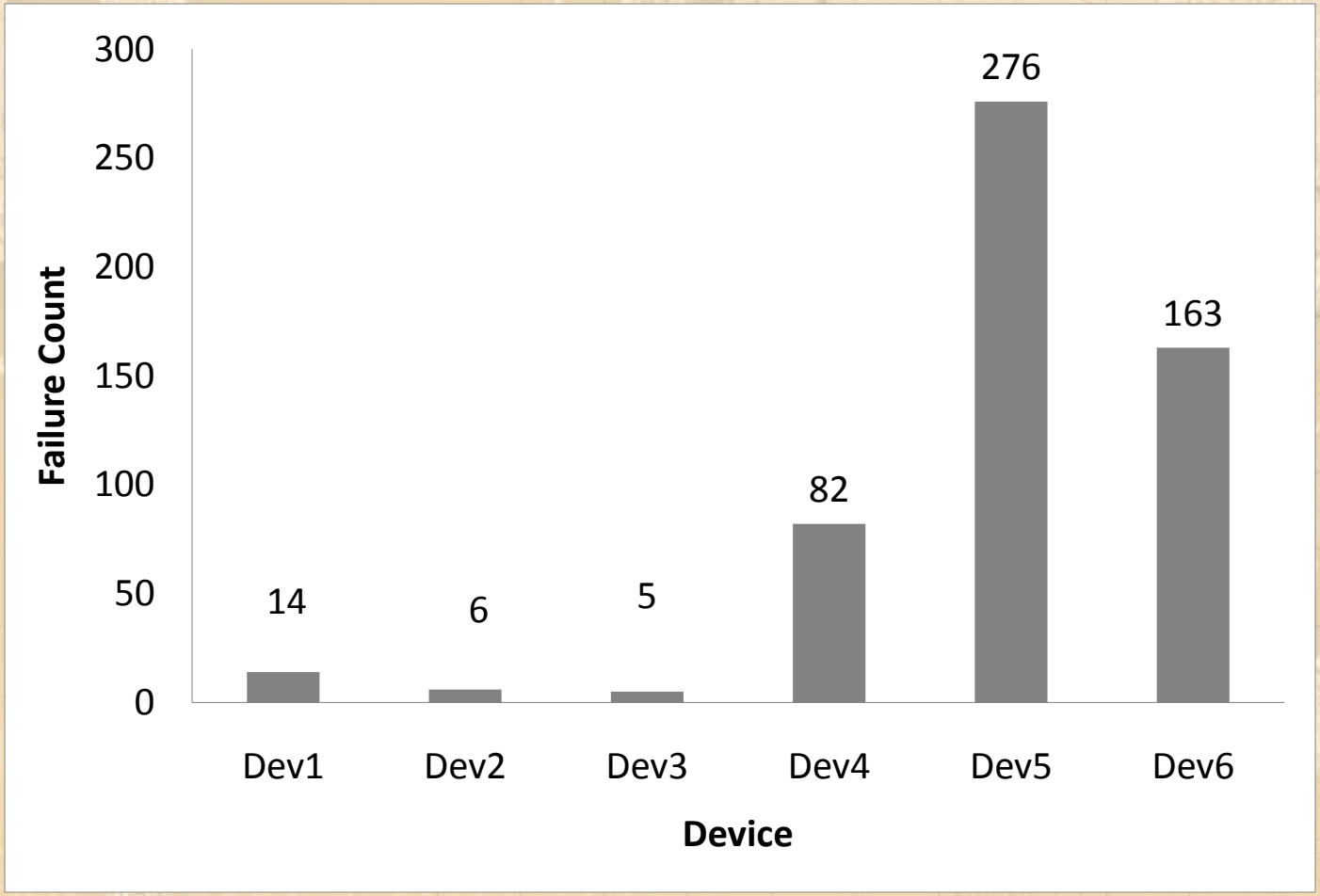
Reference/Ground Truth Collections

Modality	Collection Device	Collection Method	Example Image
Fingerprint	Ink and Paper (Roll & Slap)	Collection by certified collectors from BIMA with operational field experience; each subject collected twice. Prints of highest quality for each subject were used in the evaluation.	
Face	Canon Powershot D90 with standard backdrop	Indoor collection with uniform passport background, neutral subject expression, collected at 1 meter.	
Iris	IrisID [LG] 4000	Images inspected manually using the IrisID ICAP quality tool	

TBE Analysis Plan



Total Fingerprint Operational Failures



Tactical Assessment

- Subject Matter Experts (SMEs) with substantial operational experience and expertise in tactical biometric collection served as the Tactical Assessment Team.
- During the assessment, SMEs subjectively determined the threat level for each device based on the amount of visible light emitted during nighttime biometric collections.
- Observations were made from 25 to 50 meters during collections in the EKIA scenario.

Device	Threat Rating	Comments
Device 1	Level 3 - Low Threat	Device had a low light signature - device produced no more visible light than headlamp used by operator; however, the user needed headlamp light in order to capture face and iris - blinking red LEDs on back of device were visible.
Device 2	Level 2 - Medium Threat	Device's fingerprint platen emitted no light; however, the screen was significantly brighter than the screens of the other devices, increasing the device's signature and somewhat illuminating the collector and subject.
Device 3	Level 1 - High Threat	Both the fingerprint platen and the screen emitted significant light, enough to illuminate the collector and the subject.
Device 4	Level 3 - Low Threat	None
Device 5	Level 3 - Low Threat	Device produced no more visible light than headlamp used by operator.
Device 6	Level 3- Low Threat	Blinking red LEDs on device were visible during collection.

Operational Impact. The Tactical Assessment Team noted that all of the devices posed a threat when the operators collected face and iris images because the device must use illumination to collect these modalities.

Final Assessment & Lessons Learned

- No new device showed ***significant*** improvement over the baseline devices
  - Some devices performed better in certain areas
- Vendors are largely unaware of operational requirements for tactical devices
  - Test scenarios and evaluation results were briefed to vendors in April
  - Vendors can use feedback to improve performance
- Vendors are not implementing Development Test & Evaluation procedures
  - Substantial number of software and interface based errors observed
- The tactical biometrics community now has an established process to plan and execute relevant Operational Test & Evaluation of devices in tactical scenarios
- A follow-up Tactical Biometrics Evaluation will likely be used to reassess improved products once the vendor community has had time to assimilate results

Questions?