BIOMETRICS TASK FORCE

Keynote Remarks Given by Dr. Myra Gray

IDGA'S BIOMETRICS FOR NATIONAL SECURITY AND DEFENSE
FINAL
March 16, 2010

BIOMETRIC TECHNOLOGIES AND CAPABILITIES
Enabling Biometrics Across The Enterprise For The DoD;
Supporting The National Security Strategy

[Slide #1 -- Title slide]

Good Morning. My name is Dr. Myra Gray and I'm the Director of the Biometrics Task Force and serve as the Executive Manager of DoD Biometrics. I'm happy to be here today to speak to you about ***Biometric Technologies and Capabilities***; *Enabling Biometrics Across The Enterprise For The DoD and Supporting The National Security Strategy.*

[Slide #2 – DoD Biometrics Current Structure]

Many of you are quite familiar with DoD Biometrics, our structure, mission – and even some of our challenges. For those of you who may not be, let me

give you a brief overview. In the current structure, the Biometrics Task Force reports into the Secretary of the Army through the G 3/5/7. We work very closely with the DDR&E - PSA for Biometrics, Mr. Lemnios and the Director, Defense Biometrics, Mr. Dee.

[Slide #3 – BTF Organization]

To support me as the Director, the BTF has 3 Deputy Directors who oversee integration, operations and serve as the military deputy. BTF is organized into 4 directorates: *Strategic Integration*; *Capabilities Integration*; *Enterprise Support* and *Operations Support*. We have two primary locations: Crystal City, VA and Clarksburg, WVA. Our Automated Biometric Identification System (ABIS) resides in Clarksburg. The DoD Directive 8521.01 provides the guidance and organizational responsibilities for overall DoD biometrics capabilities and direction.

[Slide #4 – Mission and Vision Slide]

The BTF's mission is to lead Department of Defense activities to program, integrate and synchronize biometric technologies and capabilities and to operate and maintain DoD's authoritative biometric database, ABIS, to support the National Security Strategy.

[Slide #5 – Triad Current]

But of course, we don't do this alone. We work very closely with our interagency partners at DoJ and DHS/DoS. Data flows across agencies as we continue to improve and modify our processes and interactions.

[Slide #6 – *Triad Future*]

And hopefully, in the not too distant future, our relationship with these federal agencies – along with state and local agencies – will be completely symbiotic. We will share the same holistic approach to the way data is shared and transmitted and how biometrics benefits all of us.

[Slide #7 – Impacting the Warfighter Video]

The following video will give you a general overview of DoD biometrics: *Impacting the Warfighter and Beyond*

[Slide #8 – Current DoD In-Theater Applications]

As you saw in the video, biometrics are currently being used in Iraq and Afghanistan to enroll detainees and suspected terrorists. As you can imagine, many of the most dangerous targets move throughout the countryside or hideout in urban enclaves. Finding these individuals and successfully restricting their movement is critical to ensuring safe passage of lawful citizens and coalition forces.

It is also is an effective way of derailing organized terrorist acts and limiting communication between those planning to harm people or property. The more we know about this kind of person…including who they are, what they're planning, who they associate

with and what their intentions may be…the better off we will be in fighting terrorism and restoring peace and order.

[Slide #9 – Current Environment]

Since we've been collecting biometric data, we now have over 3.3 million total records stored in ABIS, which represents over 2.2 million total identities. Of those, there have been approximately 1.3 million matches so far.

Everyday thousands of records are collected and sent to either compare against existing records or to store. Those records are coming primarily from Iraq and Afghanistan but other parts of the world too.

As a result of the ABIS system, we had our 1st positive identification in July 2004. This central, authoritative, multi-modal biometric data repository, provides search and retrieval services and interfaces with collection

systems, intelligence systems and other deployed biometric repositories across the federal government. Improved functionality now expands the ways the data can be used. New software algorithms and additional modalities are improving response times and providing better matching results.

Faster response times and more accurate matches translate into better identification utilizing fewer biometric examiners and providing quicker feedback to the query. Previously the response time had been several hours to a few days.

The technology is improving such that now a Priority 1 match on a record can be made in under two minutes from a theater submission to response to the warfighter. The average overall response time is 3.37 minutes.

We also make matches from latent fingerprints and other *found* evidence. Our first latent match occurred in November 2004.

[Slide #12 – Business Functions Slide]

But in addition to biometrics being used by those fighting on the front lines or in harm's way, biometrics is being used to improve and streamline DoD business functions and processes. The use of biometrics to verify personal medical records or restrict access to a secure facility is growing by leaps and bounds.

There are so many applications across DoD that could benefit from the efficiencies and accuracy of biometrics, it's hard to imagine them all. So let me tell you about a few common applications:

1. Facility access:

The comings and goings of people, vehicles and goods at military installations and DoD facilities is 24 by 7. Whether it's the rush of workers scurrying to their cubes in the morning or the stack of pizzas being delivered for a party on base – someone / something or both – is monitoring that movement. And they need to know in seconds who is entering an office and if they should be.

[Slide #13 – Facility Access/Checkpoint Slide]

Likewise, vehicular traffic at DoD facilities presents special challenges. Identifying drivers is one thing, but what about passengers? Delivery services such as Federal Express and UPS make their money delivering packages in a timely fashion and don't want to be held up day-in and day-out because of inadequate or slow security procedures and systems. Compound that with the challenges of delivering dangerous, valuable or perishable goods. Everyone wants to make sure these deliveries get where they're

supposed to be safely and securely – whether they're delivering or receiving the goods.

[Slide #14 – International Waterways]

In addition to trucks, rail and cars, a tremendous amount of cargo and supplies are moved on ships throughout domestic and international waterways. And who would have thought that in 2009, "real" pirates would still be sailing the seven seas with the intent to burglarize and terrorize commercial shipping traffic and wreak havoc on ports and maritime commerce?

Being able to identify rouge pirates using biometrics as readily as we do suspected terrorists on the ground, will ensure safe passage on the high seas and keep the 21st century pirates at bay.

[Slide #15 – Iris Scan]

2. Physical access

Getting into buildings, bases, Navy yards, air fields, camps, offices, ports and other DoD facilities is just the beginning. Once inside, the movement continues. Today we use an array of badges, pins, codes, Smart Cards, magnetic strips – not to mention physical deterrents such as locks, fences, barriers, alarms and the like – to screen who should have access to what and when. It's complicated and slow -- particularly when people leave, get promoted or start a new job.

You may remember from the video that iris scan technology is currently in use at the Army Materiel Command building at Ft. Belvoir, Virginia. The young woman you saw, who was previously enrolled in the system, simply addresses the iris scanner outside the secure access point. Her identity is verified as well as her need to access the secure area. Once confirmed, the door unlocks letting her easily and quickly pass through.

Our success as the greatest defense force in the world comes in part, from creating and maintaining classified systems and information that must remain secure. Limiting the access to secure equipment and information is crucial. Biometrics can be used to control access and monitor movement. From the smallest file cabinet to the largest server room, utilizing biometrics provides a faster, more efficient and more secure level of access control.

[Slide #16 – Information Verification]

3. Information Verification

But what if facility access or physical access really aren't the issue? You're retired and no longer driving on base or handling classified documents. Let's face it…we live in an information-driven world. No matter what you do or where you go, you constantly need to know your name, address, zip code, phone number, social security number, relevant account number,

password, pin number, blood type, passport number, credit card expiration date, security code, mother's maiden name, city where you were born, favorite sports team, pets names, favorite high school teacher (okay, I made that one up), but I could go on and on.

So why not use biometrics instead of so many arbitrary bits of information – many of which change and can easily be forgotten or compromised – to provide identity confirmation to allow access, for example, to medical or employment history or speed financial transactions?

Yes, biometrics is here and it's only going to get more prevalent as we – both at DoD and otherwise – realize the benefits. So let me share with you a few examples of how it's working both to take the worst of the worst out of circulation and make life a little easier.

[Slide #17 – Hoax IED]

On 20 March last year, a soldier discovered what was determined to be a hoax IED device on Al Asad Air Base, Iraq. Anti-American graffiti painted on the wall included the outline of an AK-47 and a hand in the form of a fist, a possible symbol of Hamas. Eight days later, BTF examiners identified two latent prints developed from the scene to two different individuals. The latent matches gave direction in an investigation with limited investigative leads and may facilitate the identification of persons involved in the hoax.

[Slide #18 – Atlanta Airport]

Despite airports being a focus of stringent security measures since 9/11, on 16 March 2009 the BTF received ten-print images for an individual trying to enter the United States through the Atlanta International Airport.

The individual's biometrics were searched against DHS IDENT records resulting in a potential watch list

match. Our certified latent print examiners formatted the prints for submission to the DoD ABIS confirming a Tier 5 “Deny Base Access” watch list hit. Needless to say, that individual’s trip likely ended there without the benefit of frequent flyer miles.

[Slide #19 – Facial Images: Video vs Photo]

Sharing biometric data with interagency and multinational partners is also vital in securing the homeland. On 31 March 2009 facial images received from the intelligence community obtained from still and full motion video resulted in seven positive identifications. Most of the matches came from previous biometric enrollments placing the suspects either in positions of trust in Iraq or for new identification badges. These matches enable the user community to target, track, and prosecute known or potential adversaries and demonstrate the power of multi-model technology.

[Slide #20 – Wikipedia Entry]

Another dramatic example involves the case of Swar Khan. Mr. Khan has a "rap sheet" a mile long, which in biometric terms translates into many entries in the ABIS database dating back to 2003. But let me bring this case down to even more common level.

Mr. Kahn has such a long criminal history, that he has his own entry in Wikipedia.

Our ABIS records on Mr. Khan showed that he was first captured in January 2003 and quickly shipped off to Guantanamo Bay. He spent several years there and was released from GTMO in October 2006. Fortunately, the latest match to Mr. Khan which occurred in May of this year, will keep him off the streets.

[Slide #21 – Fairfax County Police Department]

Security needs span all facets of law enforcement and information sharing is critical. And while the work of the BTF reaches into the most remote corners of the world, it is also working literally in our backyard. The Fairfax County Police Department (FCPD) has been using digital fingerprints to identify criminals since 1984 and facial recognition technology since 2007. The FCPD operates the National Capital Region (NCR) Automated Fingerprint Identification System (AFIS), a fingerprint identification system connecting police departments of local cities and counties in the Washington D.C. metropolitan area. The FCPD also operates its own jurisdiction's multimodal biometric system called the Northern Virginia Regional Identification System (NOVARIS), which is a fingerprint and facial image repository that currently contains about 500,000 files.

Those files are accessible by three counties and several separate municipalities in Northern Virginia.

Data-sharing agreements are in place between the National Capital Region police departments, which are all collecting biometric data in accordance with established standards and best practices. They also conform to international standards for sharing data with INTERPOL. NCR-AFIS, which contains about 1.5 million files, was updated in 2007 to include facial imagery from arrests – or what we know as the classic "mug shot." This facial recognition technology was successfully used by a Maryland law enforcement agency to identify a bank robbery suspect.

In addition to partnering in the testing of mobile biometric collection devices during future biometric field exercises, we hope to provide NOVARIS officials connectivity and an information-sharing arrangement between its intelligence section and the DoD ABIS that would allow NOVARIS to search against the DoD database if NOVARIS officials suspect that they have data on someone who we might as well.

[Slide #22 – Helping our Veterans]

You may remember the World War II veteran, Christopher Morgan, who you just saw in the video talking about how impressed he was by the hand geometry gate at Eglin Air Force Base. Chris is 85 years old. He was a pilot in the Army Air Corps flying missions from Burma to India.

Like many veterans, he's retired now and living in the Florida panhandle. When he needs medical care, he's fortunate to have a brand new Veterans Administration medical clinic right on the outskirts of Eglin. And he's also fortunate that Eglin has a full service hospital right on base.

But getting from the VA clinic to the hospital was no easy task. That is until a partnership between the Biometrics Task Force, the Air Force and the Veterans Administration was formed that created a

biometrically-enabled gate between the two facilities. Now, when patients like Chris come to the VA medical clinic and need additional tests, volunteers who are enrolled in the hand geometry system there can put him in a golf cart and speed him through the gate and over to the base hospital. He doesn't have to drive from one place to the other – or worse yet, try to find a ride and then pass through the stringent security at the main gates of Eglin.

In this single case, biometrics are allowing an easy way for people who need it the most – the frail and elderly – to have better access to the healthcare they need with much less hassle – now that's making a difference.

These examples are just a few of those that demonstrate: biometrics ARE working. But in order to make biometrics ubiquitous for both the Department of Defense and our society in general, more uses are

developing and expanding every day. These day-to-day uses of biometrics are paving the way to make biometrics an enduring capability because it is working and it is making a difference.

So why is this important? Because attacks of terror happen every day around the world.

- They happen in far away Iraqi battle zones.
- They happen in crowded cities and bustling markets.
- They happen in international waters…on US soil…and in well-traveled airspace – the latest of which we saw on Christmas Day.

And because we are at war with the Taliban in Afghanistan, this work is central to that mission.

[Slide #23 Today in Afghanistan]

So while we're on the subject, let's talk a bit more about Afghanistan. From a biometrics perspective, it's fertile ground. While we *have* planted seeds there, we must continue to provide the nourishment needed to have the biometric operations grow and mature. Like Iraq, Afghanistan is a challenging country with diverse tribes, challenging terrain, minimal infrastructure and limited services – actually, the perfect description of a place where terrorists can hide in the nooks and crannies virtually unnoticed.

But with biometrics, we have a proven way to identify good from bad and friend from foe. We have a way of rousing terrorists from hiding places and denying their anonymity. We can also use biometrics in Afghanistan for humanitarian reasons.

If we've learned nothing from the recent earthquake in Haiti, it's that a system of identifying individuals in a timely, efficient and cost-effective manner can truly be

a matter of life and death. Knowing who is who and who needs help is crucial.

[Slide #24 -- DoD Biometric Efforts]

So where are we now and where are we going?

First, we need to optimize what we have already put in place to meet warfighter needs. The good news is that biometrics and the progress we at the Department of Defense and across the federal government have made in the past several years utilizing this technology and sharing the resulting data IS working. We have successfully connected random and seemingly insignificant bits of information and data into facts and reference points. We work with our interagency partners on a daily basis to connect and share our individual yet synergistic efforts.

Next we must improve the existing architecture for biometrics to ensure interoperability. Just like the

foundation of a well-built home, the building blocks we use to create and expand our data repository must be solid and consistent. Likewise, just as the construction industry adheres to strict standards and performance expectations for materials and systems, so too does the ease-of-use and interoperability for all of us depend on creating and implementing universal standards.

[Slide #25 -- Ensuring the Future]

Finally, we must build what we need to ensure the future of biometrics. Not to say that isn't a complicated and involved process. It is.

But I also hope you realize how important it is to do that because Biometrics is working. It's working to identify known and suspected terrorists, create greater efficiencies, and simplify business functions. And most importantly, that biometrics are MAKING A DIFFERENCE. They are making a difference to the

warfighter in Afghanistan and they are making a difference to retirees like Chris Morgan. There is no going back, only moving forward with DoD biometrics.

Again, I greatly appreciate being here today to give you an update of DoD Biometrics and the work of the Biometrics Task Force. I'll be happy to take some questions.

###