BIOMETRICS
TASK FORCE

Keynote Remarks Given by Dr. Myra Gray
NDIA 2010 Conference
January 20, 2010
FINAL

VISION FOR THE FUTURE
THE BIOMETRIC LINK – CONNECTING THE DOTS

Keynote Address (30 minutes)

[Title slide #1]

Ladies and Gentlemen, Welcome to the National Defense Industrial Association (NDIA). I am honored to be your Keynote Speaker today. For those of you who have come from outside the Washington, DC metro area, we're especially pleased to have you join us today.

Attacks of terror happen every day around the world.

- They happen in far away Iraqi battle zones.
- They happen in remote Afghan villages infiltrated by the Taliban.
- 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.

No one is immune. All we can do is work hard to prepare and protect ourselves and our country using the best resources, people and technology available. And we must demonstrate a sincere and determined attempt to stay one step ahead of the terrorists.

In the aftermath of the Christmas Day attempted bombing of yet another commercial passenger jet, President Obama noted that "we" -- referring to all aspects of the federal government – *failed* to "connect the dots" to identify and stop this attempted terrorist attack before it occurred.

[DOTs slide #2]

And he's right. Whether you call them dots or silos, a narrow view of the importance of our individual missions will not take us where we need to go. We must work

together – both within government and across government, industry and academia – to create and manifest a broad and successful strategy to defeat terrorism as we know it.

So just what are the “dots” in today’s challenging environment and how can we connect them in the most efficient manner to ensure this kind of attack – and other types not yet witnessed – don’t occur again?

In our day-to-day work in DoD biometrics, the “dots” include everything from data collection and analysis to storage and matching. They are also the individual soldiers, sailors, airmen and marines who collect biometrics as part of their jobs. They are the examiners who strain to interpret the minutia of a latent fingerprint. They are the scientists and engineers who look long into the future to visualize and create better, cheaper and faster systems. They are the researchers and teachers whose quest for knowledge and commitment to educate others will perpetuate and expand both the science and the applications of biometrics. They are the people who

ensure that all of our multilateral and interagency agreements are in place with the T's crossed and I's dotted. They are the people who develop our specifics requirements and those who properly and effectively communicate our needs and successes to all the right people. And they are certainly representatives of industry – like you – who strive to improve current systems, expand capabilities and keep us all ahead of the terrorists.

So what does it take to connect all these "dots" into a meaningful and successful operation? It takes a lot. Putting all these dots together is like creating a great work of art – no one dot is more important than another, yet together they form a strong foundation and a beautiful picture. Not to mention the impact they are having in fighting terrorism and protecting the homefront.

Today, however, I'd like to highlight just a few of the critical components we must have in place to connect the dots. First, it takes: [Determination Slide #3]

Determination, dedication and a common desire to identify and take those intent on harming America and Americans out of circulation.

It also takes: [Objectivity Slide #4]

Objectivity and the ability to visualize the bigger picture through the implementation of a common architecture, seamless integration and the interoperability of systems and data.

Furthermore, it takes the: [Transformation Slide #5]

Transformation of business practices, ways of thinking, and operational patterns to create efficiencies never before imagined.

Finally, it takes: [Standards Slide #6]

Standards that are universally acceptable, easy-to-understand, flexible and inclusive.

And if you were really paying attention to what I just said, you might have noticed that the acronym for these four critical areas is:

D O T S. Easy to remember, huh? [DOTS Slide #7]

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 disparate 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.

And through this interagency work, the need to adopt and promulgate a holistic architecture is readily apparent. 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.

Then comes your role as industry…creating, manufacturing and maintaining collection devices and data transfer systems that work within the dedicated architecture and conform to established and agreed-upon standards. Oh yes, and devices that perform faster, cost less, and are more rugged and reliable every generation. Is that too much to ask? Hopefully not, particularly when we hear about the successes we're having utilizing biometrics.

So, let me tell you about a few recent examples:

[Hoax Slide #8]

First, on 20 March 2009, 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.

[Atlanta Airport slide #9]

Second, despite airports being the 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.

[Khan Slide #10]

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. No kidding. No matter how you feel about Wikipedia as a reliable source of information, it’s there. Do you have your own personal entry on Wikipedia?

In regards to Mr. Khan, the online encyclopedia states, *“**Swar Khan** is a citizen of Afghanistan, held in extrajudicial detention in the United States's Guantanamo Bay detention camps, in Cuba. His Guantanamo Internee Security Number is 933. American intelligence analysts estimate Swar Khan was born in 1970, in Khost, Afghanistan. Swar Khan was a security official for the Hamid Karzai government prior to his capture. His boss*

told reporters that his capture was due to false denunciations from a jealous rival, whose sons worked as interpreters for the Americans, and that he had tried to tell the Americans he should be set free -- without success."

Good for us, because among the allegations noted for Mr. Khan are the following:

1. He is a member of the Taliban.
2. He is a former intelligence officer for the Taliban.
3. Mr. Khan participated in military operations against the United States and its coalition partners.
4. He had approximately six truckloads of weapons and ammunition including mortars and artillery stored in his house.
5. He was selling weapons and ammunition that were allegedly used against coalition forces.
6. The detainee swore written allegiance to the Union of Mujahadin under Commander Malem Jan Sobari, who is a Taliban guerrilla warfare leader in certain areas of Afghanistan.

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 2009, should keep him off the streets. He was detained by US Forces-Afghanistan at Regional Command East.

[Fairfax Police Slide #11]

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." Recently, 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.

These examples are just a few of those that demonstrate:

1. Biometrics ARE working.
2. Those involved in biometrics across the federal government ARE working together.
3. And those across all sectors – government, academia and industry -- ARE collaborating and sharing critical data, important successes and a common vision for the future of biometrics.

In other words, connecting the DOTS.

[Business Functions #12]

But in order to make biometrics ubiquitous across the federal government and our society in general, more uses need be developed and applications of the technology

expanded. Ordinary day-to-day uses of biometrics are paving the way to make biometrics an enduring capability. Some of those non-combat areas of the Department of Defense that are currently benefitting from biometrics include:

- Facility access [Slide #13]
    - Monitoring pedestrian and vehicular traffic at bases, ports and military installations
- Physical access [Slide #14]
    - Controlling secure areas and limiting cleared personnel
- Information Verification [Slide #15]
    - Providing identity confirmation to allow access to medical or employment history or speed financial transactions

[Eglin AFB Slide #16]

Take for example, biometrics in use at Eglin Air Force Base in Florida. Despite having a state-of-the-art Veterans Administration Medical Clinic adjacent to the base, getting from the VA clinic to the base hospital for

additional treatment or tests was no easy task. That was especially the case for the many elderly, retired or disabled veterans living in the area. That is until a partnership between the Veterans Administration and the Air Force was formed that created a biometrically-enabled gate between the two facilities. Now, when patients come to the VA medical clinic and need additional tests, volunteers who are enrolled in the hand geometry system there can put them in a golf cart and speed them through the gate and over to the base hospital. The patient 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.

[Dot Slide #17]

So as you spend the next two days here learning more about biometrics, hearing from those inside government and those across the industry, and sharing important updates with your colleagues, I hope you will all strive to connect the dots. Or, if nothing else, I hope you will at least remember my definition of that acronym as an

inspiration for moving biometrics forward: **D**etermination, **O**bjectivity, **T**ransformation and **S**tandards.

[Animation of last slide]

Just like no one is immune from terrorism, no one alone can advance biometrics. We must all work together so that biometrics curtails terrorism, fortifies our security systems and just plain makes our lives easier.

Thank you.

###