Keynote speech to Biometrics Consortium Conference
Wednesday, 0830, September 28, 2011, Tampa, FL.
By John Mears, Director of Biometrics and Identity Management, Lockheed Martin Corporation

The Future of Biometrics: Realizing the Promise

Good morning! And thank you for attending the Biometrics Consortium Conference. I'd like to thank AFCEA and the Biometrics Consortium for inviting me to keynote this important gathering of industry, academia, and government.

Exactly a year ago ***today,*** on Sept. 28, 2010, the National Research Council issued a report which said: *For nearly 50 years, the promise of biometrics has outpaced application of the technology.* A bold statement! And not entirely untrue …

I come here today, a year later, to tell you there *is* great promise, and we can use biometrics in varied ways to serve citizens of this great nation, and the world—through access control and credentialing, through criminal apprehension, through programs that aid commerce and preserve privacy—if we overcome critical challenges in three areas – I'll come back to what those are in a moment.

First, however, I'd be remiss if I didn't give credit to what motivates my remarks today. The NSTC subcommittee on Biometrics has been soliciting industry inputs to the update of the 2006 National Biometrics Challenge document. Also, In June of last year, Peter O'Neil from FindBiometrics asked me to moderate a Webinar entitled "Interoperability: At the Intersection of Policy and Public Perception ". A novel feature of the Webinar was the live opinion poll wherein we asked the listeners to vote on what they thought were the major challenges to the successful applications of biometrics today. The usual suspects got the most votes: interoperability, standards, and technology, with very few votes for policy, perception, and public law.

Now, as a recovering engineer, I can understand the tendency to believe that we can solve all problems with technology, standards, and interoperability.
Peter asked me if the result surprised me, and I had to admit to him that it did. I thought, that after moderating a Webinar that had "policy and perception" in the title, that there would be more recognition that these are truly tough issues – usually outside the domain of what engineers can address. The issue has bothered me since, and I am very certain that we, as an industry, need to become far more active in addressing the first of my three critical challenge areas. I call this first challenge area the "3 P's" - Perception, Policy, and Public Law.

The second challenge area is related to the financial realities that we all face today, although I believe that addressing this challenge area also helps to address perception issues we all face. That NRC report last year went on to quote that "while long on ideas, the <biometric> business has been short on profits." I believe that biometrics are best applied in specific mission areas, for specific purposes, often in conjunction with other factors or security measures, and yielding quantifiable financial benefit. If this can be done, I believe the operators of biometric systems can justify their business cases to themselves and their constituents, and suppliers of biometric systems can more clearly see opportunities for revenue and profits – which isn't a bad thing, since the industry is not viable without profits.

The third challenge area I'll address today has to do with education along two dimensions, and associated technical vitality for realization of that future promise. I believe as an industry we need to become more pro-active in educating the public, and as an important subset, our legislative representatives. Can we really expect to overcome perception issues, achieve good policies, and realize good laws related to our industry without making a strong effort to impart at least some of the domain knowledge we have that others don't? In the tactical time frame, we must do this. Strategically, I believe we need to support basic R&D efforts, and we need to foster STEM education (science, technology, engineering, and mathematics) to ensure the vitality of our future workforce.

I'll reference these challenge areas as "touchstones" as we talk about "Realizing the Promise" in three parts today. First is "The Promise Achieved – Success Examples".

The Promise Achieved: Success Stories

Here's where I'm going to diverge from the NRC report statement. I think the examples I'm going to give show that their applications of technology have definitely matched the promise of biometrics. Some of these four examples are from my own frame of reference within Lockheed Martin, and some are outside – I'll try to use some local examples as well.

Speaking of local, we have a number of people here from Orlando, and they include some of the people who worked on the FBI's original AFIS. It is a little known fact that may be of interest to you that our original AFIS work started with terrain-following cruise missile technology being developed in Orlando at the time. It required fast pattern recognition to match what the cruise missile nose camera was seeing versus terrain maps stored in memory. One of our engineers reasoned that if we could do fast pattern recognition on terrain, perhaps the ridges and valleys of the terrain weren't so different from friction ridges on a finger – just different scale. And so our two decade history in biometrics was born.

Today, we are proud to continue that legacy through our work with the FBI on the **Next Generation Identification** system or NGI.

I believe NGI will be the most advanced multi-modal biometric system in the world. NGI's modes include finger, palm, latents, face, and an iris study. It is being delivered in 7 increments, starting with increment 0, going through 6 (there are obviously some other recovering engineers on this project).

Some of NGI's early successes include several hundred automated hits above IAFIS when the two systems operated in parallel during NGI's first week online. Can you imagine the investigative time and money saved as a result of this development? There's also the Repository for Individuals of Special Concern (RISC) story, in which several cities participated in patrol-car based livescan fingerprint matches that took less than 20 seconds response time against a database that contains the "worst of the worst."

Another example: **Pinellas County's Facial Recognition**. During an NIJ workshop presentation by Scott McCallum, Sheriff's Dept. on Feb 24-25 of this year in Washington, DC, we heard about an unsolved murder of a young woman, with few leads. Facebook revealed unknown person, and facial matches against driver's license DB revealed suspect with multiple aliases. Evidence developed as a result solved the case.

A third example: **The Transportation Workers Identification Credential (TWIC)**. This post-9-11 initiative to secure our maritime ports has almost 2 M enrolled, and over 1.8 M cards printed. As a credentialing program, it is very successful. We also have learned lessons, as some detailed in GAO reports, that can apply to secure Medicare cards and potential worker ID cards. This new GAO report was issued September 10, entitled "Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards"

Finally, there is the **USCIS – DoS DNA trial**, where we saw evidence of fraud in petitions to bring in relatives after residency granted. This joint DHS-DoS 2008-2009 program implementing DNA testing revealed candidates from certain countries either lied about family relationships or failed to show for the testing 87% of the time. Worthy results were shown in 20% of the asserted family units. This demonstrates the potential of rapid DNA analysis to reduce fraud, reduce costs, and allow our immigration officials to focus on the truly worthy cases. A good business case.

With the advent of rapid DNA analysis technology, the ability to do this simple testing can become more routine, and could be done at consulates and embassies around the world, in addition to our own immigration facilities here in the US.

Of course there are lots of other applications of rapid DNA analysis as a biometric, and I recommend you stay for Dr. Tom Callaghan's panel discussion after this for more information on exciting developments in the application of this emerging technology.

I think these program successes show how we can advance security and reduce fraud, while lowering costs for governments, by implementing focused, mission-specific programs to significant effect. In addition, I'd assert that if the general public can understand these benefits and their associated business cases, we'll see an improvement in the perception of our industry, along with a quickening of the adoption of progressive policies and laws which take advantage of the power of biometrics, thus closing the gap on the NRC's "promise vs reality" statement.

The Promise Unrealized – Challenges

Biometrics hold great promise, but the industry must address critical issues if we're to step up to the NRC challenge. We must become more active in shaping perception, policy, and public law:

Perception

The NSTC and IBIA list of top public perception issues to be addressed include:

Biometric systems gather too much personal information. I have a hard time personally understanding this concern, since we are all presenting biometrics publicly here today (face, iris, etc.). However, I can understand this when the subject of DNA comes up. Some people think if you take their DNA in the context of biometrics and identification, you can tell something personal about them. The truth is that sections of the genome useful for ID were picked in part because they don't seem to code for any characteristic or trait we know of—but do people know this? Probably not.

The 13 markers in CODIS exhibit this characteristic, rendering them to be little more than a "DNA fingerprint" useful for identification, but not for anything else personally identifiable. Perhaps this is why Congress, in an act of wisdom, enacted the DNA Fingerprinting Act of 2005. The act, among other things, says DNA may now be taken from anyone in federal custody. It isn't widely done, though, perhaps reflecting the practical limitations of our ability to extract the profiles, as well as the backlog of more important samples. The only personally identifiable information in current DNA profiles for biometric purposes is the sex of the individual, derived from the amelogenin gene. I don't believe, however, that in our lifetimes we'll see instant DNA identification used for access control, like in the movie "*Gattaca",* nor will we see complete genetic profiles being used for some misguided utopian eugenics objectives.

The truth is that DNA as a biometric is becoming more useful, and backlogs are growing – for conviction ***and*** exoneration. I think all of us should get behind the benefits this can provide to society. There are some concerns I'm seeing, going the other way, however.

- **Biometrics will be collected and shared without permission or adequate explanation.** The privacy policy for each application needs to demonstrate the content and limits of the use of a biometric.

- **Biometrics can be used to track individuals.** NSTC's position again says system limits need to be explained.

- **Biometrics reveals personal medical status.** Not only should the limit be explained, but limits should be verified through system audits, NSTC says.

- **Biometrics can be cut off and used.** We've seen this graphically illustrated in movies like "Minority Report", and TV shows like "24", and we need to respond to this concern by demonstrating how we would protect individuals from this type of attack, through such technologies as "liveness detection", which is a common feature in our industry, I'm happy to say.

- **Biometric technology can injure you.** Again, education is needed on collection mechanisms, such as how iris recognition cameras, not lasers, photograph the eye in this biometric.

- **Biometrics are inherently fallible because they're not secrets, like PINs, passwords, and encryption codes.** Who here thinks PINs and passwords are infallible?

- **Biometrics are inherently fallible because they're probabilistic in nature, unlike PINs, passwords, and encryption.** I think the people who write password crackers would beg to differ with this statement. Our lives are inherently probabilistic. We use terms like "the preponderance of the evidence", and "beyond a reasonable doubt". We talk about "80%" solutions. If we all waited for 100% certainty, we'd never be able to live our lives.

Now, before this gets too heavy, I need to stop and tell you a little story to illustrate my point. It contrasts idealism and pragmatism. I picked up this story at an Engineers Anonymous meeting. Three young men from the University of Florida were vacationing on Clearwater Beach near here. One was a philosophy major, and he considered the other two to be dweebs, and he teased them constantly. Of the other two, one was an engineer, and the other a mathematician.

The philosopher addressed them. “Do you see that beautiful girl about a hundred meters down the beach?” They said “yes.” “Here’s the deal, you can have a date with her if you can get to her, but here’s the catch: you can only move half the distance to her in any one move.”

The mathematician gave up immediately, since all he could imagine was an infinite number of moves that never got to her. The engineer took the challenge, because he knew he could get within arm’s length. He got the date. Here’s the moral of the story: Know your application and its limitations. Sometimes close is good enough.

- **Biometrics aren’t revocable when stolen, like PINs, passwords, and encryption, so people are always vulnerable.** First, there are only a few limited cases when I’d recommend using biometrics as the only authentication factor. As well, the industry is working on revocable biometric techniques, sometimes in conjunction with encryption – again, a multi-factor approach.

- **Biometrics are costly.** This view often is exacerbated by unsubstantiated numbers, sometimes from otherwise credible sources. An example was the GAO’s report (May 2011, p.38, first sentence in the conclusion) that estimated the cost to install TWIC card readers in the ports to be $billions. An IBIA analysis with inputs from industry estimated the cost at $375M.

- **There are no discernible benefits, such as reduced levels of risk or fraud.** I’ve just given you at least 4 counterexamples.

- **Most biometric projects have been failures in implementation.** I’ve just given you at least 4 counterexamples.

Policy

Let me tell you a story that highlights an example of policy and implementation challenges, sometimes related to perception issues, and certainly created with the best intentions – usually to preserve an important but sensitive tool – like DNA evidence.

Did you hear about the case of the **Grim Sleeper**? The 10 victims of California's Grim Sleeper, who was arrested July 7, 2010, were in the news for more than two decades. The suspect's criminal record stretched back to 1989, but he wasn't caught on the serial murders until last year. They'd captured his DNA at a crime scene years prior but never enrolled him when he was convicted of a felony in 2003, an action called for in California's Proposition 69, which states DNA must be collected for all charged criminals. But probation authorities never sampled his DNA; they lacked resources to immediately collect it. If they had, this guy would have been caught much earlier, before he murdered nearly a dozen women in their sleep.

There are dozens more he may have killed, something police suspected from the 1,000 photos and hours of video collected from his computer hard drive upon his arrest. Police released 180 photos after unsuccessful attempts to identify these possible victims. How did they finally do it? It was only when the police searched the DNA profile database to find DNA with similarity to the profile, to infer a familial relationship, that they were able to locate the suspect's son, himself convicted on a felony weapons charge. Then, they made the link through undercover police work to obtain DNA on pizza crusts at a restaurant the suspect frequented to match the DNA in saliva found on the victims. If the policy were different, if the technology was more convenient, how many people could have been saved in this one example?

Contrary to what you may see on TV, DNA matches aren't accomplished in the time frame of a commercial break.

- At the Federal level, we only upload & do DNA matches in CODIS once a week
- Familial search is not a widespread tool of law enforcement
- We'll have rapid DNA technology in the next year – how will it be used?

- If you want to get a real calibration on where we are with this technology, go to Dr. Callaghan's session immediately after this one.

Public Law

Our efforts at education in privacy, technology, and in the critical budgetary solutions we offer, need to extend to the states, where we're seeing multiple efforts to kill biometrics programs. There is some good news on this front, so let me hit that first.

The best news comes from Virginia, which has approved a biometric Medicaid pilot, thanks in part to lobbying efforts by the IBIA. Virginia is still seeking funding to move forward, but the state and Department of Medical Assistance Services (DMAS) are eager to advance this initiative. It's through programs like this and their success that we'll win over officials in the more problematic states of Texas, California, Alaska, New York, Arizona, New Hampshire, and Georgia.

- **TEXAS** repealed the use of biometrics this year, eliminating an existing biometrics program aimed at eliminating duplication in its food stamp program. It also didn't go ahead with plans to use biometrics in the state Medicaid program. The reason: CMS refused to provide matching funds for biometrics, stating that it violates "maintenance of effort" provisions in stimulus and healthcare legislation.

- **CALIFORNIA** is the midst of a battle to kill its program allowing biometrics to eliminate duplication in its food stamp program.

- **NEW YORK & ARIZONA** also face pressure to stop using biometrics to curtail food stamp duplication. The politics and procedures are different; the issue isn't resolved.

- **ALASKA** introduced legislation last year to preclude the use of biometrics, including verifying identity before taking professional tests—in this case, an accounting test—which was the legislation's impetus. The measure didn't pass but that was because another issue related to oil and gas taxes with the governor intervened. The bill exempted law enforcement and provided a private cause of action.

- Legislation introduced in **NEW HAMPSHIRE** for the past several years has tried to restrict collection of biometric data by state agencies and private entities. It provides a private right of action for the misuse or unlawful collection of biometric data. And it's coming up again.

- In **GEORGIA,** legislation to reduce fraud, waste and abuse in Medicaid was introduced. After considerable discussion, the legislature decided not to include biometrics.

Business Case

Tangible mission benefits must outweigh costs – the new reality. This is certainly true for appropriated programs, and fee-based programs, although more easily financed, must still show significant and publicly acknowledged benefits. If we can do this, we offer world safer, less fraudulent way of life, with greater ease of access to services. In a time of trouble closing budget deficits and reducing debt, Medicare/Medicaid fraud, public benefits fraud, biometrics should be seen as one option to allow governments to recoup millions to close fiscal gaps.

As an example, let's discuss facial matching in airports using 1:N and 1:1 matching for different applications. I spoke to one of my friends in a government agency, and he lamented that, since 9-11, we didn't have any 1:N facial matching applications in our airports for watch list subjects. When I spoke to another agency friend, he said "Are you crazy? The false alarms will drive us nuts. How will we staff this? What are the operational procedures? How do we pay for it?" Should we use facial reco initially only for people who jump the security line so we can re-acquire them in surveillance cameras instead of evacuating the airport and re-screening everyone? We can see continued improvements in technology accuracy and reliability, appropriate to the mission uses. If we make facial recognition more accurate, does the case close? Are there better applications for face?

The Promise of the Future

I personally think that, left unaddressed, significant change in perceptions and policies related to biometrics may take a generation. However, I believe we need to accelerate the pace of change. We can't just sit in our technology-laden ivory towers, develop more technology, and expect good things to happen through natural market and political forces. Seriously, we have to do three fundamental things, for the good of our industry, and for the sake of our society.

First, we need to be more active in informing and influencing policy and public law. We are the experts, and we have a responsibility to help people make the right decisions. Second, we need to spend more time educating, both our legislators and the people they represent. Third, we need to encourage the development of talent – and by that I mean the next generations - to solve the great problems before us.

Informing and Influencing Policy and Law

We need to participate actively in organizations like AFCEA, IBIA, and NDIA, among others, to help formulate positions on the tough policy, perception, and technology problems

We need to support worthy legislation, like Sen. Schumer's worker ID, and the recent bill for a secure Medicare card (Senators Mark Kirk (R-IL) and Ron Wyden (D-OR) and Representatives Jim Gerlach (R-PA) and Earl Blumenauer (D-OR)).

We need to support the NSTC, NIST testing, standards development, and scientific working groups who are working to develop new policies appropriate to the advancement of technology and the progression of public opinion.

We need to help establish priorities. I'll pick one example. Is it right to disproportionately cut the DHS S&T budget, which includes biometrics and human factors? R&D sows the seeds of the future. As someone once said, "you can't cut your way to greatness". It is about making smart choices.

Spend More Time Educating

There are some great resources – like Biometrics.gov.   However, browsing these sites isn’t the first thing people think of when they are challenged with a problem.

For example: The Rep. Mica hearing where FAA and NIST were testifying on why pilots didn’t have biometrically enabled ID cards. The FAA representative stated they need more inter-agency help, and they needed to understand more about biometrics. We should help him!

Congressional staffers told reps of the IBIA that they could use a “Biometrics 101” pitch when the members are on recess.   We are actively working that, and could use your help to be inclusive across the industry. See me afterwards if your company can help.

Encourage the Development of Talent

According to a Duke University study, China is graduating 600,000 scientists/engineers each year, India is graduating 350,000 each year; the U.S. graduates 70,000. The U.S. has been an engine of innovation in this industry, but we often lament that technology invented here is implemented first overseas. With the graduating numbers I just cited, it is possible that the technology could not only be deployed first elsewhere, but also invented first elsewhere.

We need to encourage STEM education – across all levels. Let me tell you about a few of my favorite initiatives in the industry, and invite you to consider similar activities for your business or agency.

- **USA Science and Engineering Festival**, which caters to children of all ages

- **CITeR**, which works with Graduate students

- **AFCEA’s teaching scholarships**: In 2011, AFCEA is giving out 56 scholarships of $5k each to STEM teachers. If they graduate and become a STEM teacher, recipients get a $1k Science Teaching Tool grant per year for 3 years, provided they stay in STEM education. The AFCEA Educational Foundation and AFCEA chapters deliver over $2M a year to students and teachers in STEM fields.

- **Lockheed Martin's biometric scholarship program with West Virginia University:** Chloe Snyder and Alicia Harmon were 2011 scholarship winners and biometric systems majors in the Lane Department of Computer Science and Electrical Engineering at WVU. Alicia, clearly a leader, had been selected by her peers to be the President of the Student Association for the Advancement of Biometrics. Chloe was a deep thinker. She told me about a new biometric – the amount and types of bacteria in our intestinal tracts. I thought I knew all the biometric types, but she surprised me.

What else will smart young people develop? They are the promise of tomorrow, and generational change may one day be the reason that it becomes "the year of biometrics, the promise realized." We need your help, too. After all, we're building the future for all of us.

Summary

To close, let me ask once again: Can we—together—meet the promise? Are we up to the challenge? It will take work, but we see the great potential here. We in biometrics know that in today's world, an individual's identity is his or her best protection. We know biometrics is a powerful tool to fight crime and terrorism. We know biometrics can keep our world more secure – physically and economically.

So how will we surmount issues of public perception and policy limitations? How will we responsibly address privacy concerns? How will we realize the technology's promise while providing appropriate business case justifications? It's up to you, to inform the world, and to help develop our next generation.

Are you ready to take on the biometrics challenge and realize the full promise?