WRITTEN TESTIMONY OF
John C. Mears
Director, International Biometrics and Identification Association
Lockheed Martin Senior Fellow
Chief Technologist, IS&GS Civil Information Technology and Security Solutions

BEFORE THE
United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Subcommittee on Technology

The Current and Future Applications of Biometric Technologies
PRESENTED
10 am, May 21, 2013

Chairman Bucshon, Ranking Member Lipinski, Chairman Massie, Ranking Member Wilson, Members of the Committees, good morning and thank you for inviting the International Biometrics and Identification Association to this hearing. The IBIA is a non-profit trade group that advocates and promotes the responsible use of technologies for managing human identity. My name is John Mears, and I am a Board member of the IBIA, in addition to being a Lockheed Martin Senior Fellow and Chief Technologist for Lockheed Martin's IS&GS Civil Information Technology and Security Solutions line of business.

INTRODUCTION

The IBIA's key focus is on the use of technology in determining identity. Biometrics, which is one of the technologies playing an increasingly important role in identity management, has begun to permeate our everyday lives. The associated technology is commonly embedded and operating well today within solutions that protect our national borders and ports; identify criminals and terrorists; and secure critical facilities, computers, and networks. Increasingly, we see applications in healthcare, the financial industry, and perhaps most significantly, in personal consumer devices.

As the Committee is well aware, biometrics is not new or radical. People have used biometrics throughout recorded history to uniquely identify themselves, starting with the first handprint "signatures" of authors of paintings on cave walls 31,000 years ago. In fact, I think it is an injustice that that first caveman wasn't given prior-art credit by the patent office for what has evolved into modern hand geometry and palm print biometrics! (Note that in the last week, the FBI has added a national palm print capability to its Next Generation Identification system – NGI.)

The common thread from 31,000 years ago to today is that *it matters who I am*. In my personal relationships, and in my business transactions, *it matters who I am*, both to myself, and to the people with whom I have relationships or conduct transactions. However, in those first villages, people knew everyone intimately – by their appearance, by their voices, by their behavior, by their work products – and by their handprint signatures. It was easy to transact business based on a confident understanding of identity.

The difference today is our large and growing population, and the distributed nature of our relationships. Our relationships and transactions aren't limited to a village of a few dozen people as they were 31,000 years ago. According to the US Census Bureau, the world population today is in excess of 7 billion, and the US population is in excess of 315 million. Our economy is global, and it isn't unusual for us to do business with people almost anywhere on the planet. As powerful as the human brain is, how many of us haven't had problems remembering names and faces? It is a natural part of our evolution as a species that we apply our technology to this important question: *with whom am I dealing?* Further, *How do I keep my personal information secure, so that only I can access it?*

What makes modern biometric use highly effective are technology developments that enable precise measurement coupled with computational power. This allows measurements to be transformed into mathematical representations that can be rapidly and objectively converted to unique and secure identifiers that are quickly used to determine a person's identity. Computers allow this to be done quickly, and across numbers of people in excess of what any individual could be expected to remember.

To-date however, (pending "the singularity"), computers are not sentient, and we have to "teach" them. Compounding this challenge, our view of what constitutes human identity is evolving and becoming more nuanced than our understanding even 5 years ago. In addition, the stakes are becoming higher, whether for law enforcement, counter-terrorism, defense, intelligence, homeland security, healthcare, finance, or e-Commerce.

KEY POINTS TO CONSIDER

Before we dive into the formal definitions, and answer the Committee's detailed questions, we believe it is important to offer some key executive summary points regarding biometrics:

- Unique qualities of biometrics technology to consider
    - It's focused on the "who" – the individual
    - It's easy to use, simple to understand
    - It's inclusive and egalitarian
    - It improves security, lowers risks, and is more convenient
    - It's a contemporary solution for a complex and rapidly changing digital world
    - Given that PIN numbers and passwords are becoming less effective and ultimately obsolete, is there a better alternative than biometrics?
- Substantiating statements extracted from details to follow
    - Biometric technology is real and working today.
    - There are successful programs that prove this:
        - For identification: IAFIS, NGI, US VISIT, DoD ABIS
        - For verification: HSPD-12 PIV, DoD CAC, TWIC
    - Biometrics work better than biographics and other techniques, and are less prone to errors, spoofing, and fraud.
    - Biometrics have evolved from custom development to integration of commercial (COTS) components:
        - Example: IAFIS (1999) vs. NGI (2013)
    - Biometric systems have improved sharply in performance:
        - Example: IAFIS (92% accuracy) vs. NGI (99.6% accuracy)
    - Biometrics are expanding from Government-only projects to probable pervasive use in personal devices and applications due to consumer demand for personal experiences, data and cyber security, and privacy.
    - It is natural for us to take advantage of technology to make our lives easier and better. Identification is a human function that surely benefits from what technology – specifically advances in computing and sensing – can offer.

HUMAN IDENTIFICATION DEFINED

The practice of human identification involves making choices among the characteristics that constitute identity, and then optimizing the statistical certainty until it approaches 1. To this end, what are the choices? How is "human identification" defined?

Figure 1: Elements of Human Identification:

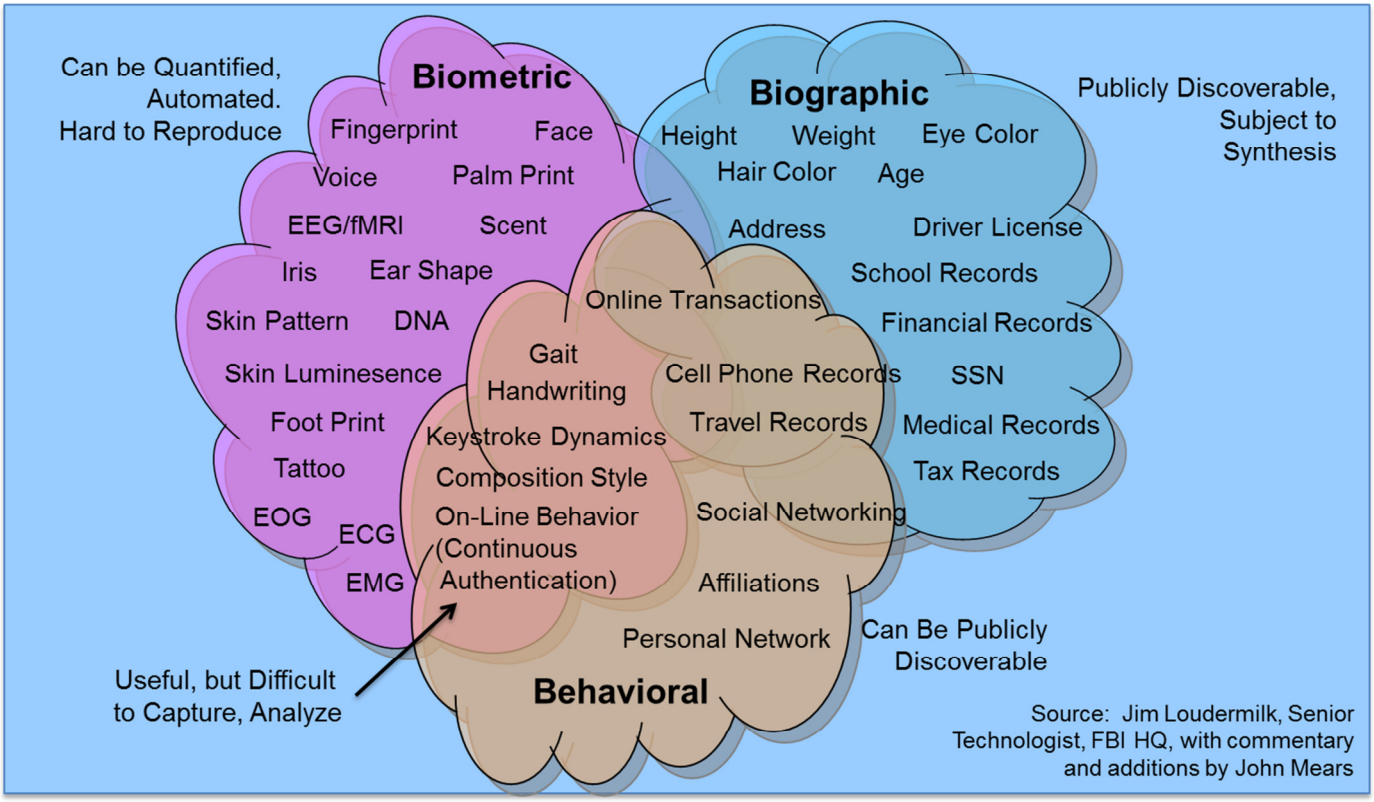


Figure 1 illustrates the three major elements that can define human identity: biometrics, biographics, and behaviors.

The National Science and Technology Council's subcommittee on Biometrics and Identity Management describes biometrics as a characteristic defined as "a measurable biological (anatomical and physiological) or behavioral characteristic that can be used for automated recognition." We are all somewhat familiar with the most common of these, since they include things like fingerprints, faces, irises, our voices, and our DNA. There are many other more esoteric biometrics, including some not listed here (like the type and number of beneficial bacteria in our intestinal tracts). However, as the definition implies, the most useful of these exhibits permanence, and can be easily observed, measured, and automated. The best ones are very discriminating, to the individual, and are hard to spoof or reproduce.

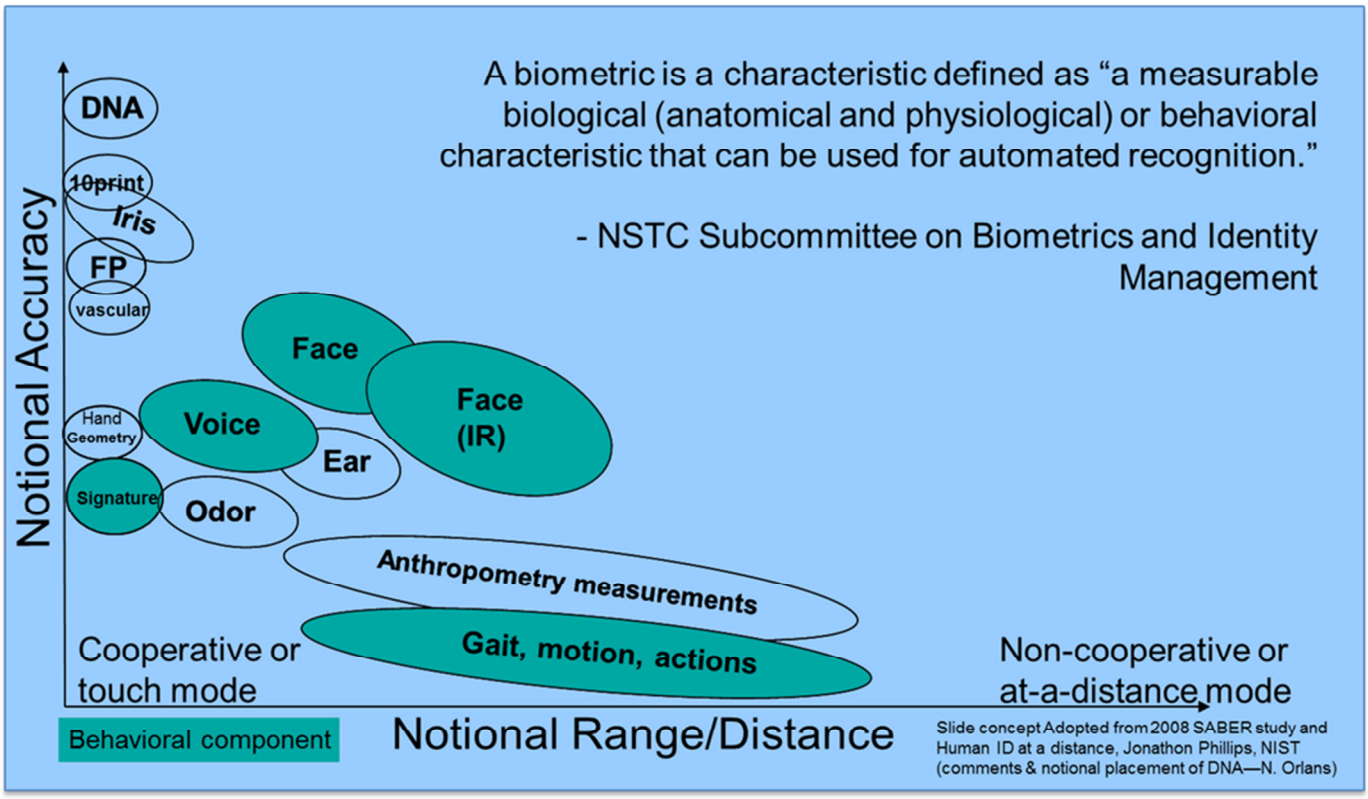
Biographics are descriptors that are assigned by others, or that we attribute to ourselves, but may change over time as we live our lives. These include things like our names, our addresses, our public records, our Social Security numbers. Biographics are useful for identification, but are generally less accurate because they do change over time, can be publicly discovered and spoofed (e.g. identity theft), and public records sometimes contain errors that are problematic (e.g. name misspellings vs. watch lists, and errors in credit reports).

Behaviors are descriptors of our actions over small or large periods of time. They can be classed in two ways: behavior in a group setting; and, individual behavior. Group behavior can be observed, for example, in postings on social networking sites, through on-line transactions, phone records, emails, and affiliations. Many of these group behaviors can be publicly observed, and can be spoofed, as we observed in the Manti Te'o case. Individual behavior includes such things as handwriting, composition style, keystroke dynamics, walking gate, and on-line behavior (useful for an emerging insider threat mitigation technology called "continuous authentication"). Many of these individual behaviors can be difficult to capture and analyze (at present), but are potentially very useful, particularly for logical and cyber security.

In practice, many techniques for authentication (identifying an individual with an asserted identity) and identification (trying to identify an unknown subject against a large number of candidates) use a combination of descriptors of identity. The security industry has evolved to evaluate threats vs. economic cost so that factors are chosen to optimize probability of correct identification vs. application vs. facilitation of commerce. See the appendix for a more detailed discussion of this principle for one example.

Biometrics can increase confidence in identification processes. However, not all biometrics provide the same level of assurance, and many factors impact effectiveness. Figure 2 illustrates this point for a selection of biometric types. The graph shows notional accuracy on the Y (vertical) axis, and notional sensing range or distance of sensing on the X (horizontal) axis. Some biometrics require physical contact for sensing purposes, and some can be accomplished at a distance. Some are best pursued with cooperative subjects, and others do not require cooperation, particularly those done at a distance. Notionally, the most accurate biometrics require touch, or are presently done at short range, like DNA, ten print fingerprints, or iris. Less accurate, although useful at a distance, are biometrics like walking gait, anthropometry, and other remotely observable behaviors.

Figure 2: Characteristics of biometric modalities for different applications:



HOW ARE BIOMETRIC TECHNOLOGIES EVOLVING?

Biometric technology development is accelerating as computing power increases, sensor technologies develop and evolve, and the associated biosciences make rapid advances. Confidence has increased with successful experiences on large programs, and more devices and algorithms from our industry have become commercial offerings, reducing risk and obviating the need for previously large custom development projects. Concerns about privacy, protection of data, and the desire for more personal experiences are driving consumer adoption, which could be the most compelling evolutionary driver that the industry will see. This, in turn, will influence and accelerate the evolution of biometrics in the more traditional domains of usage.

Large successful biometric programs which inform the evolution of our industry include identification programs such as IAFIS, NGI, DoD ABIS, and US Visit, and biometric smart card (verification) programs such as HSPD-12 PIV, DoD CAC, and TWIC. Other countries are pushing forward with ambitious biometric identification programs such as India's Aadhaar program from their UIDAI organization.

Sensor devices are becoming cheaper, smaller, faster, and more accurate, with improved capture quality and tolerance/detection of operator error. Sensors are becoming available at the component level, greatly facilitating incorporation into mobile devices, including smart card readers, laptops, tablet PCs, and smart phones. In addition, general purpose "sensors" like still cameras, video cameras, LADARs, and multi-spectral devices are seeing applications as stand-off biometric sensors for such things as iris and face recognition.

Algorithms for individual biometric modalities have increased greatly in accuracy in recent years, driven in part by algorithm improvements, and part by general advances in computer technology. For example, the FBI's venerable IAFIS system, first deployed in 1999, and running to this day, has a quoted accuracy of 92%, and was largely custom-developed. The FBI's powerful new NGI system uses commercially available algorithms, and achieves an accuracy of 99.6% against the same fingerprint gallery.

Advances in biosciences are being incorporated into evolving biometric sensors so that some of the more "traditionally hard" biometrics come closer to the practicality of fingerprint, face, and iris recognition. For example, microfluidic technology, along with advances in chemistry and microelectronics, have made rapid DNA identification cheap enough, easy enough, and fast enough (90 minutes) to be considered for forward deployment with the military, or installation in police booking stations. DNA-wrapped carbon nanotubes on arrays of field effect transistors show promise as scent sensors, both for human scent as a biometric, as well as other security applications such as explosives, drugs, and contraband detection.

We must acknowledge the contribution of the collaboration between industry, government, and the standards bodies in evolving biometrics. We have the famous Electronic Biometric Transmission Standard (EBTS) message type shepherded by NIST, and I note with interest the adoption of the National Information Exchange Model (NIEM), which has a biometric domain parallel to the EBTS standard. Standards evolve more slowly, but they have a stabilizing effect on the industry (and the consumers of the technology).

As biometric technologies become more accessible, and use cases become more compelling, we are seeing the evolution of renewed interest by healthcare, the finance industry, and organizations working to improve cyber security. In healthcare, there are multiple motivations, from patient identification, to caregiver identification, to narcotics security, billing integrity, and reduction of insurance fraud (to include Medicare and Medicaid). In the financial industry, biometrics are important for employee identification, as well as customer identification, particularly where large transactions are concerned, although there is an overriding desire to simply use biometrics to improve customer service. To this last point, it is consumer convenience, desires for privacy, and the need to protect personal data that may be the most important driver of the evolution of biometrics from this point forward.

HOW DOES INDUSTRY MANAGE THE DIVERSE FIELD OF BIOMETRICS?

Our industry manages the diverse field of biometrics along four different dimensions: tactical; strategic; standards-driven; and disruptive.

Tactically, we are driven by current customer needs and near-term Government procurements. This is often informed by experience on existing engagements and contracts, driving incremental progress and revenue.

Strategically, we look at market trends, competitive assessments, primary and secondary research, strengths, weaknesses, and gaps. We then develop action plans against a projected 5 year market trajectory, looking to fill gaps by R&D, licensing, partnering, or acquiring.

Our development plans are tempered by our participation in conferences, consortia, and standards meetings, so that we evolve offerings that comply with standards, interoperate, and ultimately drive market development for our whole industry.

Occasionally, usually through breakthroughs in R&D, and less often through business model disruption, we discover a previously untapped market segment or niche. Perhaps one recent example of this is the offering of "Identification as a Service" or IDaaS, which is a disruptive new way to provide such services in the very efficient and rapidly evolving cloud computing market.

WHAT RECOMMENDATIONS DOES IBIA HAVE FOR FEDERAL POLICY MAKERS IN THE AREA OF BIOMETRIC TECHNOLOGIES?

Our enumerated recommendations and qualifying comments are listed below:

1. Enhance familiarity with biometrics and associated technology
2. Reach out to understand what has already been done in the US and around the world
    a. What has worked
    b. What hasn't worked
    c. Lessons-learned
3. Use industry organizations (like the IBIA) as a source of information
4. Understand that biometrics can enhance privacy and security
    a. With transparency, good policy, good underlying cybersecurity, and independent audits, then privacy – and public confidence – will be enhanced
    b. IDs and passwords are increasingly hacked, and are no longer sufficient to ensure security and privacy. Fraud and identity theft siphon Government and individual funds. Biometrics present an attractive and effective authentication factor to take security to another level.
    c. Applications of biometrics do not always require a central database – your device or smart card can contain your biometrics within, and be available for local matching

5. When you are assessing feasibility of projects, reach out to industry for the latest cost estimates on available commercial technology
    a. We should all work together to see that cost estimates have a defensible basis, are as accurate as possible, and are based on the latest data (given how quickly technology evolves).
    b. The industry is evolving very rapidly, so commercial function off-the-shelf is increasing while cost is decreasing – just like other aspects of technology evolution.
    c. Much more can be accomplished now through configuring of COTS tools and equipment, without need of costly and time consuming custom development
6. Recognize that different biometrics have different ideal applications – they aren't all the same
    a. Some are dependent on touch
    b. Some are suitable for stand-off purposes
    c. All are statistical in nature
    d. Some are more accurate than others
    e. Using them in combination (something called "fusion"), or with other factors, increases confidence in identity

WHAT DO YOU ENVISION AS THE FUTURE APPLICATIONS OF BIOMETRIC TECHNOLOGIES?

We see the future of biometric technologies in two ways; first, by market segment; and second, by technology to be applied. Looking beyond the current applications in law enforcement, homeland security, intelligence, and defense, we see strong growth against a small current base in several emerging segments.

Future Applications by Market Segment

In commercial and consumer products we see the most potential for dramatic change in the market. People are accumulating more and more personal data and application power in their portable smart devices. This drives a need for more security, and a drive toward personalization. Both of these trends, along with biometric technology rapidly being developed by the smart phone industry, are driving toward biometrically secured smart phone data, and continuous authentication for protection against theft. Generational turn-over will accelerate acceptance as it becomes too compelling and easy to use to reject. As smart, portable devices permeate our lives, so too will biometrics for convenience and preservation of privacy.

In the finance industry, we'll see the acceptance of biometrics for authorization of financial transactions, primarily for convenience and customer service, and secondarily to prevent fraud.

In healthcare, there are a number of applications, from patient identity, to caregiver identity, to billing integrity, narcotic security, and to counter insurance or Medicare/Medicaid fraud.

Cybersecurity is of increasing concern, and many times *who we're dealing with* makes all the difference in defending against cyber threats. For higher-security applications, biometrics can and will be used for access to computers and networks, and behavior monitoring will provide something called "continuous authentication" so that insider threats may be detected and stopped. Migration to cloud computing will enhance our ability to secure our systems by providing a common and secure infrastructure for many applications while simplifying log-on – up to and including presentation of biometrics for the more secure applications.

Future Applications by Technology Type

There are a number of exciting technologies emerging now or on the 5 year horizon:

- Rapid DNA identification. Imagine a time when you can check a person in custody at a police booking station for DNA identification as easily as you can do a mug shot or take their fingerprints. If you can only hold them for 2 hours, wouldn't it be nice to know if they are the serial killer for whom you are looking? Technology is coming to market now from our industry that will allow an untrained policeman to test DNA on a suspect and get an answer within 90 minutes, eliminating the backlog in DNA testing that has resulted in so many criminals going free.
- Simultaneous face and iris capture. Digital cameras are being offered with such high resolution, that soon, with the appropriate lighting both face and iris biometrics can be captured and fused, resulting in very high identity assurance.
- Scent as a biometric. Mentioned earlier, advances in nanotechnology and molecular biology are allowing us to think that scent will soon become a practical biometric. In addition the same technology can be used to detect explosives, drugs, contraband, and industrial process threats so that our world can be made more secure, and man's best friend can go back to being man's best friend.
- Fingerprints can be captured forensically without dusting, fuming, or long and destructive dye treatments. Fingerprints on people can be captured without need of touching a sensor.
- Analytics can be applied to pictures and video to help extract useful identifying biometrics for real-time threat detection and forensic analysis.
- Voice, or speaker identification, will become a more routine biometric, facilitating financial and security transactions, as well as routinely aiding police investigations and sharing of data, much like fingerprints are shared for police use today.
- Portable people identification capability, perhaps embedded in glasses (like Google Glasses) or on a helmet (DoD application for soldiers).
- New biometrics will be explored, driven by biomedical developments (see Figure 1). For example, it has been shown that in small populations (e.g. squads of soldiers), cardio-pulmonary patterns are biometrics.

Our industry is dedicated to making these advancements helpful, secure, and cost effective both for individuals, and our society as a whole.

WHAT WILL THE PRIVATE SECTOR'S ROLE BE IN REACHING THOSE GOALS?

We see value in bringing our real-world experience, across a number of customers and countries, to the pragmatic development of standards and practices, participating with NIST and Government entities in the US and around the world. We expect to continue our innovative research and development work internally, but increasingly work through business alliances and relationships with academia, both directly and through organizations such as CITeR. We will continue to offer new products, services, and business models to the marketplace, where the best will survive over time, thus strengthening our industry.

We expect to play a key role in supporting privacy and associated policy. Related to this, we also expect to have parallel development efforts on counter-spoofing, liveness detection, and cyber security related to biometrics.

We also expect to play an important role in education and awareness. We have a self-interest to educate the market, so that the market will accept – and buy – our products. However, we also need to step up to the responsibility to help our policy and law-makers, since we believe the best policies and laws come from good understanding of the related domains. Not least of our responsibilities is to our next generations. We expect to remain strong supporters of STEM education, not only because it is the right thing to do, but also because it is in our self-interests. We can only continue to innovate and run our businesses if we can get qualified people in sufficient quantity, and in the case of my company, qualified, clearable US Citizens. Only a handful of Universities offer degrees in biometrics at present, and West Viriginia University, founder of CITeR, is one of them. As a result, my company offers scholarships at WVU to worthy biometrics students. However, there are many ways companies can support STEM education. At IBIA, we all know we have to do our parts.

CONCLUSION

First let me say that the IBIA is delighted that you reached out to us for information on our industry. It is one of our recommendations to your policy question that you reach out to industry, particularly for questions of fact or feasibility. We are happy to support formal sessions like this hearing, or even informal discussions with staff. Please do feel free to call on us when you think we can be of assistance.

Biometrics are, by their definition, personal for each of us. It matters *who we are*, both to ourselves, and to the people with whom we have personal and transactional relationships. With the advancement of sensors and computing capability to digitally represent and process biometrics, our lives can be made more secure and convenient on an individual level, as well as for our society. Education and good policy will ensure that security and convenience will always be preserved, even as technology advances. Consumer acceptance and adoption will likely become the predominant driver of widespread biometrics use and advancements, so it is in the interests of our industry to ensure biometrics enhance privacy, security, convenience, and a personal experience

that represents *who we are*. Thank you for your time and consideration today. I look forward to your questions.

APPENDIX

Reference to NIST FIPS PUB 201-2

This principle of matching threat to applications vs. techniques is well-known, and has even been reduced to standard practices, as illustrated in NIST FIPS PUB 201-2, Table 6-2 (reproduced below).

Table 6-2. Authentication for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
LITTLE or NO confidence	VIS, CHUID
SOME confidence	PKI-CAK, SYM-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH

The context is smart identity card-based authentication, although the principle of trading off risk vs. security need is generally applicable to many applications for which biometrics may be appropriate. In this case, simply observing the card ID number and visually inspecting the card (which includes a face photograph), gives little to no confidence that the credential and/or identity asserted are valid. Verifying with security certificates or card authentication keys gives some confidence that the card is valid. Adding the requirement for presentation of a biometric yields high confidence in both the card and the asserted identity. Having an attended (observed by another human) biometric with on card match and authentication certificate verification yields very high confidence that the card is valid and the asserted identity of the human is valid against the stored biometrics.