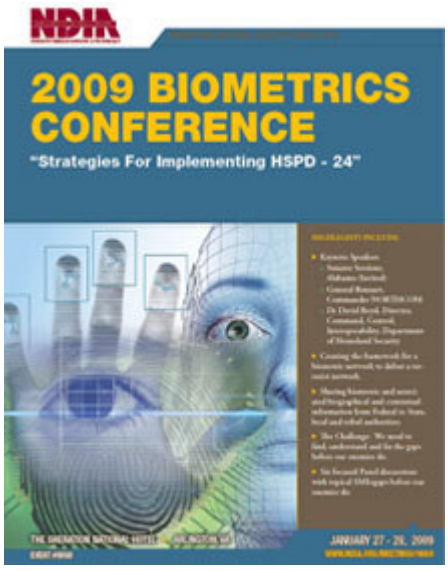
National Defense Industrial Association

# 2009 BIOMETRICS CONFERENCE "STRATEGIES FOR IMPLEMENTING HSPD-24" MEETING MINUTES




**Location: Washington, D.C.**
**Date: 27 & 28 January 2009**

# Table of Contents

### Introduction and Purpose

This document contains detailed notes on selected speaker presentations and panel discussions from the 2009 NDIA Biometrics Conference – "Strategies for Implementing HSPD-24". This document serves as meeting minutes from the conference, it is based on notes taken during the conference, and is not a comprehensive account of every presentation or discussion. The "*Q&A Session*s" are not included in every section, only select questions and answers appear in certain sections, and the lists are not exhaustive. All presentations from this conference are available at the NDIA website.

The author of this document is Mr. Benji Hutchinson. Please forward comments or questions to **james.hutchinson@hqda.army.mil** or call 703-607-1951. Mr. Hutchinson is an Associate at Booz Allen Hamilton. He has 5 years experience supporting large-scale biometrics programs at the Department of Defense (DoD) and the Department of State (DoS). He currently supports the US Army Biometrics Task Force (BTF). Mr. Hutchinson holds an M.A. in International Relations and an M.A in French from the University of Kentucky.

# 1. Day One

### Opening Remarks

From the NDIA Committee on Biometrics, Ms. Martha Karlovic and Mr. Thomas Giboney kicked off the conference by providing a summary of Homeland Security Presidential Directive (HSPD) 24 and an overview of upcoming conference discussions on strategies to effectively implement the goals of the presidential directive.

HSPD 24 is a forcing function – it will require data sharing. Many agencies already collect biometric, biographic, and contextual information in their identification and screening processes. HSPD-24 is about policy, privacy, legal, standards, political, technology and industry initiatives. HSPD-24 directs agencies "to make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security." To effectively achieve the goal of data sharing, HSPD-24 offers recommended biometric standards contained in the *Registry of United States Government (USG) Recommended Biometric Standards*, which is maintained by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (IdM). The goal of sharing this biometric data is to further develop and enhance the USG capability to screen for individuals that pose a threat to national security. Two specific categories named and implied are Known and Suspected Terrorists (KST) and National Security Threats (NST), respectively.

An important action item within HSPD-24 calls for the Attorney General, with the Secretaries of State, Defense and Homeland Security, the Director of National Intelligence (DNI) and the Director of the Office of Science and Technology Policy, to submit to the President an action plan to implement HSPD-24. Two general philosophies exist on how to build such a large-scale biometrics screening capability: centralized and decentralized. A decentralized option would require agencies that identify NST to make info available to other agencies. A centralized option is similar to KST operations. Regardless of the solution, the mission is to manage identities across the full spectrum of mission sets and to develop a biometric enterprise to defeat terrorist networks and secure our borders.

The primary challenges facing the United States (US) biometrics community include interoperability gaps, adherence to biometric standards, lack of clear government policy, and privacy concerns.

## Keynote Speakers

*Key Issues*

- Interoperability & Standards
- Policy
- Consolidation of Congressional Oversight and Funding

### A. Honorable Senator Jeff Sessions of Alabama


Senator Sessions began his remarks by reflecting on the events of September 11, 2001 and underscoring the importance of identifying dangerous individuals by using biometrics technology for screening. Biometrics as a tool strips the cloak of secrecy from threatening individuals, stressed the Senator, and denies terrorists of their anonymity. Biometrics technology is a critical enabler against terror and crime and it is an essential identification technology. The Senator highlighted major advancements in the field of biometrics. He highlighted the implementation of the automated identification systems, such as the capability maintained by the FBI.

The Senator expanded upon the goal of HSPD-24, which is to facilitate enterprise wide USG sharing of biometrics, biographic, and contextual data, to effectively screen for certain categories of threats. HSPD-24 moves us forward to a network-of-networks and will hopefully force agencies to improve existing identification systems. A long term goal is to achieve an enterprise-wide network-of-networks from the federal level to local police. Reaching these goals will increase mission effectiveness through rapid sharing of identification services, which leads to reduced crime and enhanced national security. A layered approach to identification and screening of individuals incorporates federal, state and local authorities.

The benefits to biometrics and identification technology are apparent in deterring illegal immigration and terrorism. Intelligence on various categories of national security threats is the key to success because it deters illegal entry to the US at land borders. This technology encourages people to enter lawfully in an effective way. Identification checks assist border patrol to notify authorities of illegal entries. Further, identification technology and ensuring the data is shared among agencies decreases the chances of another 9/11 by screening for terrorists.

The Senator outlined major challenges facing the USG associated with reaching these goals. Interoperability and policy continue to challenge the USG with regards to sharing data. The Senator stressed the importance of USG agencies purchasing compatible devices that implement consensus-based biometric standards and the need for the USG to continually establish and maintain memorandum of understanding (MOU) between agencies. Another big challenge facing the USG is a lack of consolidation of oversight for funding of IdM and biometrics related programs in Congress. The 9/11 Commission motivated Congress to fund such programs but the Senator warned against complacency.

Public perception is another big challenge facing identification and biometrics technology. IdM in the US is misunderstood, which creates irrational fear. The biometrics and IdM communities need to demonstrate and explain that the technology is not threatening. There is a need to show that identification systems validate good honest people. Examples of lawful use of identification include driver's licenses that prove you can drive a car, allow one to board an airplane, and historically officials were required to have a letter of introduction. The program eVerify is a good example of a modern technology used to verify someone's identity.

*Q&A Session*
Q: Could you comment on the use of biometrics for identification to vote?
A: In New Mexico, citizens do not want an ID to vote. In Georgia, citizens need a drivers license to vote. Close elections, a difference of 200 votes makes a difference and people want integrity.
Q: What will the focus on Capitol Hill be with regard to biometrics and HSPD-24? HSPD-24 is a directive that the Obama Administration will review.
A: We can show systems protect privacy rights, don't threaten our liberties but increase our national security. Not take for granted new administration will understand this. If se overall network undermined by policy changes, tell me. See PD-24 on right road, can sustain and will be received.
Q: HSPD-24 guides the USG to share information. Jurisdictions are an issue. Do you see consolidation of oversight on the Hill?
A: No. Committees take the lead, everyone is in the act after that either to stop it or alter the plan. This is democracy in America. After 9/11 there was a lot of momentum and we got a better system. We were motivated. Having not been attacked since then may lead to complacency and this would leave us vulnerable in the future if systems do not talk to each other. The USG needs to stay on top of this. President Bush had researched the law and the laws are consistent with legal rights.

**B. General Victor E. Renuart, Jr., North American Aerospace Defense Command and US Northern Command (NORTHCOM)**


General Renuart began his remarks by describing his responsibility and the mission of NORTHCOM. The NORTHCOM Mission is to support warfighter and efforts for counterterrorism and regional security and to provide force protection to military installations within the continental US to over 1,400 locations. General Renuart focused his remarks on the challenges associated with his mission and how accurate biometric data and databases support his mission.

Not since the Civil War has the military feared for their families lives in the US. Terrorists do not respect borders. Along the southern US border, a significant amount of weapons and cash moves across the US/Mexico border. This traffic fuels drug cartels. Along the northern US border, snow mobiles are used for transportation across the US/Canada border. Threats from a porous border motivate the use of biometrics and IdM technology. The use of technology allows officials to identify illegal entry at land borders and limits criminal mobility. Over 1 million transited US borders in 2007. Collected biometrics at points of entry stopped 4,000 individual who are criminals. General Renuart stressed the importance of HSPD-24. By building a database that allows users to sense a threat and take action, the US can stop illegal entry and illegal movement of drugs, guns, money and WMD.

The current problem facing NORTHCOM is the vulnerability of facilities to attack and complacency. The US military must become smarter at providing security to its bases. Biometric identification is a viable solution to these challenges. This technology will improve security measures by eliminating the possibility of stolen or forged identification, and improve situational awareness by providing a readily accessible record of who is on base.

General Renuart stressed that the threat to US military installations is real. He provided the example of the failed terrorist plot on Fort Dix, where six individuals planned an assault on the base. The group used a family pizza shop as cover to gain access and conduct surveillance on Fort Dix. The plotters acquired maps of military facilities and planned to slaughter scores of military personnel. A Circuit City clerk discovered a DVD of the men at a firing range and reported it to law enforcement entities at which time the plot was uncovered.

The challenges associated with the application of biometrics technology to the NORTHCOM mission are interoperability, the procurement of standards based equipment, and policy gaps governing the collection of various types of biometric data. The General stressed the importance of pushing industry to build equipment to consensus based standards. DoD must also determine how to push for smarter access control within the existing installation infrastructure. These challenges cannot be put off until the POM cycle. The Services, working in coordination with the Biometrics Task Force (BTF), must facilitate interoperability and common data sets. Common sets of biometric data allow decision makers to provide better security at various points of entry.

## Policy Panel Discussion

*Key Issues*

- Interagency Collaboration on Science and Technology (S&T) Initiatives
- Common Standards
- Agreement and Adherence to Strict Privacy Policy
- Consolidation and Dissemination of Watchlists Across USG

A. Mr. Steve Yonkers , Business Policy and Planning, US-VISIT for Mr. Robert Mocny, Director, US-VISIT Program, Department of Homeland Security
Greatest challenges moving forward are interagency collaboration on technology advancement, common standards, and agreement and adherence to strict privacy policy.

B. Mr. Al Miller, OSD - Policy, *US* Department of Defense
Greatest challenges lie in gaps between capabilities and responsibilities of military and law enforcement entities.

C. Mr. Thomas Bush, III, Assistant Director, Criminal Justice Information Services Division
Moving forward, greater emphasis will be placed on international sharing of biometric data, integrating the intelligence community into unclassified processes, and integrating DNA into the existing USG biometrics enterprise architecture.

D. Mr. Tony Edson, Senior Advisor, Consular Affairs, *US* Department of State
Different organizations capture biometrics to support different missions and HSPD-24 further refines and defines roles and responsibilities for government agencies on how to employ biometrics technology.

## Government Panel Discussion

*Key Issues*

- Consistent Adherence to Biometric Standards
- Obtaining Devices that are Faster, Lighter, and Cheaper
- Political Will to Affect Change
- Common Set of Rules for Sharing Biometrics Data Across the Interagency Landscape

A. Mr. Vickers, Special Assistant to the Director of the Biometrics Task Force (BTF)
Mr. Vickers began his brief with the importance of BTF mission and the implementation of biometrics as a force protection technology. The DoD and its mission is out on the pointy end of the spear. DoD components collect biometrics on population sets of the highest risk for terrorist activity. Biometrics intelligence and data are only valuable when the USG and our allies use it. Purpose of biometrics is to deny enemy anonymity.

"Defense in depth" is a strategy to strip anonymity of individuals abroad and increase the number of encounters with individuals. Moving forward, one challenge will be to engage our multinational allies in sharing efforts to screen threats across databases. DoD Challenges include: interoperability and standards, challenge of obtaining a better, faster, stronger biometrics capability, and the will to impact outcomes through organization, technology, and policy.

B. Ms. Angela Miller, Consular Affairs, US Department of State

Ms. Miller provided an overview of the Department of State (DoS) biometrics capability. The strategy of the DoS is "Open Doors and Secure Borders". The DoS biometrics capability includes three major components: name check, fingerprint check, and facial recognition check.

Fingerprinting at post involves clearance checks. 220 posts send fingerprint data to the Consolidated Consular Database (CCD) which forwards to IDENT, which is a US-VISIT database that contains the biometric information of international travelers to the United States who are enrolled through DHS's US-VISIT program, as well as known or suspected terrorists, criminals, immigration violators and others. Namecheck systems are used to vet applicants of passports and visas. Numbers of name checks have gone from 1,000 to 50,000 from 1970 to 2008. Major Namecheck Tasking – more interagency data sharing, international data sharing of lost and stolen passports, and redesigned CLASS for infinite searches.

The Facial Recognition (FR) System works through the CCD to distribute templates to posts for verification. FR uses three pass analysis: vector feature analysis, local feature analysis, and surface texture analysis (STA) "skin". FR process goes from post capture of face image, to FR software enrollment in CCD, search results are displayed, KCC inspects images, and results return to post.

DoS has the largest facial recognition data base in the world with 73 million images in system. The Chief Information Officer (CIO) of DoS is interested in initiating an iris database. DoS is interested in working closely with BTF to leverage iris technology implemented in Next Generation Automated Biometric Identification System (ABIS). Data available on the CCD is used by DoS, DHS, FBI, DoC, and DoD.

C. Mr. John Kress, Acting Chief, Force Protection and Mission Assurance Division, USNORTHCOM/J34)

NORTHCOM anticipates and conducts Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the US and its interests. From NORTHCOM perspective, biometrics is predominately an interagency effort.

As a result of HSPD-24, the following initiatives need to be initiated: Biometrically enabled access control at all DoD installations, maritime interdiction, protection of borders, and collaboration with all mission partners to share common data. In the defense of our homeland, one central focus is installation access security.

D. Ms Johnna Hoban for Ms. Kimberly DelGreco, Section Chief, Biometric Service Section, Federal Bureau of Investigation

Ms. Hoban kicked off her brief with a statement of how USG agencies are using biometrics for their own mission specific goals. Currently, 60 million records reside in IAFIS, with biometric, biographic, and contextual data all indexed by fingerprints. Next Generation IAFIS will expand upon IAFIS capability to include flat fingerprints, palm, and potentially other future modalities.

Ms. Hoban provided an overview of the Center of Excellence and its efforts in S&T, standards, and other biometrics efforts. CJIS HSPD-24 initiatives include working with NCTC on KST collection,

storage, use, and sharing of biometric and biographic data. DoJ is a co-chair, along with the Office of the Director of National Intelligence, for the interagency working group on NST.

E. Ms. Patricia Cogswell, Executive Director, Screening Coordination Office, DHS

Ms. Cogswell initiated her brief with definitions of screening and a few statistics of the DHS capability. DHS processes 1.2 million inbound travelers at ports of entry, 630,000 aliens. DHS screens 1.8 million domestic air travelers and conducts 135,000 biometric checks for visa applications. This is set to increase to 300,000 per day by next year. DHS processes 30,000 immigration benefit applications, including asylum seekers. DHS verifies the employment status of 3.2 million new employees, which includes a photo tool that returns an image of individuals. DHS manages trusted traveler programs and designs and executes background checks for critical infrastructure workers.

Current DHS efforts in biometrics include: Watchlist service, TSC/DHS efforts to identify existing biometrics, and R&D efforts. Currently, there is no standardized way to categorize quality across vendors. In the area of 10 print fingerprint enrollment roll out, so far 2,500 workstations have been implemented around the country and they have collected 6.6 million 10 print submissions. TECS is a text database containing the no-fly lists.

*Q&A Session*

Q: How does one get their record expunged from a DHS whatchlist?
A: TRIP is a request system that allows DHS to examine records.
Q: What is the order of implementation for NGI?
A: Incremental approach on modalities based on the state of the art technology at that time: 1st is palm print, 2nd face and iris, without exact dates. Dates can be provided later.
Q: General comment: NORTHCOM is prepared to purchase equipment using their own dollars and they run the risk of buying non standard equipment.
A: DoD responded by saying DoD entities need to ask this question in appropriate working groups.
Q: What are large scale government agencies doing to anticipate the 5-8 year picture of the USG biometric capability?
A: DoD should have a much tighter coordination effort with law enforcement. DoS is working towards developing a Center Of Excellent (COE) in September 2009 and implementing iris. DoS will probably not do much with all modalities except leveraging existing technology. FBI will be implementing NGI, supporting intelligence, and working with more partners. DHS wants faster, cheaper, smaller because USG biometrics is moving towards a multimodal environment. DHS wants to tag data to develop a common rule set for sharing data across programs, this will decrease barriers to sharing.
Q: Industry needs to know what big projects to invest in?
A: DOS is looking at iris, to get a biometric center together. There is an RFP for iris. NORTHCOM: Program of Record (POR) is where the military services plan into their budgets, the O&M piece. All COCOMS requirements are recognized. FBI: NGI implementation; need fusion to support intelligence and lead value to see the overall picture. Who is the person at a distance collection. Forums talk to industry to tell them the challenges. DHS: Want faster, cheaper. All going Multimodal. Do quick identification, speed is important. Existing biometrics in background, are they no longer eligible to get access. Tad information in a smarter way. Rule sets make sense with programs. Artificial barriers removed to access information. BTF: Digital requests bounce from database to database. Have enough fidelity, need vision, what do with this person.

## Commercial Industry Panel Discussion

*Key Issues*

- Privacy

A. Ms. Katherine Stokes, Associate General Counsel, Graduate Management Admission Council
Ms. Stokes provided an overview of GMAT, which facilitates the movement of talent around the world. Biometrics provides a technological capability to prevent fraud during the administration of GMAT. Legal challenges with fingerprints exist in the US and the European Union (EU). In the US, no right to privacy codified in US Constitution. There is a patchwork of sector and state laws. In Europe, there is a strong sensitivity to fingerprints. The right of privacy is "fundamental human right" essential to civil society, rule of law, and democracy. The Graduate Management Admission Council (GMAC) is the industry leader in privacy compliance worldwide.

GMAT implements palm vein technology, which enhances GMAT security with 1:N matching on the horizon. This technology is designed to meet EU requirements such as user leaves no trace on device, no surreptitious collection, no image stored, and encrypted. Unique Fujitsu-Pearson VUE algorithms, non reversible and not interoperable with other palm vein systems.

B. Mr. Jason Silbeck, Chief Technology Officer, CLEAR
CLEAR is the largest registered traveler program operating at US airports with over 250,000 members since June 2005. Partnerships are established with airports and airlines, plus major marketing partners. Technical interoperability is achieved with all certified registered traveler service providers. All capital and operating costs are supported by voluntary membership – no cost to taxpayer or airports.

Key Points: Attention to customer service can rapidly speed growth and satisfaction. Interoperability provides flexibility and encourages stakeholders. True security benefits are an important part of the service offering. Registered travel has a history dating back to 2004. Vigilent is a competitor to CLEAR. Currently CLEAR collects 10 prints, 2 iris, 1 photo, and biographic/contextual data. The prints and irises are used for matching but not the face. CLEAR card meets the technical requirements for an identification card in the airport, perhaps the only one you'll need because of these features. Interoperability and open technology standards for fingerprint, iris, facial photo, smart card. CLEAR worked with DHS to develop "RTIC Technical Interoperability Specification" published in 2006, provides guidelines for implementers.

*Q&A Session*
Q: Without getting into the nitty-gritty details, does CLEAR today or in the future plan to use a standardized fingerprint template to exchange data within your architecture? Or is it a proprietary format with the ability to generate the standard, if needed.
A: CLEAR uses standards.
Q: Does CLEAR currently screen biometric samples against IDENT?
A: No, but it could if it needed to do so.
Q: What is the liability of using biometrics for these commercial applications?
A: For CLEAR, they must meet standards put forth by USG and TSA to obtain insurance against terrorism. For GMAT, they comply to several recognized standards.

# 2. Day Two

## Keynote Speakers

*Key Issues*

- Coordination and Cooperation Between Local, State, and Federal Entities

### A. Dr. David Boyd, Director, Command, Control, Interoperability, US Department of Homeland Security

Initiated discussion about the mission of Command Control and Interoperability (CCI). Continued about the communications challenge on the frontlines. Emergency responders, such as police officers, fire personnel, and emergency medical services (EMS), need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large scale emergencies. History dictates which band certain responders use for communications. Certain bands were available during certain times and often times proprietary systems were fielded, which adds to the challenges.

Why does interoperability fail? Locals have almost all the information, about 99%. Local responders know all the details on the ground plus the own the systems collecting information. Federal agencies need locals' data. State and federal direct structures that feed their needs. State and federal usually offer little or no value added or incentive to locals. So, sovereign locals don't play.

In a practitioner-driven approach, a successful strategy for improving interoperability and information sharing must be based on user needs and driven from the bottom up. The Constitution works this way – think of representation vs. federal representation of agencies. This approach ensures that resources are aligned with users. Locals know that they have most of the biometric information. Federal data bases are often searched last because criminals are often located in the state or an adjacent state in which the crime was committed. The key is to incentivize locals to share data with federal systems – we need them more than they need us.

Funding from the federal level for such systems is not as large a contribution as many think. Typically federal funding accounts for a small percentage of the total funding for communications systems. Plus money from the federal government is often slow to arrive. Current interoperability focus is on point to point information exchange boundaries – focus is on the technical interfaces. This focus allows time to be spent on development of standards to create an open framework to facilitate the exchange of information. There are about 60,000 agencies most of which are have a small number of officers and these agencies raise their own funding for equipment.

Current initiatives include interoperability of systems and managing day-to-day information using the National Information Exchange Model (NIEM). Standards are an important aspect of this interoperability process. Project 25 compliance assessment is another program. Data messaging standards support tagging data elements, that will allow users to strip apart data and know how to process it correctly.

Critical Infrastructure Inspection Management System (CIIMS) allows state of Maryland to reroute aircraft after mission is complete during the return flight so as to make the overall flight more efficient. Saves on fuel cost and maintenance fees that can be transferred to other projects.

*Q&A Session*
Q: In the biometrics world, local proprietary AFIS systems exist at the local level. How do we reach down to that data?
A: No interoperability issues are technological, they are human elements. Leadership commitment is the first hurdle. HSPD's direct federal agencies to fall in line, not the locals. Standard operating procedures and common training courses facilitate interoperability and must be developed. Governance is a critical piece – how does the consensus agree that who will be in charge and who will pay. Locals are sovereign and don't typically have to play.
Q: Do you see more partnerships between the private and public sectors working together to solve interoperability challenges?
A: Yes, federals work with locals by paying for the consensus building process (meetings, travel, etc.). Federal level should not dictate standards – we must begin at the bottom and work our way up.

**B. Pete Marone, President, Consortium of Forensic Science Organizations; Director of the Virginia Crime Lab**
From his perspective, interoperability is different depending on the level from which you sit. Locals are typically concerned with interoperability with other locals. Federals are concerned with federal interoperability. Mr. Marone spoke about variations in the production of fingerprint templates between various vendor algorithms. Due to proprietary formats, this poses a challenge to locals. Need to work on better ways to standardize digitization of fingerprint cards.

The DNA data in the NDIS systems resides at the state level. When DNA data is stored in the VA database, it resides in a VA column within NDIS. When VA draws down that DNA data, the total number of VA files decreases. In other words, the federals do not control state databases. Locals and states work better together than the locals, states, and federals do. 95% of hits are local, however, hits in other states are increasing. Local entity can't search the federal database. There is a state coordinator that forwards searches from the state level to the federal level. Once a week, state coordinators forwards files to NDIS/CODIS for searches. This is critical for DoD to consider when developing its integrating DNA into the DoD biometrics architecture.

IAFIS does not work that way. "A camel is a horse made in committee." Need to be conscious of this detrimental. Federal level needs to determine how to deal with local requirements that clash with federal requirements, and state requirements for that matter.

*Q&A Session*
Q: Local, state, and federal data requirements often differ. The challenge to strike the balance between making a system cumbersome and satisfying everyone requirements within a standard. Are there any effective incentives you can share that bring decision makers to the table to discuss these issues? What are some effective ways you've seen to display added value to a system from the consensus driven process besides simply stressing the interoperability language?
A: Locals are goal oriented. Unfunded mandates do not do it.
Q: Going forward, can we resolve interoperability issues by mandating one single ID as opposed to individual state IDs.
A: Deferred to his technical lead.

**Technologies Panel Discussion**

*Key Issues*

- Interagency Interoperability
- Quality of Biometric Sample Data
- Indexing, Tagging, and Tracking Biometric Data

A. Mr. Brad Wing, IT Specialist, National Institute of Standards and Technology (NIST)

Mr. Wing began by discussing the NSTC *Registry of USG Recommended Biometric Standards*, which is referenced in HSPD-24. The "Registry" along with other biometrics standards initiatives are addressed within the Office of Science and Technology Policy (OSTP), NSTC Subcommittee on Biometrics and IdM, Standards and Conformity Assessment Working Group. The NSTC Subcommittee on Biometrics and IdM has working groups on policy, standards, RDT&E, conformance testing programs. The Registry lists recommended biometric standards for USG wide use that are available and adopted within many USG organizations. First and foremost, interoperability success depends on the US broad biometrics community knowing that the Registry exists.

The Registry contains standards for collect, store, exchange, transmission profiles, credentialing profiles, technical interface, conformance testing methodology, and performance testing methodology. There is a difference between conformance and performance testing (may conform but have poor performance). The Registry evolves over time. Standards are evaluated and updated to the Registry.

Biometric standards for voice and DNA are under development and will be added to the Registry. Biometric standards for fingerprint, face and other biometrics have already been added. These standards allow for the transmission of biometric information among law enforcement agencies in extensible markup language (XML) format, which is an alternative to binary. The NIST Information Technology Laboratory (ITL) has completed an XML version of the ANSI/NIST ITL 2-2008 standard, titled Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2: XML Version. This standard will be expanded to handle additional modalities and is used to transmit information to INTERPOL.

Mr. Wing stressed the importance of testing. Conformance testing output is a function of format data process. Performance testing includes error rates, throughput, and responsiveness under various conditions. Who does the Testing? First Party is the manufacturer, Second Party is the user or purchaser, and Third Party is the independent group (Underwriter's Lab). A Robust Standards and Conformance Assessment infrastructure includes Product developers, Second Party, Lab Accreditation, and Third Party validates Certification Bodies. Tools and Standards for Conformance Tests are another critical element for a robust testing infrastructure. In 2005 BioAPI Standard became an ISO standard. In 2006, NIST's Image Group's Minutiae Interoperability Exchange Tests (MINEX). In 2008, Common Biometric Exchange File Format (CBEFF) – wrapper around biometric data by NIST.

Tests underway include:

- NIST Iris Exchange (IREX08): Objectives: support development and interoperability of iris images, establish iris images as the primary exchange format. Examine storage format for iris data and push developers into implementing ISO standard implementations. Establish compact image formats. Evaluate state of the art iris recognition performance. See: http:iris.nist.gov/irex
- Multi Biometrics Test and Evaluation (MBTE): Look at potential for iris or face use in maritime scenarios. Compression of photographs used in ePassports at DHS. Do conformance to capture standards and quality assessments and human factors. Evaluate the potential for iris and/or facial biometrics for use in pedestrian/maritime scenarios.
- Multi-Biometrics Evaluation (MBE) 2009: Follow-up to the Multiple-Biometrics Grand Challenge 2008. Tests to be performed by NIST using code provided by developers. Run against larger,

sequestered data sets. Summer 2009 Staggered start of three tracks: Portal and Video, Executable, Based on FRVT 2006, ICE 2006, and MBGC, Still face track, Operational data, and Submission of SDKs will be an option.

- Multiple Biometric Grand Challenges (MBGC): The MBGC Evaluation Team has designed three challenge problems: Still Face Challenge, Portal Video Challenge and Video Face Challenge. Laboratory (NavLab) certified to perform test on biometric equipment. Lab should be operational this year. Exciting development. First application is airport access control.
- Qualified Products List (QPL) of Biometrics Products: FBI's Certified Products List (CPL) for Fingerprint scanners/card readers, TSA QPL for Biometric Airport Control Systems, Approved Product List for FIPS (201) PIV. FIPS 201 (Federal Information Processing Standards Publication 201) is a USG standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

Moving forward, a groundbreaking USG-wide standards selection process is now in place to align USG-wide standards. This is a great step forward. Agencies go through standards and can incorporate into their acquisitions processes. Can audit for compliance. Augmenting the existing USG Conformity Assessment capabilities in support of the recommended standards is now underway. Registry will be updated as new standards emerge or older ones become obsolete.

B. Mr. Ken Martin, Past President, International Association for Identification

HSPD-24 discussion focused on various references to interoperability. Funding is only mentioned once in the HSPD. Mr. Martin discussed HSPD-24 from a state and local perspective, where there is a divergence of law enforcement and DoD missions. Law enforcement needs to achieve criminal prosecution and meet the challenge of court unlike DOD which is intelligence focused. In state and local domains, there are 18,000 state and local law enforcement entities with approximately 800,000 law enforcement officers. Police, chiefs, sheriffs will not give up their domain.

The implementation of HSPD-24 poses several challenges. On compatibility, HSPD-24 calls for compatible methods and procedures but what is the incentive to do this? The directive does not impose requirements to state and local law enforcement and it does not provide new authorities to any agencies. Federal agency databases contain only what they receive. Funding is only mentioned once in the HSPD. Fingerprints are the biometrics base upon which to build but this is not a solid base. There are pre-existing problems. AFIS has its own database structure and algorithms. Interoperability does not work at the state level because information is over classified. If information crosses state borders, no more control, therefore many entities are reluctant to pass data on. There are legal mandates as well including groups, watchdogs, mandates from USG and lobby not to change state law. Funding sent to state and local increases competition on who gets what amount of money. Often, work is not carried out due to lack of manpower to maintain the database.

Local law enforcement issues with collections include when a person is arrested, what goes into a database, and the need for rapid info on person. Fingerprints ink vs. electronic is also a challenge. Locals use cards that don't make it into the databases. DNA categories of crime, time of arrest vs. conviction vs. conditions of release all require database updates. State AFIS are not interoperable nor compatible. In 1995, predictions were made that all AFIS were interoperable. In 2008, this remains the case and change is slow moving. AFIS not a standard database, it is decentralized, and 30 years old. A directory of users is unavailable. The good news is that CODIS is interoperable. Laws are different in each state. For example, wire tap laws differ in many states and conflict at the federal level.

Federal IAFIS has 56M records. NGI will include palm and scars, marks and tattoos. Interoperability is over 10 years. Vendor's best algorithms, search hit rates, law enforcement is reluctant to give up. Accuracy needs to be maintained and one way to do this is to resolve image quality issues.

Resource Issues include workload management where units run 24/7 and hardware/personnel costs are high but resources are thin. To be successful, states need resources for personnel and hardware, MOUs for standardization, and increased connectivity and networking.

C. Dr. Stephen Elliot, Associate Professor of Industrial Technology, Purdue University
How can academia get involved in HSPD-24? Academia can play an active role in a variety to was including: participation on standards, testing and evaluation of products, working with certification bodies, training (external and within the curriculum), testing effectiveness of standards, and play an advisory role for those that need to implement standards. When creating curriculums that involve standards, some curriculums must be replaced, it cannot simply be added. Dr. Elliot focused on many issues surrounding fingeprints, their sensors, and their scanners.

D. Dr. Marios Savvides, Director of Biometrics, CyLab
Dr. Savvides will reiterate much of what Dr. Elliot described with regards to the contributions academia can make in the realm of biometrics and the implementation of HSPD-24. Main focus is face and iris. How can we enhance collected images?

This discussion kicked off with results of tests conducted on facial images to compare the verification rates of images (performance) to tweak algorithm performance. (FRGC is the testing effort). How do we move to consider different face poses and poor quality images that are not megapixel imges? How does one leverage existing infrastructure to deploy effective biometric collection and matching equipment while preserving matching performance? Carnegie Mellon database of facial images provides images of off-pose angles, various facial expressions, and different levels of lighting. Analyzing these variations in facial images allows academia to baseline problems in matching performance. Facial expression analysis. Pose correction using symmetry…

3D morphable models (2D → 3D) From 2D images, 3D images are generated that can be used for matching. Awesome technology for many applications! Iris Sarnoff iris on the move portal. Beyond 20 feet, illumination issues arise during collection. Academia is developing and tweaking algorithms for face and iris that can directly contribute to the performance of matching algorithms.

E. Dr. Arun Ross, Associate Professor, Lane Department of Computer Science and Electrical Engineering, West Virginia University
There are a few words that stick out in HSPD-24 with regards to research: storage and sharing. Within academia, discussion focuses on flow of data from sub-systems (functions) within the biometric process. For example, data flowing from collection sensor to matcher to storage and so on. Biometric databases are becoming increasingly populated by multimodal data of an individual. Indexing techniques are needed to restrict the search to a subset of the database for a quick search.

Multibiometric indexing: the fingerprint modality can narrow the number of possible matches and direct the query image to a particular "bin" of identities. In summary, database organization, template security, and sensor interoperability.

*Q&A Session*
Q: When will the results of the MBGC be published? Also, I hear calls for interoperability, which is not something addressed until much later in a products lifecycle. How does vendor community engage in implementation of standards earlier in the product lifecycle?
A: It will be quite a while, fairly soon. Agree with second question. Vendors are need to be involved in the standards. Early in the process, companies don't want standards b/c they want to maintain a competitive edge. However, in the long run it is in vendor's best interest to implement standards. Standards are difficult o link to the bottom line of a company. Mr. Brad Wing provided a real world anecdote about the importance of building consensus on passport chips with big manufacturers.

Combination of laboratory and operational testing was crucial in getting the systems conformant to standards.

**International Panel Discussion**

*Key Issues*

- Privacy

A. Mexico, Mr. Carlos Raul Anaya Moreno, Director General, National Register of Population and Personal Identification

The Identity Service Mission can best be explained with a comparison to a three legged stool. The three legs are legal identity, living identity, and biometric identity. Legal identity: If there is no legal identity, the chair becomes weak and won't deliver security and trust. Examples of this are voting, or police control. Living identity: Vulnerability of personal data confidentiality, which happens when sold by the private sector without the intervention or audit of public sector. Biometric identity: Lacks physical identity, allows for identity fraud, multiple identities and changeable identities. When one of the legs of the identity service stool is missing or one focus is stronger than other legs – identity service is unbalanced and problematic. Mexican systems use the standards ANSI/NIST ITL 1-2007 Part 2: 2 iris, 2 face, and 10 fingerprint records.

Objectives of the Identity Service Mission: Include guarantees to the right to identity, certify Mexican citizenship (Mexican Constitution, 36 Article), comply with the Universal Declaration of Human Rights (Article 6), strengthen the person's management capacity, simplify and reduce procedures, support full access to the new information society, grant certainty to the economic and social sectors through a document that reliably certified identity; help to generate trust in commercial and financial activities.

Deployment of 100 million ICAO compliant national identity cards over the next 5 years. People are not transactions. We have to break the "transactional paradox" of database processing and retake the concept of Public Service, respecting the dignity of the people and there right to privacy. There is a Mexican website open to the public for all Mexican identities, which includes passports and other personal data elements (name, date of birth, sex). Public website exists for fingerprints as well.

B. INTERPOL, Mr. Joseph Orrigo, Senior CI Advisor, Terrorism and Violent Crime Division

Mr. Orrigo provided an overview of Interpol, which serves as an investigative tool in biometric data sharing. Interpol's mission is to promote and coordinate international police activity. It was created in 1923, it is in 187 countries. The heart of Interpol is its tools: notice program and its data bases, which include the Interpol Criminal Information system (ICIS) and automated search facility (ASF). ICIS is the criminal history of individuals. ASF is the search engine for a number of other databases on various crimes and biometric modalities: DNA profiles, stolen motor vehicles, stolen works of art, child pornography, among others.

US National Central Bureau (USNCB) is located in DC. Project Face Off included a search between Interpol's fingerprint database and the ABIS. 30 individuals were matched. One of which was involved in the 2003 Casablanca bombings. Project Ocean View – involved a matching effort of only names first between Interpol records and databases at DMDC. 10 were identified. Current effort is to match one fingerprint using images stored for CACs. Interpol prints are now converted for matching in IAFIS. New Concept Project is to support DoD and FBI CT overseas efforts: obtain, fingerprints, two way conversion, conduct searches in Lyon, and provide feedback. Approximately 10 minute matches from DoD to Interpol.

Way ahead: IPSG Lyon, expand and upgrade, NIST viewer license, NIST Software, Purchase of V700 Scanners, Increase Storage, virtual data base global system of links, deployment of IRT Team major

events 39. Other New Approaches…Project Oasis in Africa and Mexico focused on building African fingerprint matching capability. Palm prints capability for storage in early 2009. Forensic area, Interpol is working with various countries/disciplines (Canada-explosives, Romania-fingerprint dating, Colombia-artificial prints). Domestic initiatives include Interpol Portal in 2009 and closer coordination with IAFIS-FBI.

*Q&A Session*
Q: How difficult has it been to obtain the concurrence of all federal agencies to adopt Mexican model? How did you get concurrence between federal, state, and local? Who is bearing the cost of Mexican implementation?
A: Federal program is providing system. No need for state local to implement. 70% of funding is federal, 30% is state/local.
Q: How did Mexico deal with privacy and civil rights groups on identity?
A: All American countries agree with fact that identity is a human right and not an individual/personal right. US needs to put push a more communal perspective. US is the only country in the Americas that doesn't agree with Mexican position on identity.
Q: Identity theft a problem in Mexico?
A: No. Benefits outweigh challenges.
Q: How does Mexico establish the trust of citizens? How costly is the system? Does the Mexican fingerprint system track encounter information?
A: Article 36 of the Constitution requires citizens to provide identity information to the government.
Q: Intrigued about 187 countries involved in Interpol. US doesn't have extradition treaties with each country. How are these things worked?
A: Some of these countries are our enemies. With terrorism, some countries are apt to sharing data. Countries work with Interpol to figure out a way to route an individual to a country that does have an extradition law with the US.
Q: How does Interpol convert fingerprints from one format to another?
A: The process is automated.

**Interoperability Panel Discussion**

*Key Issues*
- Interagency Standards for Sharing Data
- Adherence to Standards
- Coordinated Congressional Oversight and Funding

A. Mr. Dirk Rankin, NCTC, Office of Mission Systems Architecture, Engineering & Investment
The National Counter Terrorism Center (NCTC) was stood up in 2004 as a part of the US Intelligence and Reform Act. Cooperative users: rapid and quality collection of unique biometric data. Need standardized collection methodologies. Need to facilitate efficient updating of changes to biometric features (cosmetic surgery, etc.). Biometric data will drive storage solutions geometrically versus biographic-only based designs. Binary data is exponentially larger than ASCII data. Solid certification and accreditation criteria and process is crucial.

Non-cooperative/Uncooperative Users involves issues related to rapid and quality collection at a distance and a growing need for ruggedized sensors worldwide. NCTC phased implementation approach to biometric enabled intelligence (BEI) for counterterrorism. Sharing data is a challenge. Need data standardization, this requires recognition and ownership of problem then adoption of standards. NSTC policy for Enabling the Development, Adoption and Use of Biometric Standards was a step in the right direction. Intelligence Community (IC) Information Sharing Data Standards Coordination Activity is underway through the use of TWPDES, NIEM, & UCORE.

Policy considerations include a way ahead for data exploitation: which model? Bring data to the processor (replication model – high cost) or bring processor to the data (services model – high integrity).

Technology considerations include a way ahead for databases: Relational (Oracle, "pair-at-a-time") or Hierarchal (XML, "many-at-once"). Web 2.0 technologies and cloud computing (shared processing, storage, etc.) should be considered along with service oriented architecture (SOA) constructs. Modernized, fast moving code base – open source, commercial, government should be the goal of USG.

Community considerations must include access and dissemination across security domains. User authentication (LDAP, etc.) must converge on methodologies, standards, formats, security, schedule, cost, performance, risk maintenance, and refresh. Implementation synchronization is hard to do. Unified CONOP required to minimize number of variables, and lower cost. How to integrate Vertical/Horizontal paradigms. Vertical is top-down, policy and budget. Horizontal is peer-level stakeholder implementation.

B. Mr. Paul Grant, Office of CIO, US Department of Defense

Mr. Grant initiated his brief by discussing biometrics within the context of IdM, which includes the tracking of red, blue, and gray forces. IdM also includes tracking all things (objects/people) moving within the Global Information Grid (GIG). Value proposition is the context, strong Identity and Access Management (IdAM) are key to sharing in cyber space and physical access to sensitive locations.

Major move forward in this field was signing policy approving external PKI list. DoD CIO and Northrop Grumman CEO used their respective cards to exchange certificates and exchange sensitive information. This allows external contractors to exchange signed and encrypted emails with DoD. Synchronized Pre-deployment and Operational Tracker (SPOT) is used to track contractors who end up in an Area of Responsibility (AOR). Partners can expect strong credentialing of our employees and robust access to PKI certificates. EADS has the lead to deploy the same in UK Ministry of Defense (MoD), which will allow cross exchange between US and UK. Most of our coalition partners do not have credentials like DoD.

In summary, strong IdAM are key to information sharing and collaboration. We need a clear, consistent, published course for ourselves and our mission partners.

C. Mr. Paul Garrett, Special Assistant To The Chief Information Officer, Department of Justice

Mr. Garrett led off with "Aren't biometrics Really just data?" Mr. Garrett strives to be a mouthpiece for activity in the interagency sharing initiatives. Issues related to sharing need to be elevated within various agencies. Sharing becomes more of a policy and funding problem and less of a technology issue.

Impediments: Congressional funding and oversight is currently stove-piped. How do we as a community push more Congressional oversight? How do you get the attention of the policy makers? Agencies leave critical work on sharing to the techies. No one likes standards to be mandated in a program. Competition is a good thing in markets but not necessarily in government.

The importance of NGI should not be understated. This program has the potential to serve many USG needs. CJIS has a history of service and it possesses the ability to support USG biometrics activities in the long term. Universities (WV & Pitt) and the private sector will need to play a bigger role along with the expanding role of DoD.

USG enterprise must be a federated system with a minimal amount of matching databases. How many matching algorithms does the USG really need? Most of the technical issues have largely been figured out.

Challenges with US-VISIT: Segmentation issue – criminal in IAFIS but criminal and civil information in IDENT. MOUs with others are impacting FBI and FBI customers without realizing the potential damage. Not following Guideline 4. Without exit pushing more work on FBI systems. Keeping data up to date, especially expunged records (2 systems vs. 1 system) audits are slow and expensive.

Concluding Thoughts: Can't separate biometrics from other sharing efforts, can't fund biometrics separately, standards are good and needed. It's a complex issue that requires policy makers to pay attention as it touches: access, privacy, and safety of the homeland.

D. Mr. Thomas Lockwood, Senior Advisor, Screening Credential Office, US Department of Homeland Security

*Q&A Session*
Q. What is the architecture for sharing attributes within a FIPS 201 framework. Need to rely on trust, need to use standards.
A. How do we change digitized decisions and exchange that with partners? How does that identity and supporting information move beyond the federal architecture? Biometrics can be added into this process to help out.
Q: Didn't hear much about integrating biometrics into the PKI, logical, and physical access spaces?
A: Credentialing and use FIPS201, use of biometrics on the card. Biometrics is bound to the identity.

# 3. Consolidated List of Key Issues

NDIA tracks the progress of key issues facing the biometrics and identity management arena. These issues will be tracked periodically throughout the year. At the next Biometrics Conference, NDIA will report on the status of each issue.

| # | Key Issue Description |
|---|---|
| 1 | Consolidation of Congressional Oversight and Budgets |
| 2 | Interoperability: Procurement and Implementation of Biometrics Equipment that Adheres to Biometric Standards |
| 3 | Coherent Policy Across the USG Governing the Use of Biometrics |
| 4 | Unified USG Conformity Assessment Program for Testing Conformance to Biometric Standards |
| 5 | Privacy: Ability to Protect and Expunge Data |