Special Report: Biometrics in Law Enforcement

BIOMETRIC UPDATE.COM

Rawlson O'Neil King, Lead Researcher, Biometrics Research Group, Inc.

About the Biometrics Research Group

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which in particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.

Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

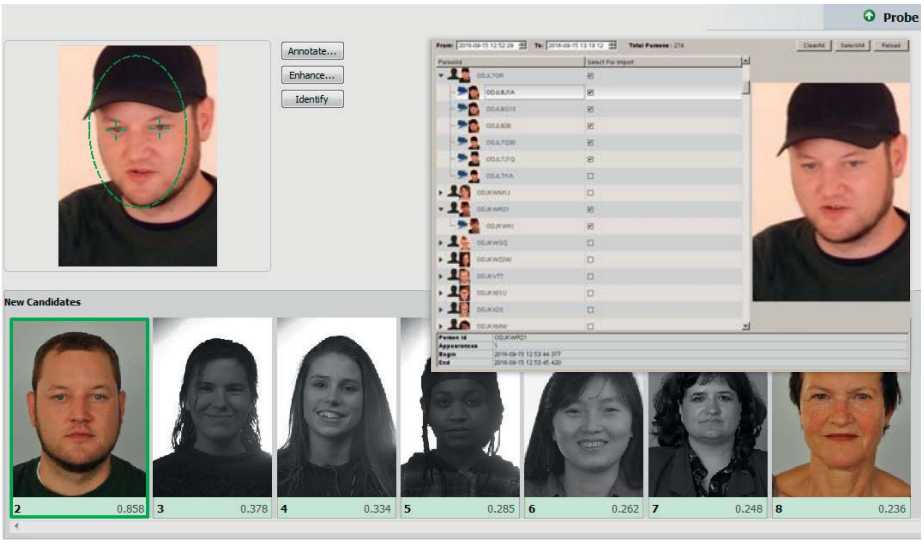
Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

Premier face recognition technology

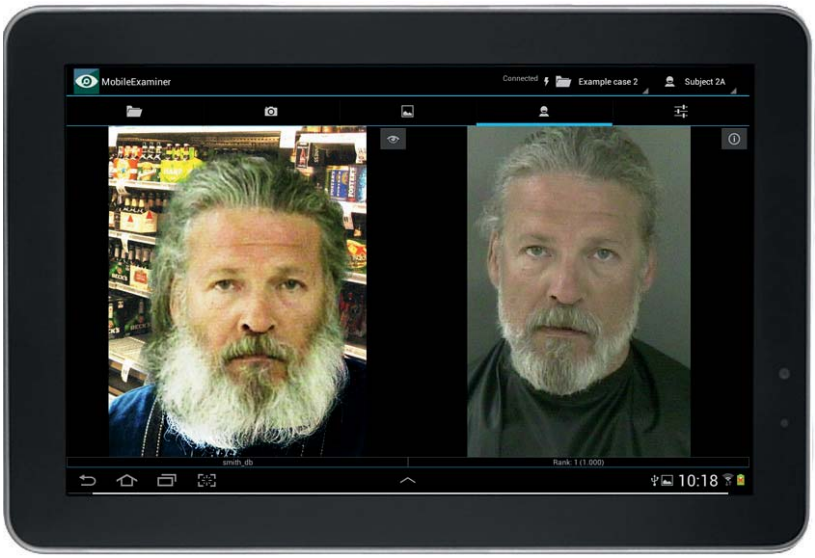
for fast and accurate criminal investigation

FaceVACS-DBScan with Examiner instantly matches crime scene photos, composites and surveillance video images against your mug shot repository to support efficient suspect identification.

The software enables fast import of video footage and selects the optimal image for database search.



for image capture and search at the scene



FaceVACS-DBScan for Android devices allows agents to take suspect photos in the field, send authorized comparison requests to a centralized database and instantly receive a candidate list.

The technology runs as a stand-alone application or can easily integrate and interact with existing law enforcement IT environments.

Cognitec develops premier face recognition technologies and applications for facial image database search, video screening and analytics, border control, ICAO compliant photo capturing and facial image quality assessment.

Biometrics & Policing

Law enforcement biometrics refers to applications of biometric systems which aids policing. Biometrics Research Group Inc. projects that the total global biometrics market will grow to US$35.5 billion by 2020 from its 2015 value of US$15 billion. We approximate that more than half of this 2020 spending, equaling US$18 billion, will be spent on law enforcement biometrics worldwide.

The law enforcement market includes the use of biometrics to identify or verify the identity of individuals who have been: apprehended or incarcerated because of criminal activity, suspected of criminal activity, or whose movement is restricted as a result of criminal activity. Biometrics may be used to identify non-cooperative or unknown subjects, to ensure that the correct inmates are released, or to verify that users under home arrest are in compliance.

Biometrics Research Group, Inc. defines biometrics as measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity. Biometrics is the process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity.

In terms of biometric technologies, automated fingerprint identification and fingerprint biometric technologies will account for the greatest share of the biometrics spending in the U.S. law enforcement sector, followed by iris, facial, and voice recognition biometric technologies.

Biometrics Research Group, Inc. estimated that in fiscal year 2012, automated fingerprint identification systems accounted for US$3 billion in global law enforcement spending, while combined spending on face, iris, facial, and voice recognition accounted for approximately US$1 billion. For 2015, Biometrics Research Group estimated that spending on global fingerprint systems totalled US$5 billion, while spending on the other combined biometric modalities equalled US$2.5 billion. Biometrics Research Group projected that total global spending on biometrics for law enforcement totalled US$7.5 billion in 2015.

In 2020, we believe that at least US$15 billion in global spending on law enforcement biometrics will be allocated to automated fingerprint identification systems while the remaining US$3 billion spent in the sector will be allocated to secondary modalities including face, iris, vein, and voice recognition biometric technologies.

The wide-ranging "law enforcement biometrics category" includes automated fingerprint identification and recognition, mobile biometrics identification devices, criminal ID solutions, as well as access control systems. Biometrics Research Group, Inc. estimates that global spending on automated fingerprint identification by 2020 will total US$13 billion, while other fingerprint recognition systems, including access control systems will total US$2 billion. Spending on mobile biometrics identification devices and criminal ID solutions will equal US$2.5 billion and we expect spending on experimental and emerging technologies, including DNA, will total $0.5 billion.

Biometrics Research Group notes that investments in law enforcement biometrics will accelerate throughout North America and Europe, especially in the United States. Recent evidence of this investment trend in the U.S. abound. At its 2017 annual meeting, the Southwestern Border Sheriffs' Coalition (SBSC) voted to partner with BI2 Technologies to expand its biometric identification program and system. BI2 Technologies has committed to work with SBSC to improve and expand biometric identification capabilities at 31 Sheriffs' Offices along the U.S. and Mexico border to ultimately increase border security and combat criminal activity.

SBSC — which is an IRS certified 501 charitable organization whose mission is to insure the

safety and security of the country's Southwestern border by assisting elected Sheriffs — has provided initial funding to immediately expand the capabilities while seeking additional federal funds. BI2 is providing the system free to the Cameron County and El Paso County sheriff's departments for three years. In addition, SBSC is seeking federal funds to cover the complete rollout, with each device costing US$2,500 each year.

SBSC members voted unanimously for BI2 to provide all 31 U.S. sheriff's departments along the U.S.-Mexico border with technology that combines iris-scanning with fingerprint- and facial-recognition capabilities.

"The SBSC will implement our advanced iris biometric identification technologies at Sheriff's Offices, as well as in-the-field mobile, smartphone-based, multi-modal (iris, fingerprint and facial biometric identification) devices," Mullin said. "These technologies will provide each Sheriff with immediate access to national, state and local criminal justice and law enforcement databases. This will enable Sheriff's staff to positively identify previously enrolled individuals in seconds, regardless of the often fraudulent identity presented."

Cameron County Sheriff Omar Lucio noted that the system, which is compatible with the records-management systems used by most sheriff's departments, would be installed and operational in the first two counties by April. He added that the system will be used in the intake/booking process, along with potential plans to use it in the field with handheld scanning devices. The biometric identification system will provide the department with immediate access to national, state and local law enforcement and criminal justice databases.

"I don't think we can go wrong with that technology. It's just an additional tool to keep our communities safe," said Lawrence "Larry" Guerra, executive director of the SBSC. "The 31 Sheriffs who comprise the SBSC are literally the frontline of defense against criminal activity along the southwest U.S. border with Mexico."

Expansion of law enforcement biometrics can be expected to be driven by a political agenda that will drive future federal appropriations to invest in technology for securing the border, as well as allocating funds to hire additional police staff and increase detention capacity. With more law enforcement capacity predicted for the southern border, we can project that more policing biometrics will be required for criminal identification. Much of this capacity will be driven by the integration of automated fingerprint identification and cloud-based systems.

Biometrics Research Group estimates that cloud-based solutions across all modalities will constitute at a minimum 50 percent of biometric offerings marketed to law enforcement agencies in the United States by 2020. In terms of revenue breakdown, we estimate that cloud-based solutions will total US$12.5 billion by 2020. We believe that the majority of cloud-based systems will incorporate automated fingerprint identification and will rely on mobile biometrics identification devices.

Fingerprint Recognition

Biometrics Research Group defines automated fingerprint identification as the process of automatically matching one or many unknown fingerprints against a database of known and unknown prints. Automated fingerprint identification systems are primarily used by law enforcement agencies for criminal identification initiatives, the most important of which include identifying a person suspected of committing a crime or linking a suspect to other unsolved crimes.

An automated fingerprint identification system (AFIS) is typically described as a biometric identification methodology that uses digital im-

aging technology to obtain, store, and analyze fingerprint data. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity, but historically has been the most used. AFIS is primarily used for criminal cases and have been deployed by national, regional and local law enforcement agencies, alongside national border patrol services.

With greater frequency in recent years however, automated fingerprint identification systems have also been used for large-scale civil identification projects. AFIS are being used for a variety of civil purposes, including criminal identification, applicant background checks, receipt of benefits, and receipt of credentials, including passports. A chief purpose for civil fingerprint identifications system is to prevent multiple enrollments in an electoral, welfare, driver licensing, or similar system. Another benefit of a civil fingerprint identification system is its use in background checks for job applicants for highly sensitive posts and educational personnel who have close contact with children.

Due to these types of applications, the AFIS market is mature by biometric standards, having already reached a substantial percentage of its potential deployment purposes. Many countries including Canada, the United Kingdom, India, Israel, Pakistan, Sri Lanka, Argentina, Turkey, Morocco, Italy, Chile, Peru, Venezuela, Australia and Denmark have deployed AFIS. Intra-national organizations including the European Union and the International Criminal Police Organization have also deployed these systems.

The country with the largest deployment of the AFIS technology is the United States. The Integrated Automated Fingerprint Identification System (IAFIS) in the U.S. holds all fingerprint sets collected for criminal justice purposes and is managed by the FBI. Launched in 1999, the FBI's database is used by federal and local law enforcement agencies to solve and prevent crime and catch criminals and terrorists. IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses.

IAFIS is the largest criminal justice biometric database in the world, housing the fingerprints and criminal histories for more than 70 million subjects in its criminal master file, along with more than 34 million civil prints. Included in its criminal database are fingerprints from 73,000 known and suspected terrorists processed by the U.S. or by international law enforcement agencies. Many states also have their own AFIS. AFISes have capabilities such as latent searching, electronic image storage, and electronic exchange of fingerprints and responses.

In 2012, the U.S. Federal Bureau of Investigation announced its decision to widen its Integrated Automated Fingerprint Identification System (IAFIS) to become multi-modal. As part of its Next Generation update to the national fingerprint database in the United States, the Federal Bureau of Investigation has begun rolling out facial recognition to identify criminals. Facial recognition is a computer-based application system for automatically identifying or verifying a person from a digital image or a video frame from a video source by comparing selected facial features against a facial database.

The implementation of new biometric identifiers in the FBI's Integrated Automated Fingerprint Identification System is part of the FBI's new "Next Generation Identification" program effort. The program is designed to advance the bureau's biometric identification services, providing an incremental replacement of its current integrated automated fingerprint identification capabilities with a multimodal biometric database.

According to the FBI, the future of identification systems is currently progressing beyond the dependency on a uni-modal, fingerprint biometric identifier towards other multi-modal biometrics, including voice, iris and facial recognition.

Voice recognition systems, broadly as known as 'voice biometrics', is a biometric modality that

uses an individual's voice for recognition purposes. It is a different technology than "speech recognition", which recognizes words as they are articulated, which is not a biometric. The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual.

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle.

The Next Generation Identification program is designed to advance the integration strategies and indexing of additional biometric data that will provide the framework for a future multi-modal system that will facilitate biometric fusion identification techniques.

The framework is expandable, scalable, and flexible to accommodate new technologies and biometric standards, and will be interoperable with existing systems. Once fully deployed, the new FBI biometric initiatives and multi-modal functionality will promote a high level of information sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification.

The existing database currently consists of iris scans and DNA samples, but the newly updated database will also contain tattoos. Another proposed element of an updated database includes an image matching service. Under such a service, images of a person of interest from security cameras or photos accessed from sources such as the Internet could be compared against a national repository of images held by the FBI.

The FBI will also expand its capability to accept, store, and search palm print submissions from local, state, and federal law enforcement and criminal justice agencies. The bureau's new system will provide a centralized repository for palm print data that can be accessed nationwide, providing local police with an additional tool to solve crimes.

The objective of the program is to reduce terrorist and criminal activities by improving and expanding biometric identification and criminal history information services through research, evaluation, and implementation of advanced technology that would be made widely available to local law enforcement agencies.

In addition to being used by the FBI and local police forces, the NGI now is used regularly by the U.S. Department of Homeland Security as the agency sends prints to NGI from all border crossings and port-of-entry checkpoints. Additionally, the Defense Department and the Office of Personnel Management regularly depend on the FBI to process fingerprints against NGI.

Due to these developments in the AFIS market, new portable devices tied to central databases for field suspect identification through mobile identification technology has become increasingly important. Mobile identification technology devices provide an essential front-line security measure for both government agencies and commercial users. Based around a central biometric identification system (BIS), mobile biometric identification devices extend the functionality and capabilities of a static BIS by allowing users to capture fingerprints and facial images out in the field, and compare fingerprint minutiae templates or images against a biometric database, either stored locally on the device, or remotely in centralized biometric matching systems.

Mobile identification technology solutions typically consist of products and services that allow law enforcement agencies to conduct mobile criminal record checks. Using name-based and biographical information, along with biometric database matching tools, these solutions allow police services to search national police databases as well as their own local records when conducting criminal record checks for private employees or in the field during criminal inves-

tigations. Over the last several years, numerous new mobile devices and applications have been introduced to the marketplace.

3M, as an example, offersla w enforcement clients its BlueCheck 2U product, which is a Bluetooth-enabled mobile identification handheld device that is designed for single-handed operation. BlueCheck 2U's lightweight and compact design features an FBI-certified 500 ppi capacitive sensor. Designed for single-handed operation, BlueCheck 2U securely transfers captured fingerprints to a host, such as a PDA, laptop, or smartphone, via Bluetooth. Using the 3M MobileID application or the 3M WebID secure Web portal, the host device can submit ANSI-NIST format files via SMTP or SOAP (Web service) to a remote server or to an Automated Fingerprint Identification System (AFIS) for fingerprint identification. BlueCheck 2U is FBI Mobile ID FAP Level 10 compliant according to NIST Mobile ID Best Practices Guidelines.

In another example. QiSQi Identification Technologies has also developed a mobile automated biometric identification system platform and app that can register and identify fingerprints, faces, and iris within less than a second. The app operates on a standard Android mobile phone, enabling users to seamlessly and quickly deploy its capabilities without investing in any additional hardware. Equipped with mobile and touchless biometrics software from Diamond Fortress, the app obtains high-quality fingerprints via the mobile phone's camera. The face recognition has 2D/3D enhancement features, which enables the system to deliver highly accurate information. With the iris recognition capability, the mobile automated biometric identification system platform is the first mobile phone to feature all three major biometric identification algorithms.

Criminal ID

Criminal ID solutions are crime analysis tools that enhance and integrate AFIS technology and mobile devices to create an all-encompassing ecosystem of tools that can be utilized for crime resolution. Such tools are classified as "integrated systems" that can unify centralized crime data databases with data mining algorithms to assist with analysis of crime information to aid with crime pattern detection and solving open investigations. Such tools are increasingly advanced by a myriad of firms.

Cognitec Systems

Cognitec Systems was founded in 2002 by a team of experts who recognized the growing need for software and hardware solutions in the field of biometrics. The firm has worked on algorithms for the FaceVACS face recognition technology since 1995. FaceVACS-DBScan, designed specifically for law enforcement, can instantly compare facial images from various sources to large image databases, supporting the biometric identification, comparison, and verification of persons. Law enforcement professionals can identify individuals in crime scene photos, videos stills and sketches by matching facial images against the agency's mugshot repository. ID issuance agencies can compare ID portraits to large image databases to prevent ID fraud or detect clerical errors. The firm's Examiner toolset can enhance images for better comparison to the gallery. For example, image processing filters can improve the quality of images retrieved from low quality

video footage. The pose correction filter uses 3D modeling technology to generate frontal views of faces taken under lateral angles. Examiner also provides a set of inspection tools that help identify the person by comparing images side by side or by measuring facial features. Operators can develop watch lists of potential matches while recording a full audit trail for each step in the process. Finding a suspect in a timely manner allows investigators to act upon the search results in the critical time period after a crime has been committed. Cognitec also offers police, intelligence, and military forces the capacity to identify suspects in the field using mobile devices. Cognitec's face recognition technology can be used on handheld devices to capture a suspect photo and compare it to central image databases through mobile networks.

Crossmatch

CROSSMATCH®

The world identifies with us.℠

Crossmatch® is an innovative provider of secure authentication and biometric identity management solutions. Trusted by hundreds of millions of users and leading integrators worldwide, Crossmatch has been solving unique identity management and cybersecurity challenges since 1996. Crossmatch biometric identity management solutions incorporate a wide range of trusted biometric hardware and software delivering the highest quality and performance required for critical identity applications. The modular ArcID software platform provides a backbone for identity management with Pre-enrollment, Enrollment, Store and Forward and Identity Management modules. Coupled with Crossmatch's biometric acquisition hardware—including the benchmark Guardian® tenprint, L Scan® palm print and highly-mobile Nomad™ thin film transistor module and reader line—there is a configuration to meet individual use case and budgetary requirements. Identity solutions include border and immigration screening, visa and national ID issuance, criminal booking and mobile identification, and applicant background screening—just to name a few.

Allevate Limited

Allevate

Allevate works with law-enforcement, intelligence and government agencies to enhance public safety by ensuring positive identification through the application of biometrics. With its partners, it enables virtualised cloud platforms (private, public, hybrid) to forensically analyse vast video and photographic repositories with the application of face recognition. The same platform can be used to index and submit for searching faces detected in live video streams in real-time.

JENETRIC Gmbh

JENETRIC GmbH produces the world's smallest ID flat scanner. Utilizing the firm's new capturing technology, the scanner combines unmatched user friendliness with high quality fingerprint images. Its integrated touch screen provides easy to understand instructions that reduce failure to enroll rates and shorten the capture process. The firm also provides a software development kit that provides a streamlined interface for comfortable and fast integration of JENETRIC's biometric scanners into enrollment applications. Its API enables full access both to the scanner and a broad range of sophisticated features making the capture process as easy as possible. JENETRIC recently announced the establishment of a wholly-owned U.S. subsidiary, entitled JENETRIC Inc. The subsidiary will assume control over American sales operations.

Integrated Biometrics, LLC

Integrated Biometrics, LLC designs and manufactures FBI-certified fingerprint sensors for identity solutions serving government agencies and commercial markets worldwide. The firm's products utilize patented light emitting sensor (LES) film to deliver best-in-class performance in speed, size, weight, ease of use, and durability for affordable high performance mobile solutions.The technology outperforms traditional prism-based devices in size, power consumption, and usability. These innovative sensors enable organizations to enroll and verify individuals within large populations for use in national ID programs, elections, social services, homeland security, law enforcement, military operations and countless commercial applications. Integrated Biometrics offers the only Appendix F FBI-certified sensors that meet the mobility requirements demanded by end users.

OT-Morpho

OT-Morpho offers multi-biometric identification services for friction ridge, face, and iris recognition in the cloud. The firm's offering, MorphoCloud, is a secure and flexible "AFIS as a Service" solution for OT-Morpho's flagship Biometric Identification Solution (MorphoBIS). MorphoCloud is hosted on Microsoft Azure Government, the cloud platform designed to meet the U.S. government's requirements for data security and continuity of operations. Backed by the Microsoft Azure Government platform, MorphoCloud complies with the stringent security standards for storage, transmission, monitoring, and recovery of digital information, including standards issued by the FBI's Criminal Justice Information Services (CJIS). In addition, the firm's multi-biometric solution offers tattoo recognition, and voice recognition, as well as cloud-supported services, such as video analytics as-a-service, disaster recovery as-a-service, and, when approved by the appropriate authorities, Rap Back as-a-service, a capability of the FBI's Next Generation Identification (NGI) system that provides authorized agencies notification of criminal activity and, in limited cases, of civil activity, that occurs after the initial processing and retention of criminal or civil transactions.

NEC

NEC has developed NeoFace® Watch, which is a high performance, highly scalable face recognition software application, providing the very accurate and fastest results for some of the most demanding real-time or post-event face recognition use cases, including: large volumes of data throughput, large numbers of users, large numbers of devices, and large scale deployments. The system works by obtaining facial images from video streams (CCTV surveillance cameras,

mobile video cameras or archived video footage), still image storage (mobile cameras, smart devices and digital databases) and third-party integrated systems. The system then assesses individual frames of video and still images, detects faces and analyses each face to determine its unique facial signature. The system then creates a small template for each unique face and then compares each template image against an enrolled image database until a match is found. The system maintains a history of matches and then allows configuration of real-time alerts or messages to be sent to users or external integrated systems if there is a positive match against a database image.

DERMALOG

DERMALOG AFIS is the result of more than 20 years of experience in the development of Automated Fingerprint Identification Systems, DERMALOG's core product. Being a pioneer in the field of automated fingerprint identification DERMALOG's AFIS has helped tremendously to revolutionize forensic fingerprint analysis more than two decades ago. Since then, DERMALOG's AFIS has been implemented in numerous large scale mission critical projects all over the world. Due to continuous advancements DERMALOG has managed to develop an identification system that is far ahead of its time, being the first ever AFIS in the world capable of matching more than 129 million fingerprints within one second on a standard server without loss of accuracy. The renowned international SGS INSTITUT FRESENIUS has acknowledged that this combination of speed and accuracy is unique throughout the world. Simple and intuitive to operate, DERMALOG AFIS is synonymous for the highest levels of reliability and security.

Gemalto

Gemalto offers Protiva Defender Suite, a product portfolio specifically designed for law enforcement agencies, justice and security departments and first response teams. Protiva Defender Suite is a comprehensive portfolio of easy-to-use, easy-to-deploy authentication software, digital credentials, secure devices such as ultra-secure smart cards, one-time passwords (OTP), mobile PKI and related services. This extensive solution comes in direct response to the growing number of mobile computing devices used by civil servants, and solves their need to have a convenient way to securely access law enforcement central networks. Protiva Defender Suite also directly addresses the increasing industry regulations mandating strong digital identity verification when accessing secure networks containing citizen information. Protiva Defender Suite is a solution for law enforcement and other civil servants who regularly conduct their work out of the office. With a single identity credential, officers can quickly and securely gain access and transfer critical information from anywhere, through any digital media device, such as a tablet or customised handheld device. In addition, they can perform administrative tasks remotely, file paperwork securely, protect e-mail communication, and digitally sign documents, reducing physical paper forms with verified electronic versions. Protiva Defender Suite can also be extended to integrate eCitation solutions that dematerialise and streamline citation issuance for violations and payment processing, resulting in fewer errors and lower costs. Gemalto recently acquired 3M's identity management business.

Animetrics

Animetrics, through its ForensicaGPS product, offers an advanced investigative facial recognition solution for law enforcement and forensic investigators. The product allows law enforcement agencies to convert 2D images into 3D avatars for facial feature superimposition. The firm also provides its FaceR Identity Management Solution, which is a centralized storage and management system for advanced 3D facial recognition powered by Animetrics' FaceR technology. Animetrics' FaceR technology can be used to find human faces, detect feature points, correct for off angle photographs, and ultimately perform facial recognition. The Animetrics Face Recognition API will also detect and return the gender and orientation, or "pose" of faces along 3 axes.

Aware, Inc.

Aware, Inc. provides a wide variety of biometric solutions for law enforcement applications, helping police perform fingerprint identification and face recognition, and also to utilize centralized AFIS and ABIS biometric identification services, such as those provided by the FBI. Live scan and card scan fingerprints, palm, face, and iris modalities are all supported. At the heart of several Aware solutions for law enforcement is Biometric Services Platform (BioSP™). BioSP is an off-the-shelf software product that runs on a server to execute custom workflows and data processing steps. It is configurable to support specific data formatting and routing requirements, and can be easily installed in a network to 1) ensure an open, modular network design that is agnostic to specific hardware and software products, 2) make EFTS records more accessible and useful, 3) save time and prevent errors through automation of critical functions, and 4) ensure compliance and quality. BioSP-based solutions include the Mobile Device Gateway Server used to enable search of biometric databases from mobile devices, and search of local biometric data such as mugshots. Administrators can configure the system, read and edit data, and run custom reports from a browser. Aware also provides workstation applications for biometric capture and forensic analysis. URC is a biometric enrollment application. FaceWorkbench is used to submit facial images to the FBI's Interstate Photo System or some other facial image database, then analyze the results to determine a match. There are other useful forensic applications in the firm's WorkbenchSuite family of products.

BioID Technologies

BioID Technologies provides devices designed for the public safety applications in the field. Its BioTablet™ is an Android based multi-biometric device which is FBI EBTS Appendix F Mobile ID certified, and designed to rapidly authenticate the identity of an individual by using their demographic and biometric data. The BioTablet™ delivers the highest degree of speed and accuracy for mobile fingerprint capture to ensure the best image quality required in the process of 1:1 verification or 1:N identification. Its BioMatch™ device is designed to rapidly authenticate the identity of an individual by using their demographic and biometric data. The BioMatch™ delivers the highest degree of speed and accuracy for mobile fingerprint capture to ensure the best image quality required in the process of 1:1 verification or 1:N identification.

FaceFirst

Headquartered in Los Angeles, FaceFirst empowers organizations to detect and deter real-time threats, transform team performance and strengthen customer relationships. FaceFirst proudly develops software in the United States that is used worldwide by retailers, airports, military bases, and other great organizations. The firm is the market leader in robust facial recognition software for law enforcement, including police, highway patrol, sheriff departments and other public safety agencies. The FaceFirst security platform is highly accurate and scalable, offering a full range of biometric surveillance, mobile and desktop forensic face recognition capabilities for a wide range of needs, including patrols, station security and investigative work. The FaceFirst API easily integrates with existing data and technology systems.

Imageware

Imageware offers law enforcement software that is a scalable, easy-to-use digital booking, identification, and investigative solution accessible via PC, Web, wireless, and data sharing platforms. IWS Law Enforcement database software components listed below cover the full range of Law Enforcement booking and investigation. ImageWare's Law Enforcement database software creates records and captures images (facial, fingerprint, iris, SMT, etc.) as well as biographic text data. This information may easily be synchronized with existing agency's JMS, RMS, or Livescan systems so redundant data entry is either limited or eliminated. Officers can use this law enforcement records management sofware to perform detailed searches that allow them to create unique reports and print ID badges or wristbands. The investigative module of Image-

Ware Law Enforcement software provides for the creation of non-prejudicial electronic mug books and photo lineups. In-depth searches allow for the display of similar images, either in a printed format or displayed directly from a computer screen, for viewing by a witness. The Web version of the ImageWare Law Enforcement database software allows a user with credentials to search, view, and print record information/images from any computer that may access the intranet. The creation and printing of electronic mug books and photo lineups are also included. The software supports facial recognition which adds significant power to the suspect identification process. This option searches through the database for matches to a suspect probe image. All potential matches to the image are displayed quickly and in order of confidence. Facial recognition searches may be performed via the Investigative or Law Enforcement Web client.

Tygart Technology

Tygart Technology offers a video and photo forensic analysis system called MXSERVER™. MXSERVER is a server-based system that processes vast amounts of video and photo collections quickly transforming files extracted from captured computers, cell phones, SIM cards and video surveillance systems into searchable resources. MXSERVER is enabling forensic examiners, investigators and security personnel to more efficiently and effectively analyze video and photo collections to discover, document, and disseminate information of intelligence/investigative value. The system enables real-time collaboration among users by leveraging next-generation Web 2.0 and Cloud Computing technologies – which are revolutionizing collaboration, knowledge sharing and system scalability in the public sector.

Identiwhorl

Identiwhorl is an Australian company delivering the future of mobile biometrics with a focus on law enforcement and the security industry. The company's flagship product is the Identiwhorl mobile app, for law enforcement field identification. It captures and identifies fingerprints using the built-in camera of standard consumer smartphones. It can be delivered as a standalone app, embedded in an agency's own mobile software or as a complete patrol solution, operating on Android, iOS, Blackberry or Windows.

Sciometrics

Sciometrics, formerly Gannon Technologies Group, has been developing object recognition technology, primarily under the sponsorship of the U.S. government, for over a decade. The technology emerged from optical character recognition technology, and its first new target was handwriting recognition for the intelligence community. The firm's discoveries led to algorithms for multiple languages in handwriting biometrics, which is now used by the FBI and DOD. Over the last decade, Sciometrics has used its graphing techniques to perform a number of pattern recognition research and development projects for intelligence and law enforcement agencies. Utilization of the algorithms for more general distribution has taken place over the last three years, resulting in our two current products: AFIS Afterburner our advanced fingerprinting product and FlashID, which is our industry leading handwriting biometric product. Currently, Sciometrics products have been tested and used by the FBI and the Department of Defense.

Intellicheck

Intellicheck's Law ID® increases an officer's situational awareness by making it possible to quickly scan an unknown contact's ID while minimizing the officer's loss of visual contact with that person. With Law ID® an officer can quickly scan an unknown contact's ID with minimal loss of visual contact. Law ID® instantly authenticates the contact's identification using a smartphone or tablet. Law ID instantly authenticates the contact's identification using a smartphone or tablet. Highlighted, critical fields from DMV and criminal records are also clearly visible at a glance, so the officer can quickly assess whether caution is warranted. The system enhances officer and citizen safety with real-time authentication of scanned identification on a smartphone

or tablet and enables officers to quickly view highlighted, critical fields of DMV and criminal records without losing sight of the contact. The system also improves reporting accuracy and efficiency by automatically populating incident report forms with data from retrieved records and increases citizen safety by providing instant situational awareness to the officer that can quickly deescalate a potentially tense encounter. The system also provides accurate and up-to-date data by authenticating all U.S. state, Department of Defense and Canadian province barcode formats and also offers extended search capabilities via fast integration with other government and custom databases. The system is available as a subscription service or customized solution designed to meet specific needs.

Access Control

Access control is any mechanism or system that manages access through the authorization or revocation of rights to physical or logical assets within an organization. Access control systems vary widely in type and complexity. However, regular access control systems consist of at least the following basic components: access cards and card readers. Biometric access control, on the other hand integrate devices including fingerprint readers, retinal eye scanners and hand geometry readers. Unlike keys, cards or number sequenced entry controllers, biometric security readers provide access control that cannot be transferred. Access control systems utilizing biometrics are now beginning to gain prominence in jails and prisons to control physical access to premises by law enforcement authorities.

DNA

Law enforcement is coming to increasingly rely on the use of DNA-based technologies as an aid in solving crimes. Although not yet at the point of other biometric technologies in terms of speed, DNA matching cannot be ignored in this discussion. DNA is being used to process criminal suspects to separate the guilty from the innocent. It is also being used to identify victims and to match convicted offenders to outstanding crimes. To aid these processes, the establishment of DNA data banks is either underway or under consideration in several jurisdictions including Canada and the United States.

DNA is generally used to solve crimes in one of two ways. In cases where a suspect is identified, a sample of that person's DNA can be compared to evidence from the crime scene. The results of this comparison may help establish whether the suspect committed the crime. In cases where a suspect has not yet been identified, biological evidence from the crime scene can be analyzed and compared to offender profiles in DNA databases to help identify the perpetrator. Crime scene evidence can also be linked to other crime scenes through the use of DNA databases.

Among various possible biometric modalities, DNA provides the most reliable personal identification. It is intrinsically digital, and does not change during a person's life or at the time of their death.

Deoxyribonucleic acid is a molecule that encodes the genetic instructions used in the development and functioning of all known living organisms and many viruses. In the human body, DNA, which can be thought of as the blueprint of biological design, is folded inside the nucleus of each cell. It is estimated that the human body is composed of approximately 60 trillion cells.

DNA are nucleic acids. Alongside proteins, they compose the three major "macro-molecules" essential for all known forms of life. DNA is a polymer, and is composed of nucleotide units that each has three parts: a base, a sugar, and

a phosphate. The bases are adenine, guanine, cytosine and thymine, abbreviated A, G, C and T, respectively. These four letters represent the informational content in each nucleotide unit. DNA also has a backbone made of alternating sugars (deoxyribose) and groups of andphosphate material (which is related to phosphoric acid), with the nucleobases (G, A, T, C) attached to the sugars.

DNA is well-suited for biological information storage, since the DNA backbone is resistant to cleavage and the double-stranded structure provides the molecule with a built-in duplicate of the encoded information.

Variations in the nucleotide sequence bring about biological diversity, not only among human beings but among all living creatures. Phosphate and sugar form the backbone structure of the DNA molecule. Within a cell, DNA exists in a double-stranded form, which can be visualized as two antiparallel strands that spiral around each other in the form of a double helix.

DNA is an excellent biometric identifier because it unique to each individual. Although 99.9 percent of human DNA sequences are the same in every person, enough of the DNA is different to distinguish one individual from another, unless they are monozygotic twins.

Biometrics use methods for unique recognition of humans based upon one or more intrinsic physical or behavioral traits. DNA can be classified as one of humanity's most intrinsic features. As a result, DNA profiling is often used for criminal investigations.

The DNA profiling technique was first used in 1984 and devised by Alec Jeffreys at the University of Leicester in England. The technique is now the basis of several national DNA databases used for criminal justice. Dr. Jeffreys's profiling technique was made commercially available in 1987, when Imperial Chemical Industries (ICI) started a blood-testing center in England.

DNA profiling begins with a sample of an individual's DNA (typically called a "reference sample"). The most desirable method of collecting a reference sample is the use of a buccal swab, a non-invasive collection of DNA cells from a person's cheek, which reduces the possibility of contamination.

When this is not available, other methods may be used to collect DNA, including: a sample of blood, saliva, semen, or other appropriate fluid or tissue from personal items such as a toothbrush or razor. Stored samples such as banked sperm or biopsy tissue can also be used. Samples obtained from biological relatives can also provide an indication of an individual's profile, as can human remains, which had been previously profiled.

A reference sample is then analyzed to create the individual's DNA profile using one of a number of techniques, which include RFLP, PCR and STR analysis, as well as Y-chromosome and mitochondrial analysis, along with AmpFLP and DNA family relationship analysis.

The DNA profile is then compared against another sample to determine whether there is a genetic match. Such profiling is often used to solve high-impact and high-profile crimes, such as murder and rape. The technology has be popularized in the media, by highly-rated dramas such as the CSI: Crime Scene Investigation television franchise.

DNA evidence is generally linked to DNA offender profiles through DNA databases. In the late 1980s, the federal government laid the groundwork for a system of national, state, and local DNA databases for the storage and exchange of DNA profiles. This system, called the Combined DNA Index System (CODIS), maintains DNA profiles obtained under the federal, state, and local systems in a set of databases that are available to law enforcement agencies across the country for law enforcement purposes. CODIS can compare crime scene evidence

to a database of DNA profiles obtained from convicted offenders. CODIS can also link DNA evidence obtained from different crime scenes, thereby identifying serial criminals.

In order to take advantage of the investigative potential of CODIS, in the late 1980s and early 1990s, states began passing laws requiring offenders convicted of certain offenses to provide DNA samples. Currently all 50 states and the federal government have laws requiring that DNA samples be collected from some categories of offenders.

The acronym CODIS describes not only the software used to maintain and operate law enforcement DNA databases but also the FBI's program of software support and training for federal, state, local, and international forensic laboratories. The acronym NDIS stands for the National DNA Index System or National DNA database, the highest level of the CODIS hierarchy (national, state, and local).

One of the underlying concepts behind the development of CODIS was to create a database of a state's convicted offender profiles and use it to identify suspects for crimes in which there are no suspects. Historically, forensic examinations were performed by laboratories if evidence was available and there was a suspect in the case. Beginning in the early 1990s, states began to create databases of the DNA profiles of convicted sex offenders and other violent criminals. The databases allowed federal laboratories to analyze those cases without suspects and search those DNA profiles against the database of convicted offenders and other crime scenes and determine if a serial or recidivist rapist was involved. It is expected that this new tool will enable forensic laboratories to generate investigative leads or identify suspects in cases, such as stranger sexual assaults, where there may not be any suspects.

An identification tool that was initially thought to benefit the investigation of sexual assault cases has proven to have wider application in the investigation and prosecution of crimes. States have observed this firsthand with their CODIS hits and sought to expand coverage of their databases beyond convicted sexual offenders—first to more serious violent felony offenders, then all felony offenders, and now to persons arrested for sexual offenses and, in many states, persons arrested for any felony offense. Currently, 26 states, the federal government, the Department of Defense, and Puerto Rico upload DNA profiles of various categories of arrestees to NDIS. Twelve states are collecting DNA samples from all felony arrestees, and another 15 states are authorized to collect DNA samples from persons arrested for serious felonies such as murder, manslaughter, kidnapping, sexual assault, robbery, and burglary. Another dozen states have legislation pending to authorize the collection of DNA samples from arrestees or to expand their current coverage of arrestee sample collections.

The CODIS software is used to maintain these DNA databases and search the DNA profile against the DNA profiles of convicted offenders/arrestees and other crime scenes. For example, a DNA profile of a suspected perpetrator is developed from the sexual assault evidence kit. If there is no suspect in the case or if the suspect's DNA profile does not match that of the evidence, the laboratory will search the DNA profile against the Convicted Offender and Arrestee Indices. If there is a match in the Convicted Offender or Arrestee Index, the laboratory will obtain the identity of the suspected perpetrator. If there is no match in the Convicted Offender or Arrestee Index, the DNA profile is searched against the crime scene DNA profiles contained in the Forensic Index. If there is a match in the Forensic Index, the laboratory has potentially linked two or more crimes together and the law enforcement agencies involved in the cases are able to share the information obtained on each of the cases.

The FBI Laboratory works closely with the DNA and CODIS communities as well as other stakeholders, such as laboratory accrediting bodies, law enforcement, defense attorneys, and prosecutors, to evaluate new technologies and procedures for the CODIS program (e.g., familial searching, NDIS enhancements, Rapid DNA). Over the years, the CODIS software has been updated to include the collection and mainte-

nance of additional data elements to facilitate missing person searches, upgraded telecommunications circuits, and routers, to name a few. Many of these CODIS technologies and procedures included consultation with the affected stakeholders, software development, testing, evaluation, implementation planning, and user training; processes that the FBI continues to follow for Rapid DNA.

CODIS is installed in approximately 200 federal, state, and local forensic DNA laboratories nationwide. The FBI provides the CODIS software to public forensic DNA laboratories that are accredited, that follow the FBI Director's quality assurance standards, that are audited annually, and that agree to comply with the Federal DNA Act for participation in NDIS. To date, CODIS has generated more than 285,000 investigative leads for law enforcement. All 50 states, the FBI, the U.S. Army Criminal Investigation Laboratory, and Puerto Rico contribute DNA records to and participate in the National DNA Index System. As of June 1, 2015, NDIS contains almost 14 million offender/arrestee DNA records and over 630,000 forensic (crime scene) DNA records.

When used to its full potential, DNA evidence solves and prevents the most serious violent crimes. However, the current federal and state DNA collection and analysis system needs improvement. In many instances, public crime labs are overwhelmed by backlogs of unanalyzed DNA samples. In addition, these labs may be ill-equipped to handle the increasing influx of DNA samples and evidence. The problems of backlogs and lack of up-to-date technology result in significant delays in the administration of justice. In order to clear out the backlog, new technological advances are now being employed. New portable rapid DNA machines are being designed for use by law enforcement officers in booking stations to initiate DNA collection of arrested individuals in order to expedite analysis.

With several government agencies in the United States and Europe incentivizing development efforts, the first generation of "Rapid DNA" prototypes systems have been made available for evaluation.

Lockheed Martin and ZyGEM Corp. Ltd. released a version of their rapid DNA analysis platform in 2012 designed to simplify and speed DNA analysis for human identity testing. Pre-production units of the platform will be released this summer to select customers in the forensic, homeland security and intelligence communities.

With the successful development of a fully-integrated cartridge device, new Rapid DNA platforms have the potential to transform today's existing DNA identification process from one that takes a great deal of training, sophisticated equipment and time into a far simpler, more affordable process that can be performed in the lab or field in under 90 minutes.

Lockheed's platform leverages the latest in microfluidic research and development to accelerate the DNA identification process, essentially building a laboratory on a small, single chip that reduces the processing steps and time needed for analysis.

Lockheed is targeting its rapid DNA system to assist the U.S. Department of Justice's backlog of DNA requests. It is expected that the technology will also be of interest to law enforcement agencies in the United States and the United Kingdom.

Field-testing has also occurred of another mobile, rapid DNA lab service that yielded full DNA profiles in two hours or less. RapidHIT, the system developed by IntegenX Inc. and Promega Corporation will allow law enforcement to produce DNA profiles for human identification from mouth swabs and other human samples.

The RapidHIT service has been described as a breakthrough sample-to-profile biometric system because it allows DNA analysis at the point

of collection, such as an arrest or detention, setting a new standard in the usage of DNA profiles as an actionable biometric.

By contrast, human DNA samples currently must be transported or shipped to laboratories that rely on highly trained technicians using multiple instruments for analyses taking 10 to14 hours, with access to results delayed up to 30 days or more.

It is important to note that Rapid DNA is still considered experimental. The FBI uses the term "Rapid DNA analysis/technology" to describe the fully automated (hands-free) process of developing a CODIS Core Short Tandem Repeat (STR) profile from a reference sample buccal swab. The 'swab in—profile out' process consists of automated extraction, amplification, separation, detection, and allele calling without human intervention. The FBI's objective for Rapid DNA technology is to generate a CODIS-compatible DNA profile and to search these arrestee DNA profiles within two hours against unsolved crime (forensic) DNA while an arrestee is in police custody. Rapid DNA technology has been designed for use within and outside the forensic DNA laboratory, as the Rapid DNA instruments are self-contained machines that require no human intervention beyond the loading of the DNA samples and analysis cartridges into the machines.

Following any legislative authority, the FBI envisions Rapid DNA integration occurring in two-phases. Phase 1 involves the booking station CODIS enrollment and searching of Rapid DNA profiles. Phase 2 of integration is the direct "hit notification" to booking stations and investigative agencies. The initial (Phase 1) impact of Rapid DNA analysis in the booking station will be the elimination of the weeks-to-months it currently takes for arrestee samples to be mailed, received, inventoried, and analyzed for registration in the CODIS system. The eventual real time notification (Phase 2) of an arrestee's DNA hit to an unsolved case is expected to conserve valuable investigative resources and focus them on specific arrestees. Equally as important will be the protection of the public when perpetrators are identified at the point of collection before being released back into their communities at the completion of the normal booking process. Rapid DNA CODIS registration will not lengthen the booking process.

The FBI initially established a Rapid DNA initiative in 2006 and partnered in 2008 with the Departments of Defense and Homeland Security on the development of point-of-collection DNA analysis for the production of CODIS DNA profiles (containing the 13 CODIS Core Loci) within a two-hour period. In 2010, the Criminal Justice Information Services' Advisory Policy Board (CJIS APB, a federal advisory committee established by the FBI) established a Rapid DNA Task Force, and the FBI's Rapid DNA Program Office was created within the FBI Laboratory Division to coordinate the Laboratory and CJIS Division's Rapid DNA activities. These groups have provided the FBI with recommendations that we have adopted for our Rapid DNA implementation, such as the use of the State Identification Number (SID) as the cornerstone identifier for Rapid DNA profiles and the addition of a data element to an individual's criminal history record to indicate whether there is a DNA profile already in CODIS, information which will assist states in determining if a DNA sample should be collected at arrest.

For implementation within an accredited forensic laboratory, the Scientific Working Group on DNA Analysis Methods (SWGDAM) empanelled a Rapid DNA Committee to review and evaluate whether additional quality measures were necessary to ensure the accuracy and reproducibility of the records produced by the Rapid DNA instruments. Based upon recommendations received from SWGDAM, the FBI issued an addendum to the quality assurance standards for DNA Databasing Laboratories, required by Federal law, providing a foundation for implementation of Rapid DNA within an accredited forensic DNA laboratory.

The FBI Laboratory is also developing CODIS software modifications to facilitate the searching of Rapid DNA instrument-generated DNA profiles against forensic DNA records. Along with these development efforts, steps are being taken to identify information technology

enhancements needed for state criminal history record repositories, booking stations, regional, county, and local jails, to comply with FBI CODIS requirements for uploading DNA records generated at the time of arrest. As noted previously, Rapid DNA technology has been designed for both laboratories (approximately 200 forensic DNA laboratories participating in CODIS) as well as law enforcement booking agencies across the nation (potentially thousands of law enforcement booking facilities).

The CJIS and Laboratory Divisions are working together to determine the interfaces necessary for the integration of the Rapid DNA components into the criminal history record and booking station infrastructure originally established for the Automated Fingerprint Identification System (AFIS). As one example, integration of the Rapid DNA instruments with CODIS and Arrestee State Identification Numbers is necessary to facilitate the notification of CODIS hits to law enforcement agencies in order to act on investigative leads. The FBI Laboratory's Rapid DNA Program Office is working with the CJIS APB's Rapid DNA Task Force to plan Rapid DNA workflows and develop requirements for implementation.

The Federal DNA Act requires that the DNA records maintained at NDIS be generated by accredited laboratories in compliance with the FBI Director's quality assurance standards (42 U.S.C. §14132(b)). Rapid DNA technology has been designed for use by law enforcement agencies at the point of booking for integration following live scan fingerprint enrollment of an arrestee. Thus, statutory authorization for the use of FBI approved Rapid DNA instruments by criminal justice agencies would be needed before the DNA records generated at police booking stations can be searched at NDIS.

The emergence of DNA as a crime solving tool, along with greater investments in all biometric modalities for law enforcement means that innovation will continue to flourish. Biometric Research Group expects continued growth as advanced countries increase their investments with the intent to modernize their criminal justice systems.

World Border Security Congress

20th-22nd March 2018

Madrid, Spain

www.world-border-congress.com

Collaboration and Interaction for Action

Converging and Enhancing Border Security Through Constructive Dialogue

SAVE THE DATES

The world is experiencing the largest migration movement in history, with challenges for the border management and security community, as little sign of peace and security in the Middle East is apparent and porous borders in Africa and Asia continue to provide challenges.

International organised criminal gangs and human and drug trafficking groups exploit opportunities and increasingly use the internet and technology to enhance their activities.

Controlling and managing international borders in the 21st Century continues to challenge the border control and immigration agencies around the world. It is generally agreed that in a globalised world borders should be as open as possible, but threats continue to remain in ever evolving circumstances and situations.

Advancements in technology are assisting in the battle to maintain safe and secure international travel. The border security professional still remains the front line against these threats.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

REGISTRATION NOW OPEN

Register online today at www.world-border-congress.com

We look forward to welcoming you to Madrid, Spain on 20th-22nd March 2018 for the next gathering of border and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

---

Supported by:

ISIO - International Security Industry Organization

International Association of CIP Professionals

NS&RC

Media Partners:

BORDER SECURITY REPORT

WORLD SECURITY REPORT

World Security-index.com