BIOMETRICS RESEARCH GROUP, INC.

Port Security
White Paper

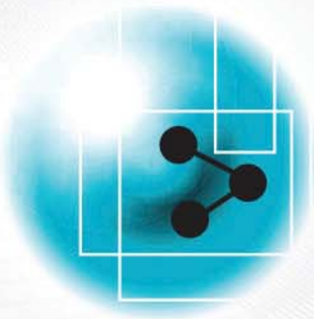
This paper examines biometric transportation worker credentialing at U.S. seaports along with the security challenges caused by lack of holistic biometric access control options.

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

All content, including forecasts, analysis and opinion, has been based on information and sources believed to be accurate and reliable at the time of publishing. Biometrics Research Group, Inc. makes no representation of/or warranty of any kind as to the accuracy or completeness of any information provided, and accepts no liability whatsoever for any loss or damage resulting from opinion, errors, inaccuracies or omissions affecting any part of the content.

FEDERAL REPUBLIC OF HAPPY TRAVELLERS
PASSPORT
PASSEPORT
Type/Type
P
Code/Code
FRHT
Surname/Nom (1)
TAYLOR
Given names/Prénoms (2)
ERIC
Nationality/Nationalité (3)
HAPPY CITIZEN
Date of birth/Date de naissance (4)
28 DEC /DEC 49
Sex/Sexe (5)
M
Place of birth/Lieu de naissance (6)
HAPPY TOWN
Date of issue/Date de délivrance (7)
13 MAY /MAI 11
Date of expiry/Date d'expiration (9)
28 MAY /MAI 21
Authority/Autorité (8)
IPS
Holder's signature/Signature du titulaire (10)
Taylor
P<FRHTRTAYLOR<<ERIC<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
7188508301FRHT5023395M3216397<<<<<<<<<<<<<<<<<<<<<<<<13

IDGA
Institute for Defense and
Government Advancement presents . . .



BIOMETRICS FOR GOVERNMENT & LAW ENFORCEMENT

January 26-28, 2015 | Washington DC

Biometrics for Government and Law Enforcement returns for its 9th consecutive year as the only biometrics event to exclusively cater to the needs of federal government and local law enforcement. Join hundreds of biometric professionals (both industry and end users) to preview the future of biometric initiatives and technology, first hand from those leading the direction of our upcoming efforts.

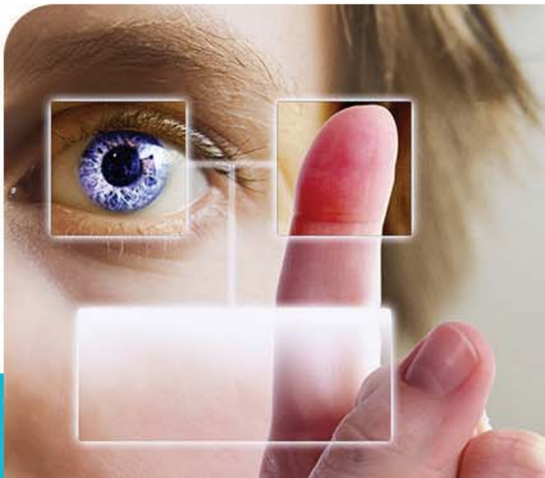
Featured Speakers:

- **Leslie Hope,** Biometrics Chief, **DHS/UCIS**
- **James Loudermilk,** Senior Level Technologist, **DOJ**
- **Chris Melton,** Biometrics Training Lead, **U.S. Army**
- **Paul Good,** Assistant Chief, Biometrics, **Office of Border Patrol Enforcement Systems**
- **Jeremy Slavish,** Director of Biometrics/Identification, **Michigan State Police**

Topics will include:

- Reducing error margins in facial scans and fingerprint scans
- Improving identification rates of latent and forensic scans
- Securing biometrics tools from cyber attacks and evasive tactics
- Mobilizing biometrics scanning mediums
- Establishing national data standards and formats for improved interoperability
- Providing core training and implementation initiatives for hands on operators

For more information, including full speakers and sessions, visit:



www.BiometricsEvent.com

TABLE OF CONTENTS

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.

Port Security Overview

Due to the large amount of trade transacted on the high seas, port security must always be a major international consideration. It is estimated that more than 4,000 ports make up the world's maritime transportation system. The United Nations Conference on Trade and Development (UNCTAD) estimated in 2001 that 5.8 billion tons of goods were traded by sea in 2001, equaling more than 80 percent of the world's trade. Because ports are the main point-of-entry for most of the world's imported cargo, a large amount of risk exists in the maritime transportation system, since ports constitute major targets for international terrorist and criminal syndicates.

Ports are inherently vulnerable to terrorist attacks and criminal activity due to their size. They are generally located in open and accessible metropolitan areas, near both water and land, where large amount of goods are transported, including hazardous materials, vis-a-vis a multitude of transportation links. Ports are usually large facilities, housing many asymmetrical activities, dispersed over hundreds of acres of land and water, which simultaneously accommodate ship, truck and rail traffic, petroleum and liquid offloading, as well as container storage. With so many activities occurring at one geographic space, a port and its associated facilities and infrastructure collectively represent one of the single greatest unaddressed challenges facing the security of nations and the global economy.

Both the private sector and international governments have identified a myriad of weaknesses in port security within the United States and throughout the world. Much of the security weakness revolves around the lack of specific international security standards. While port facilities must have security plans, security officers, and certain security equipment, there is no uniform code specifying security protocols. As a consequence, there are no minimum training standards for security staff and no mandatory guidelines for what constitutes perimeter security at a port. The U.S. government however has taken some slow steps to enhance security. Since the inception of its International Port Security Program in 2004, the U.S. Coast Guard (USCG) has assessed the effectiveness of antiterrorism measures in more than 1,000 foreign port facilities. The Coast Guard conducts an average of 200 assessments per year. In addition, in support of the U.S. armed forces and international efforts to build maritime security capacity and protect the maritime environment, USCG port security units provide security at strategic port locations. However, though the U.S. has focused on enhancing security in key locations, it still has not mandated requirements that govern facility access controls. Physical security provisions at seaports are often therefore only defended with guns, gates, guards, and identification cards.

Notwithstanding the current lack of standards and enforcement authorities, port facility owners, operators, and the maritime industry are certainly able to take independent actions to protect their assets. Biometrics Research Group, Inc. identifies port security in the United States as a potential US$750 million revenue opportunity for original equipment manufacturers and installers in the biometric sector. While the U.S. government has created a defined credential for transportation workers, access control standards do not exist. The greatest opportunity to enhance revenue streams will therefore stem from attempts to upgrade security measures that control facility access.

Transportation Worker Identification Credential (TWIC)

Currently, the main biometric initiative undertaken by the U.S. government concerning port security surrounds the introduction, deployment and use of the "Transportation Worker Identification Credential" (TWIC). The credential was established by Congress through the Maritime Transportation Act of 2002. It is administered by the Transportation Security Administration (TSA) and U.S. Coast Guard.

TWICs are tamper-resistant biometric credentials issued to all USCG credentialed merchant mariners, as well as workers who require unescorted access to secure areas of ports and vessels.

The TSA issues workers a tamper-resistant smart card containing fingerprint biometric data, to allow for a positive link between the card itself and the individual carrying it. Facility and vessel owners/operators are required to notify employees of their responsibility to possess a TWIC based on their need to have unescorted access to secure areas of vessels and facilities. Federal guidelines state that employer notification should be provided in a timely manner to give individuals sufficient time to complete the entire enrollment process by the compliance date.

Facility owners and operators are encouraged to provide this same information to personnel who are not facility or vessel employees, such as contractors and truck drivers. Contractors, who are not direct employees of a port owner or operator, can apply for a TWIC as long as they meet the eligibility requirements and, at a minimum, are expecting to pursue contracts on federally regulated vessels and facilities where the owners or operators have determined a need for unescorted access in secure areas. If circumstances change and the individual no longer meet certain conditions, they are required to surrender their TWIC.

In April 2009, all USCG credentialed mariners had been required to hold a TWIC in order for their license, Merchant Mariner Document (MMD), Certificate of Registry (COR), or Standards of Training, Certification, and Watchkeeping (STCW) endorsement to remain valid.

Applicants obtain a TWIC by way of a three-step process. Step one involves an applicant visiting a government Web site to pre-enroll and schedule an appointment at the nearest enrollment center. Step two involves the actual visit to an enrollment center in person, in order to produce identification documents and be photographed, along with submitting fingerprints. The application is then encrypted and securely sent to the government for a background check. Step three involves notification of approval or rejection. If approved, a subsequent appointment is scheduled at the enrollment center where the original application was made. There, the applicant's identity will be verified allowing the TWIC card to be activated. The cards can be picked up at the center or mailed to the applicant's home.

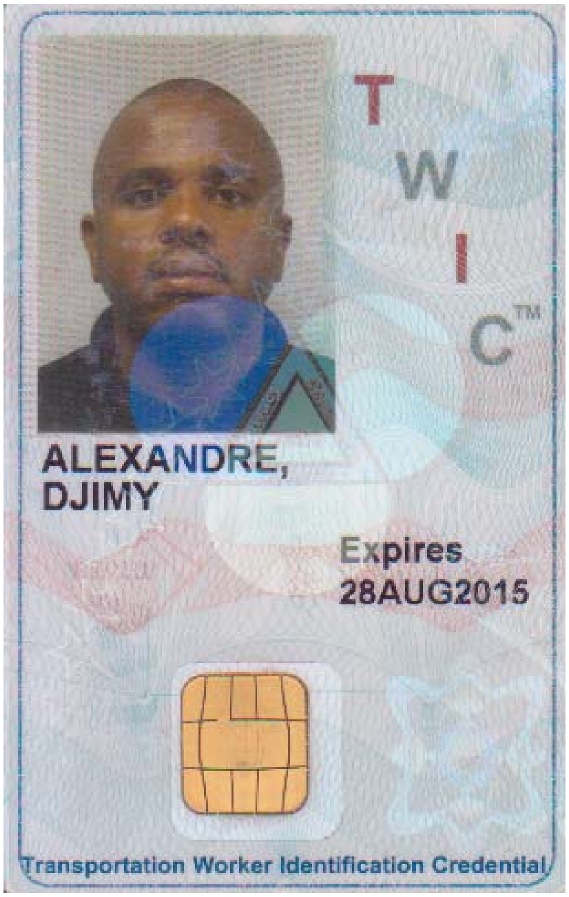
During the process, an applicant's eligibility is determined. TSA completes a security threat assessment based on the name and identity documents presented at the time of enrollment. This security threat assessment is tied to a specific identity. In the event of a name change, an individual is required to re-enroll with the information and documentation supporting the name change. This triggers a new assessment to be performed.

An applicant is permanently disqualified if convicted of the following felonies: Espionage, sedition, treason, terrorism, a crime involving a transportation security incident, improper transportation of hazardous material, unlawful acts involving explosives, murder, bomb threats, serious racketeering offenses, or attempts or conspiracy to commit these acts.

An applicant can also be disqualified for a period of over five to seven years for other convictions. These include: unlawful acts involving firearms, extortion, fraud (not include welfare or passing bad checks), bribery, smuggling, immigration violations, drug distribution and importation, arson, kidnapping, rape, assault with intent to kill, robbery, fraudulent entry into a seaport, and lesser racketeering offenses, or attempts to commit such acts.

In addition to criminal offenses, TSA will determine immigration status and look for records indicating mental incapacity. TSA may also conduct other analyses, including searching international databases, terrorist watch lists, National Crime Information Center (NCIC) databases, and may search to see if other foreign or domestic criminal convictions exist.

TWICs last for five years, unless the expiration date is based on a comparable credential such as the Free and Secure Trade (FAST) card, Merchant Mariner Document/License, or Hazmat Endorsement. The expiration date is displayed on the face of the TWIC. TWIC



holders are responsible for knowing when to begin the renewal process.

As of May 2014, according to TSA records, there were 2,999,058 people enrolled in the program. The cost for a typical, single applicant to apply is US$137.25. The TSA has therefore potentially charged at over US$410 million in TWIC application fees.

The TWIC card, as shown in the illustration below, contains a computer chip, known as an integrated circuit chip (ICC), which stores the cardholder's information and biometric data. The chip can be read by inserting it into a reader or holding it near a "contactless" reader. There is also a magnetic strip (similar to a credit card) and a linear barcode on the back of the card, which are alternative card reading methods.

During its initial rollout, TWIC was used primarily for visual identity checks. TWIC holders present their cards to authorized personnel, who compare the holder to his or her photo, inspect security features on the TWIC and evaluate the card for signs of tampering.

TWIC Approved Technology Solutions

The Coast Guard also conducts vessel and facility inspections and uses hand-held readers during spot checks to ensure credentials are valid and identity is verified. A number of portable readers have been verified by the TSA for use with the TWIC Privacy Key (TPK) and TWIC Reference Biometrics standards.

Vendor	Hardware Manufacturer/ Model	Software Company/Product	URL
Codebench	Cross Match/ Be.U Mobile	Codebench/ OMNIcheck	www.codebench.com
Codebench	DAP/ CE3240BWE	Codebench/ OMNIcheck	www.codebench.com
Codebench	Datastrip/ DSV2+Turbo	Codebench/ OMNIcheck	www.codebench.com
Codebench	Datastrip/ DSV3	Codebench/ OMNIcheck	www.codebench.com
Codebench	MaxID/ iDL500	Codebench/ OMNIcheck	www.codebench.com
Codebench	MorphoTrak/ MorphoCheck	Codebench/ OMNIcheck	www.codebench.com
CoreStreet	DAP/ 3240B	CoreStreet/ Pivman	www.corestreet.com
CoreStreet	Crossmatch/ BE.U	CoreStreet/ Pivman	www.corestreet.com
CoreStreet	DataStrip/ DSV2 Plus Turbo	CoreStreet/ Pivman	www.corestreet.com
Cross Match	Crossmatch/ BE.U SMC-800	CoreStreet/ Pivman	www.crossmatch.com
DataStrip/Codebench	Datastrip/ DSV II SC	Codebench/ TWICCheck	www.datastrip.com
Eid Passport Inc.	RAPIDGate RCx	Intermec CN3	www.eidpassport.com
idSoftware	MC 75a	idSoftware/ SecureGate Ports	www.idsoftware.us
MaxID	MaxID/ iDLMAX G	Corestreet/ Pivman	www.maxidgroup.com
MaxID	MaxID/ iDL500/ iDL500i	MaxID/ MaxIDentity Suite TWIC Application	http://usa.maxidcorp.com/idl500.php
MaxID	MaxID/ iDL300	MaxID/ MaxIDentity Suite TWIC Application	http://usa.maxidcorp.com/idl300.php
Mobilisa	Moblisa/ IM2700	Moblisa/ Defense ID	www.icmobil.com
MorphoTrak	PSION Teklogix/ Workabout Pro	MorphoTrak/ TWIC PIV Morphocheck	www.morpho.com
Motorola	Motorola/ MC 75	Motorola Mobile Software	www.motorola.com/biometrics
Port Solution Integrators	Real ID	Port Solution Integrators	www.portsolutionintegrators.com
Salamander Technologies	Motorola MC75A	InterTRAX Mobile PIV Software	http://www.salamandertechnologies.com/
Salamander Technologies	Dap Technologies 3240	InterTRAX Mobile PIV Software	http://www.salamandertechnologies.com/
TransCore	DAP/ RMT CE 3240B	CoreStreet/ PIVMAN	www.transcore.com

Ultimately, the TWIC Privacy Key (TPK) and TWIC Reference Biometrics standards are meant to be leveraged for access control requirements. The TSA has also approved a number of vendors for fixed reader deployment.

Vendor	Hardware Manufacturer/Model	Software Company/ Product	URL
3M Cogent, Inc.	MIY-ID GOV	3M Cogent, Inc.	www.cogentsystems.com
3M Cogent, Inc.	MIY-Card GOV	3M Cogent, Inc.	www.cogentsystems.com
EID Passport	Rapid Gate CN3	EID Passport	
Innometriks	Innometriks/ Rhino-XS-TWIC	Innometriks/Rhino Software	www.innometriksinc.com
L-1 Identity Solutions	L-1 Identity Solutions / 4G PIV-TWIC Station Extreme2	L-1 Identity Solutions/ Secure Admin	http://www.l1id.com/pages/664-4g-piv-twic-station- extreme
L-1 Identity Solutions	L-1 Identity Solutions / 4G PIV-TWIC Station2	L-1 Identity Solutions/ Secure Admin	http://www.l1id.com/pages/666-4g-piv-twic-station
L-1 Identity Solutions	L-1 Identity Solutions/ TWIC-Station	L-1 Identity Solutions/ Secure Admin	www.l1id.com/pages/494- bioscrypt-twic-station-
MorphoTrak	MorphoTrak/ MA120w	MorphoTrak/ Lenel/ MSO350/Maris/ TPK-ServerDemo.exe	www.morpho.com
MorphoTrak	MorphoTrak/ MA521	MorphoTrak/ Lenel/ MSO350/Maris/ TPK-ServerDemo.exe	www.morpho.com
MorphoTrak	MorphoTrak/ OMA521 Outdoor	MorphoTrak/ Lenel/ MSO350/Maris/ TPK-ServerDemo.exe	www.morpho.com
TELVENT DTN	PC3-TRB	Guardian 3 Terminal Automation System	www.telvent.com
Veridt	Veridt/ 900W0034	Veridt/AMAG symmetry 6.1 (Homeland Security edition)/Firmware Version: 010993/PIVCHECK Desktop Edition	www.veridt.com
Veridt	Veridt/ 900W0099	Veridt/AMAG symmetry 6.1	www.veridt.com
Veridt	Veridt/ 900W1020	Veridt/PIVCheck	www.veridt.com
Veridt	Veridt/ 900W1030	Veridt/PIVCheck	www.veridt.com

The above selected vendors will benefit from the next stage of biometric security implementation: which will ultimately focus on access control. TWIC cards can also be used not just at security gates but to enter secure buildings. Increased fixed unit deployment would allow for secure access points to be monitored. Of course, the logical extension of such an approach would also be to extend a biometric, fingerprint sensor-based scanner system throughout seaport facilities.

Biometric Access Control Option

With the TWIC extended beyond the physical credential, ports and government authorities will not have to contend with lost, stolen or forged badges. Fingerprint-based readers could be more readily used to determine the identity of every employee or contractor at more entry points throughout port facilities. Biometrics Research Group estimates that if the extension of TWIC credentialing was extended to all facility access control functions in the United States, then an additional US$750 million in revenue could be realized by biometrics manufacturers. Another US$250 million would also be realized by system installers.

The extension of these systems to access control functions also makes sense since they could further be extended to simplify the process of automating container handling by significantly reducing cargo handling time, while increasing security levels. Such headway in access control will only occur however if the TWIC mandate is further expanded. Press and independent government reports reveal that there are considerable challenges to simply managing and maintaining the existing system. Consequently, Biometrics Research Group does not expect a wide, concerted effort to be made towards implementing holistic access controls throughout all U.S. seaport facilities. Individual U.S. ports will continue to maintain a level of autonomy over those systems. As a result, we can expect some to look at modernizing their facilities, but we consider those ports will be in the minority. However, in the interim, biometric manufacturers and vendors will continue to innovate, as they have been doing over a number of years.

As an example, a few years back, Sense Holdings, Inc., a developer of next-generation biometric and explosive detection security technologies for government and commercial security markets, developed a market-ready biometrics-based platform technology designed to provide advanced security for maritime cargo leveraging biometrics. Sense's CheckPrint Cruisetracker Vessel Access System (CPVAS), was designed to fill a critical gap in homeland and port operations security in the maritime cruise and cargo industry.

The CheckPrint system was designed with input from security experts and represents a novel merger of new and proven technologies into a single security system that combines cutting-edge fingerprint biometrics with customizable computer databases to track authorized vendors or others on vessels and in overall shipping environments.

Ultimately, CPVAS is a real-time access control security product. The proprietary solution integrates photographic and fingerprinting identification technologies with computer database solutions to enable vessel personnel or other security personnel to track individuals moving through the ports.

The CPVAS system is based on an Intranet browser that allows internal users access on site or remotely via a Web browser application. Sophisticated, multi-layered security applications provide the hierarchy of authorization processes. In addition, the system is designed to be fully integrated with existing security systems. CPVAS also keeps track of all information and can generate printed security reports or others for transmission electronically.

In our opinion, these are the types of systems that are necessary in order to secure marine facilities. While we acknowledge that both the U.S. and the world faces a difficult task in providing effective security across all marine ports, technology, especially biometric technology exists that can improve the global port security environment.

If the U.S. makes an effort to mandate that technology to extend to access control, and asks for international use and compliance of such technology at the seaports of major exporting nations, then greater progress in terms of security will be made.

In terms of specific vulnerabilities, many worldwide maritime ports do not require background checks on dock workers, crane operators or warehouse employees. Most ports also lease large portions of their facility to private terminal operating companies, who are responsible for their own security. The result of this is a "balkanized", uneven system of port security and operations management as a whole. Such vulnerabilities can only be addressed by uniformed standards and the implementation of technological solutions. Biometrics Research Group believes that while movement towards better rules and access control implementation will be slow, innovation and development of new biometric solutions by vendors capable addressing port security challenges will be rapid. It will be up to government policymakers and decision-makers to accelerate the pace.

About the Biometrics Research Group, Inc.

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 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.