Biometric Technology Application Manual, Vol. 3

“In Their Own Words”
First Person Case Study Interviews
Spring 2010
Researched and Published by NBSP
Table of Contents:

About NBSP 3
About BTAM 4
Analysis of Case Study Interviews 9
Case Study Interviews
   Hong Kong Immigration System 17
   Union Pacific Railroad 27
   BayCare Health System 35
   Technology Credit Union 47
   Parkview Adventist Medical Center 53
   Pearson Vue 62
   Wood County WV School District 67
   Canadian Air Transport Security Administration 78
Master Summary of Interviews 89
Update On Major Government Initiatives 120
   Existing Programs 126
      US-Visit 126
      TWIC 132
      Registered Traveler 138
      Real ID 141
      NEXUS 143
      DOJ IAFIS 143
         Next Generation Identification 146
      Dept. of State
         Electronic Passport 147
         Secure Network Access 147
DoD Programs 148
   DoD Organization for Biometrics 149
   Automated Biometric Identification System 149
   Common Access Card 153
   Combat Zone Applications 158
      Biometric Automated Toolset 158
      Biometric Identification System For Access 161
The National Institute of Standards and Technology 162
   Standards Development 163
   Biometric Modal Research and Training 164
      Fingerprint Projects 164
      Face Projects 165
      Iris Projects 166
      Voice Projects 167
      Trends 167
Conclusion 168
About the National Biometric Security Project

NBSP is a non-profit biometric consultancy that provides secure biometric access control expertise to organizations seeking greater protection of their physical and cyber assets including personal information. Our ISO/IEC laboratory testing accreditation and proven performance combined with a history of biometric innovation enable us to deliver highly secure customized biometric access control solutions. Our application services, including but not limited to access control, address the complete range of biometric deployment considerations from initial vulnerability assessments to post-implementation support. As a 501 (c) (3) non-profit corporation, NBSP is able to assure a technology-neutral, vendor-independent posture and focus on user requirements.

NBSP adds dimension to its biometric application services with robust Testing, Training and Research capabilities. Performance Testing helps determine whether biometric products will meet manufacturers’ performance claims. Conformance Testing evaluates a biometric product’s conformance to applicable, published ISO/IEC standards. Custom Testing includes, for example, vulnerability assessments, comparative testing, algorithm testing, sensor testing, product development tests, and interoperability testing.

Our Introduction to Biometrics Course, and Biometric Technical Training Course provide a unique multi--course curriculum. Additionally, all students are eligible for Continuing Education Units (CEU) upon completion of any NBSP training course.

NBSP conducts research into the social impacts of biometrics, including detailed analyses of U.S. and international privacy laws and their effect on the use of biometrics. A semi-annual update of all published and emerging biometric standards is also available as a resource to anyone interested in learning more about standards progress.

The permanent staff of NBSP is efficiently supplemented, as required, by external organizations contracted to perform substantive research and technical work, highly specialized and experienced consultants, and research organizations focused on biometrics or identity matters. These include West Virginia University and other academic institutions associated with the Center for Identification Research (CITeR), as well as other reputable U.S. and international sources.

About the Biometric Technology Application Manual (BTAM)

Published by the National Biometric Security Project (NBSP), the Biometric Technology Application Manual (BTAM) is a comprehensive reference manual on biometric technology applications. This reference work, in three volumes, has been compiled for biometric technology users and for those who are evaluating biometrics as an enabling technology within an integrated system or program for security and identification assurance. BTAM is intended to be a rational and practical tool for those who specify, buy, integrate, operate, and manage biometric technology-based systems.
The experienced biometric practitioner will see much that is familiar in BTAM. The publication is not intended to provide all new (never before published) scientific information. Rather, it is a compilation of published and experience-based information designed to inform the rapidly growing community of new users, integrators, and designers, and assist them in their search for practical application solutions.

Generally, this manual has been compiled and is intended for individuals and organizations that have responsibility for protection of national defense, infrastructure security and identity protection. These include, but are not limited to:

- Civil infrastructure agencies
- Other government agencies
- Private sector organizations and businesses
- Academic institutions
- International organizations, businesses, groups, and governments
- Consultants and practitioners in biometrics
- Security and identity management administrators

There is a significant volume of valuable work on the subject of biometrics by many authors. BTAM was not published to replace that body of work, but rather to compile some of the best of that content in an organized and focused product with emphasis on the user. Equally important, the objective of BTAM is to help solve the issue of short shelf-life of biometrics publications in a rapidly evolving technology base by including a process for regular updating of each volume.

In researching and compiling BTAM, the authors relied heavily on secondary research from published, public sources. For a list of the reference materials, authors, publications, and other sources used and referenced in this compilation, please see appropriate footnotes as well as the Bibliography.

**Purpose and Objectives**

BTAM is designed to assist the reader in:

- Comparing how various biometric technologies perform and have performed in real-world applications (both successfully and unsuccessfully), and why.
- Providing a means to evaluate various biometric solutions based on specific application parameters and requirements.
- Determining where, when, and why a biometric-based solution is a good fit, or not.
- Supporting technology evaluation by defining the questions to ask, identifying other considerations that may exist, and understanding the issues generated by the need for interoperability.
- Answering such questions as: How do I write a requirement? How do I evaluate various systems? How do I integrate/apply the technology? How do I use the technology? What is the best technology for my application?
Summary Volume 3 – Biometric Case Studies... “In Their Own Words”

This latest volume of BTAM expands on the biometric fundamentals and application briefs contained in the first two volumes by focusing on biometric application case studies. Eight case studies appear in the form of interviews conducted with client and integrator personnel. The interviews crossed a broad span of market sectors including the education, medical, transportation and financial segments and covered most of the leading biometric modalities (iris, fingerprint, vascular and multimodal.)

Interviews were conducted with:
- Parkview Adventist Medical Center
- Wood County WV School District
- The Hong Kong Immigration System
- BayCare Health System
- Pearson Vue
- Technology Credit Union
- Union Pacific Railroad
- Canadian Air Transport Security Administration

Each case study interview covers (in varying degrees) the factors that led to the exploration of biometrics as a solution, the methodology for choosing the appropriate modality, evaluation of potential technology providers, the business case analysis, privacy issues and concerns, training considerations and the operational and financial impact of the technology.

In addition to the individual case study interviews, Vol. 3 features a summary update of the major U.S. Government applications. These include:
- US-Visit
- Transportation Workers Identity Card (TWIC)
- Registered Traveler
- Real ID
- DOJ Automated Fingerprint Identification System (IAFIS)
- Department of State (Electronic Passport)
- DoD Programs
  - Automated Biometric Identification System (ABIS)
  - Common Access Card (CAC)
  - Biometrics Automated Toolset (BAT)
  - Biometric Identification System for Access (BISA)
- Next Generation Identification (NGI)
- National Institute of Standards and Technology (NIST)
  - Standards Development
  - Biometric Modal Research and Testing

A synopsis of the first two volumes follows:
Summary Volume 1 – Biometrics Basics

Although the overriding purpose and objectives of this three-volume set are similar, Volume 1 was developed to be more of a primer on biometrics as it presents and defines biometrics on a fundamental level, including:

• **Fundamentals of Biometrics.** An entire Section of Volume 1 introduces biometrics so the reader has a basic foundation and generic understanding of the science behind the technology. Beginning with the origins of biometrics, and taking the reader through explanations of the terminology, elements, and performance criteria, this Section provides a solid foundation for those who are just learning about these technologies.

• **Types of Biometric Technologies.** Some biometric technologies (or modalities) are better known than others, but this Section presents information about how 11 different technologies work. Presented in both text and easy reference matrix format, it is an important Section intended to help readers understand why one technology might fit their needs more than another.

• **Biometric System Design.** This Section presents guidance and insight as to how system requirements should be defined and the appropriate performance specifications documented. Issues such as technical requirements, operational capabilities, performance expectations, architectural aspects, and other related concepts are presented in this Section.

• **Biometrics Standards and Best Practices.** The development and adoption of standards is important for the biometrics industry to become mainstream and more fully integrated into our critical infrastructure. This Section provides the reader with information as to the current state of standards development, enabling insight into the various types of biometric technologies and their vendors – where they are in terms of complying with industry-approved standards – and explaining why biometrics standards are critical to integrating full-solution systems.

• **Testing and Evaluation.** Insight regarding testing protocols and system evaluation is presented in this Section. Issues such as understanding system performance, scalability, and usability, standards compliance, performance measurement and comparison, and evaluations are discussed, providing the reader with a very practical guide for evaluating various biometric solutions.

• **Biometric Social and Cultural Implications.** This Section presents considerations on three key societal issues: legality, privacy, and user acceptance. An appreciation for these issues is critical to successfully implementing a biometric-based security and identification management solution. • **Trends and Implications.** The final Section of Volume 1 presents some key trends and implications for biometrics in general, and sets the stage for follow-on information and additional detail in Volume 2.
Summary Volume 2

Volume 2 of BTAM continues the mission to provide a complete set of reference tools that are readily available to the biometric community regardless of the reader’s specialty or level of activity in the technology. Here, we examine “best practices” and even “not so best” practices, recognizing therein that the deployment and operation of biometrics systems is still a work in progress.

• **Biometric Applications**

A biometric device can be applied in virtually any scenario in which one might otherwise use keys, identification cards, security cards, personal identification numbers (PINs), or passwords to gain access to a physical facility, a virtual domain (information system), or a process, or to determine eligibility for a privilege. The real value of biometrics is the potential for use in applications where keys, ID cards, and passwords would be of no value whatsoever: the “negative identification” applications. The application of biometric technologies is increasing over a wide array of industries as organizations and individuals look for higher levels of security and identity assurance. Advances in biometric devices have made the technology more affordable and less intimidating for applications where high security, which was a compelling reason initially, is not the primary objective. More routine applications, such as access to school dining halls, are now joining the traditional high security applications such as access to military resources and nuclear power plants. In addition, with the advent of credible identification systems (the one-to-many process of comparing a submitted biometric sample against all of the biometric templates on file to determine whether it matches any of the templates), the breadth of applications which can be achieved has expanded greatly. Today we are not limited to applications where a claimant must provide a claim of identity such as a user name, PIN, or password to facilitate the recognition process. Thus a new class of applications such as refugee processing/control, watch lists, benefits eligibility determination, duplicate checks, repudiation prevention, forensic identification, and others not yet conceived or applied are available.

Disclaimer

The National Biometric Security Project (NBSP) and the Biometric Technology Application Manual (BTAM) do not and cannot provide any legal advice nor is the BTAM a substitute for professional engineering design support. The information in this publication is for general information purposes only. None of the information contained in this manual, Volume 1 or Volume 2, is intended to be or should be relied upon as specific or definitive to the design of a particular program, or system, or process, or legal policy. The reader should obtain the advice of a suitably qualified engineer, attorney, or experienced practitioner before taking any action in the application and use of any of the information contained in this publication.
Updates and Errata

Finally, the reader is strongly encouraged to help make the BTAM a living and current tool by recommending changes and improvements in any area. All such recommendations will be carefully reviewed by NBSP Editors, and by an independent review Board constituted as required to address controversial proposals for change. Readers are encouraged to share their thoughts and impressions on the BTAM as well as any suggestions for content corrections, typos, or errors of omission. Please send feedback to:

National Biometric Security Project
Attention: BTAM Editor
17251 Melford Boulevard, Suite 104
Bowie, MD 20715
btam@nationalbiometric.org

Every effort has been made to contact copyright holders for content and images used in this manual. The publisher apologizes in advance for any unintentional omissions and will insert appropriate acknowledgements in subsequent editions of this publication when so advised.
ANALYSIS of Case Study Interviews

Interviews were conducted with the following organizations:

ATECH = Integration and implementation of a large scale Automated Passenger Clearance System (360 gates) and an Automated Vehicle Clearance System (42 lanes) at border control points for the Immigration Department of the Hong Kong SAR Government between 2004 and 2006.

BCHS = BayCare Health System is a nine-hospital health care system in the Tampa Bay, Florida area which implemented a vascular recognition biometric system (palm vein), in 2007 - 2008 to correctly, and privately, identify patients when they enter BayCare facilities.

CATSA = Canadian Air Transport Security Authority, created shortly after 9/11 as the government of Canada’s agency dedicated to aviation security.

PAMC = Parkview Adventist Medical Center is a 55 bed hospital in Brunswick, Maine serving the healthcare needs of the residents of mid coast Maine since 1959. Affiliated with the Seventh-day Adventist Church, Parkview is one of about 70 acute care Adventist hospitals in the United States. There are approximately 200 worldwide. PAMC implemented a fingerprint-based biometric system in 2006. The application was part of a larger project to develop a secure, paperless medical records system.

Pearson VUE = A leading provider of global computer-based testing solutions for clients in the information technology, licensure, certification, academic admissions, regulatory, and government testing service markets. They provide a full suite of services from test development to data management and deliver millions of tests a year primarily through a network of 5,000 test centers in 165 countries.

TCU = The Technology Credit Union provides financial services to end customers serving over 80,000 members with over $1.3 Billion in assets. Tech CU is among the top 1% of the nation’s credit unions with nine full service branches with close to 30,000 online banking users and about 10,000 bill pay users.

Union Pacific Railroad = Union Pacific Railroad, is North America's premier railroad franchise, covering 23 states across the western two-thirds of the United States. It is comprised of 32,000 route miles and employs 45,000 people at an annual payroll of $3.8 million. The railroad is the nation's largest hauler of chemicals, much of which originates along the Gulf Coast near Houston, Texas. Union Pacific is also one of the largest intermodal carriers – that is the transport of truck trailers and containers.

WCSD = Wood County School District is a public school system in West Virginia, whose main offices are in Parkersburg WV, with a total of 27 schools, grades K – 12. Their fingerprint-based biometric system was implemented to positively identify students
at the point of service in their cafeterias – approximately 1.8 million identifications annually.

As you read through the case study interviews you will notice that they attempt to elicit key pieces of information. These include:

- Factors Leading to Exploration of Biometrics as a Solution
- Formal Documentation of the Acceptability and Efficacy of Biometrics
- Making a Business Case or Assessing the Economic Impact of Biometrics
- Methodology for Selecting the Appropriate Modality (technology)
- User Resistance
- Evaluation of Providers (vendors)
- The Training Process
- Impact of New Biometric Applications.
- Installation, Integrators and Third Party Consultants
- Preparation of the User Community for Implementation
- Surprises Along the Way
- Lessons Learned – What Went Well?
- Lessons Learned – What Things Didn’t Go as Well as Planned?

We have culled the most relevant case study responses to these queries and summarized them below. While we encourage you to read all the case studies the response analysis may prompt you first go to a case study that is of particular interest.

**Factors Leading to Exploration of Biometrics as a Solution**

These were as varied as the individual applications, but all included such issues as improving through put rates, efficiency and security. Although the two medical applications, **BCHS** (BayCare Health Systems) and **PAMC** (Parkview Adventist Medical Center), varied widely both in scope and user base (patients in one and medical staff in the other), there were significant commonalities in motivation. Priority concerns for both were the security of patient information, and efficiency/productivity (of both staff and patient processing). A common motivator, or change agent was the introduction of an EMR (Electronic Medical Records) program. BCHS was also seeking a means to identify impaired or unconscious ER patients.

The two applications involving air transportation, The Hong Kong Immigration Office, referred to here as ATECH, and the Canadian Air Transport Security Authority or CATSA, were motivated by governments’ response to 9/11 specifying use of biometric technology, although Hong Kong expanded to include border control at places other than the airport. Another transportation company, Union Pacific Railroad had a significant history with respect to biometrics. Many years ago, they employed one of the first commercial voice recognition systems for managing the switches and related equipment in their rail yards.

Others factors included fraud avoidance in testing, banking and time-and-attendance; meeting government reimbursement requirements in school lunch programs; reducing billing errors; high cost of material and labor to replace manual card systems; high help-
desk costs in PIN-based systems; and getting a competitive edge over others in the financial industry.

**Formal Documentation of the Acceptability and Efficacy of Biometrics**

In the six applications where biometrics was not mandated by an outside entity, all documented the acceptability and efficacy of biometrics by presentations to management rather than written reports. Additionally, documentation was provided by records of SWOT (Strengths, Weaknesses, Opportunities, and Threats) assessments, formal testing of alternative solutions, reports of previous experience with biometrics in other applications within the organization, or formal vulnerability assessments and requirements analyses.

**Making a Business Case or Assessing the Economic Impact of Biometrics**

There was only one respondent (TCU) that conducted a cost/benefit analysis, which fit the organization’s business model. Most included some estimate of cost reduction in presentations. At least three did not justify the application on a financial basis.

**Methodology for Selecting the Appropriate Modality (technology)**

In our small sample of eight, four chose a fingerprint-based biometric, two chose vascular, one chose iris, and one chose both fingerprint and iris. The process ranged from a rigorous, formally documented series of criteria (Pearson VUE and ATECH), to selection based more on what the vendor could bring in the way of single sign-on than to the nature of the biometric (PAMC). In one case both the modality and vendor were chosen because of what they did not offer (WCSD). Union Pacific’s selection of iris was driven by the impact of difficult working conditions on the fingers and palms of their employees. Also, they were confident of the high accuracy and throughput of iris.

At one end of the spectrum, Pearson VUE established these selection criteria:
- Usability without extensive training
- High enrollment rates
- Low unit cost
- Acceptability (from a privacy perspective) to candidates, clients and regulators
- Form factor (small footprint, suitable for desktop use)
- Accuracy - low false rejection and false acceptance rates
- Global support on the part of the vendor

In the other cases, criteria were at least articulated to be:
- An adequate level of security
- Cost
- Efficiency
- Customer awareness

Some modalities were rejected because of issues such as excessive cost, stigma, non-universality of the biometric feature, unreliability, or un-proven nature of the technology.
A formalized requirements list was a feature of most of the major procurements, but not in the smaller and less formal ones.

Performance characteristics (False Match and False Non-match Rates) were central to the selection of the biometric in one case ATECH, but were only one of several requirements (and not the most important), in the other cases. “Adequate” seemed to be the guiding philosophy in most implementations.

Privacy policies and assessments were a part of most implementation although this issue had been addressed historically and adequate policies were already in place in most cases. No one reported a major problem with compliance.

User Resistance

This appeared to vary according to the context of the application. In a unionized industrial context (UBS/Union Pacific), it was vigorous and vocal, although not so much at the individual level as at the union level. In most other cases, it was accepted well, particularly if it solved some of the users concerns such as smoothing and expediting their entry or access. Many of the implementers were farsighted enough to anticipate resistance and be pro-active in development of alternatives in the event that individuals wished to opt-out of the biometric system.

In large implementations, selling the application to management and key players (physicians in a hospital context, and school boards and administrators in an educational context), made implementations much easier. In almost every case, rank & file adapted and ultimately welcomed the added convenience & other benefits.

Evaluation of Providers (vendors)

The methodology varied widely depending on the size of the implementation, resources of the implementer, and experience. In the case of the Hong Kong border control system, the prime contractor, selected for the job (ATECH), evaluated vendors in-house based on criteria approved by the Hong Kong government: 1) technical characteristics, 2) compatibility with other parts of the system, 3) maintainability, and 4) costs. CATSA used a formal competitive bidding process for both the biometric vendor and the overall system integrator.

Pearson VUE engaged International Biometric Group (IBG) to provide technical development services as well as consulting services including requirements definition, system design, and solution integration support. They then conducted an in-depth evaluation of the technology itself and the vendors offering such products in conjunction with IBG and selected the vendor.

The one financial institution (TCU), also hired an outside consultant to help with the selection process by testing the various vendor’s technologies and claims. They then made their selection based on the robustness of the technology, the vendor’s previous experience with AFIS systems, and the speed at which it could be integrated with their banking system, and total cost.
In two cases (BCHS and WCSD), where there was only one vendor who could satisfy the end-user’s needs, there was no competitive selection process. It is interesting to note that all implementers but one, used some form of outside assistance to augment their in-house efforts or expertise at some point in the implementation process.

The Training Process
It’s nearly a tradition in the industry for vendors to train client personnel to train users. Beyond that fundamental, there are many nuances. One respondent (BCHS), had (and has) a full time staff of 5 trainers who provided 1.5 hours of training to each user, and remained on-site for 3 days, 24 x 7 for any assistance needed. Others in smaller operations trained a few staff members to provide training of significantly less time to users. Another (PAMC) used nursing staff prior experience with biometrics to leverage a larger training and cleverly tantalized trainees into formal sessions. Others train customers during the initial enrollment.

Impact of New Biometric Applications.
Operational impact
Security has been improved by satisfying the high security requirements passenger verification, and providing a vehicle to insure that security clearances are not granted under multiple identities. The era of card sharing has been ended throughout the air transport system in one North American country. There has been a reduction in various types of test-related fraud and malfeasance, including the use of impersonators (also known as ‘proxies’) and other misrepresentations of identity. Fraudulent bank transactions have been reduced as has the opportunity for fraud by the visibility of the authentication devices.

Authentication time has been reduced from the 1 minute it took to compare imaged signature cards to an average of 3-5 seconds using the biometric system. Both teller and member transaction times have been reduced.

Through put rates have improved and biometric reliability assures high availability 24 x 7 with minimum maintenance. In some instances, the small footprint of biometric equipment and a move away from manual systems & operations has provided more room and increased processing capability.

Patients, school children and customers are identified more quickly and accurately and retrieval of medical histories and other information provides better and swifter treatment. In some applications, the need for physicians and staff to memorize multiple passwords has been reduced or eliminated and login/logout has become easier and more convenient resulting in a more efficient work force.
Financial impact
Redeployment/reduction of staff (hence operating costs), has been possible, and helpdesk costs have been reduced. Reduced IT support costs and resource requirements have been noted. The expense of printing cards at the beginning of the school year has been eliminated, as has the cost of the special cartridges to produce the cards.

Other
By deploying a biometric authentication solution, implementers distinguish themselves from others by demonstrating to clientele that they are priority when it comes to protecting their financial assets and ensuring fast service when they visit.

Installation, Integrators and Third Party Consultants
Of the eight interviewees, seven used outside assistance in all or portions of their implementation.

Preparation of the User Community for Implementation
In general, the more thought and effort that went into preparing the users, and related community for implementation, the better the results.

Insightful implementers focused on selling the system to management and influential groups of the user base by presentations to senior management, staff physicians, school boards and the like. Some put the new systems in the context of being a solution to the needs of the user community and reducing processing time at border control stations; eliminating passwords, PINs and log-on/log-off; better protecting the assets of customers – including personal information; and protecting against identity theft.

Anticipating possible parental concerns, the Wood County School district communicated extensively with parents before implementation, and provided opt-out provisions for those who chose not to let their children participate. All provided written as well as verbal information to the user community, although in at least one case they concluded that a face-to-face encounter was by far the most effective method.

Surprises Along the Way
These varied widely according to the particular implementation. Of the commonalities among the eight respondents, they were all positive, and included how well installations went and how positively the implementations were accepted.

Lessons Learned – What Went Well?
In general, most respondents reported that the most fundamental outcome of all – the project was completed according to plan: on time and within budget, went well. Many reported the installation phase went well, and the implementation was well accepted by the community. BCHS reported that one year after their first site visit, 24 facilities across three counties were up and running. Pearson VUE reported that a phased approach, including a pilot test and anticipated tweaks of procedures and technology made for a successful implementation, including additional modular capabilities such as 1:N capabilities. Another (WCSD) felt that the presentation of a business case and
selling a project to management went very well. Most felt training and enrollment went well, and some felt the same about follow up and problem resolution.

Managing change and expectations was cited numerous times as a critically important issue in implementation. In some installations biometrics might not always speed the process (whatever that may be). Management should be educated to expect that, and the other positive benefits such as greater security, accuracy, reimbursement, etc. should be emphasized as important goals, not just speed. Likewise, it should be clear that workarounds need to be provided for that percentage of the user population that have difficulty with or can’t use the biometric. A quote from WCSD conveys the idea, “I temper my expectations with my knowledge about the evolution of child-focused biometrics. It is an evolving process and every reader gets better with improvements on a yearly basis. So, is it the top-of-the-line, 100% perfect? No, because I am always reaching and stretching and they [vendors], are as well.”

Biometric implementations promote ancillary benefits as another partial quote from PAMC illustrates: “Although Parkview initially invested in finger biometrics to solve its password problems and strengthen IT security, the technology has provided additional benefits, for the process, called “bedside medication verification,” which greatly reduces medication errors and ensures patient safety. Parkview now barcodes and scans every medication that enters the hospital and each patient is also identified by a barcode on their wristband. Scanning tells the nurse if the medication being administered was ordered for that patient and is being given at the right time”.

Customers (particularly in the financial industry), were impressed and pleased with the institution for employing the latest technology in an effort to further protect their assets and identity.

**Lessons Learned – What Things Didn’t Go as Well as Planned?**

Among the many lessons learned (some of which we are sure were not shared with NBSP), some stand out.

Equipment failed to live up to expectations in a number of cases. In the Hong Kong border system the autogate vendor had to be replaced during the project, principally because the fingerprint readers did not meet performance requirements of 99.8% effectiveness. In the TCU implementation, a concise quote highlights the equipment issue and offers some advice: “The hardware scanners we initially deployed went bad quickly due to low Electro Static Discharge ratings and had to be frequently replaced. Since the software solution we deployed was an open solution, we did not have any problem to switch to another hardware vendor’s scanners. The key lesson here is to always make sure you are not locked into a proprietary system and you work with a vendor that provides an open system which gives you the flexibility to switch hardware vendors so you don’t have to re-enroll your customers.”

In another installation, fingerprint readers were installed on a vertical surface in a way that was not effective from an ergonomic perspective and trial-and-error tests were required to identify optimum installation given the very diverse demographics of users.
Tunnel vision is always a threat and at least one responded that their focus on enrollment detracted from their monitoring of the authentication process as users began to use the system. In hindsight they would have enrolled their most active facility (the one with the greatest volume of authentications) first, and made sure that users were having success in authenticating. In a similar vein, a respondent told us that the training was given, but there was no validation that the training was aimed at the correct issues and was, in fact, adequate.

Formal after-action analyses seemed not to be the rule, with only two (Hong Kong/ATECH, and TCU) being reported.

Case Studies
Interviews were conducted with personnel associated with six of the eight companies whose case studies are featured here. Written responses to the interview questions were received from the other two companies. In most cases the interviews were with company employees. In some, they were the integrators and device manufacturers who were speaking on behalf of the user company (with the user company’s permission. NBSP interviewers were Russ Ryan, Vice President, Marketing and Jerry Williams, consultant to NBSP.

**Hong Kong Immigration System:**

The following is a composite of responses to NBSP’s written questions, a Biometrics 2008 conference presentation by Mr. Otto Poon BBS, OBE, CEng, and a telephone interview with NBSP in August of 2009. Mr. Poon represented ATAL Technologies Ltd. of Hong Kong, referred to below as ATECH

**NBSP:** Before we discuss details of the application, perhaps, you would spend a few minutes describing your industry and your company’s position within the industry.

**ATECH:** Hong Kong has a land mass of approximately 1000 square kilometers with a population of about 7 million people so it is one of the most densely populated areas in the world. Before China opened up, the main flow of traffic was from the air and the airport was the main transport hub. In the last 10 – 15 years there has been a great increase of land-based traffic. This has been a combination of Hong Kong citizens working in mainland China and goods traffic between China and Hong Kong. It has been reported that in the Pearl River Delta there are 80,000 factories owned by Hong Kong Business people employing 10,000,000 people. So you can look at Hong Kong as part of the Pearl River Delta. At the present time, the Hong Kong immigration offices have to process a total of 220 million passengers every year, 50 million of whom pass through the airport. So you can see the amount of traffic between Hong Kong and China and the rest of the world.

In 2004, the Hong Kong government, because of the rising traffic, decided they needed to automate their system of controlling passenger and vehicle traffic between Hong Kong and the mainland. They approached a number of device manufacturers who expressed interest in providing such a system, and after an international competitive bidding process. ATAL Technologies Limited (ATECH), a provider of integration services for technology applications in the field of border crossing clearance, access controls, and identity management was awarded the contract. ATECH is a subsidiary of the Analogue Group of Companies whose core business is in electrical and mechanical engineering.

The contract required ATECH to design, integrate and implement a large scale Automated Passenger Clearance System (360 autogates) and an Automated Vehicle Clearance System (42 lanes) at border control points for the Immigration Department of the Hong Kong SAR Government between 2004 and 2006. To our knowledge this was the first in the world of this scale and we still provide 24x7 on-going support, upgrade and maintenance to these systems today.
NBSP: Given that as background, what led you to research biometrics in respect to your business? Were you trying to solve a business problem or trying to capitalize on a business opportunity? Were there economic, security, or competitive factors that may have spurred the investigation of biometrics?

ATECH: ATECH applied our biometrics expertise according to the customer’s requirements as specified in the contract. The Automated Passenger and Vehicle Systems were initiated by the Hong Kong Government to improve the throughput rates, efficiency and security at border control points.

NBSP: Can you describe the pre-acquisition process for us...i.e.: did you undertake a risk/vulnerability assessment...and if yes, can you describe how it was done and what the results were...obviously, without giving up proprietary information?

ATECH: The Hong Kong Government had conducted a feasibility study before going ahead with the project, the bidding process and award of the contract.

NBSP: Can you provide more detail on the scale of the feasibility study...i.e.: what was evaluated?

ATECH: I think at the feasibility study phase, the Hong Kong Immigration Department consulted a number of potential vendors, we being one of the four. The government tried to get technical information and performance projections from different vendors, and we worked closely with the government at that stage when they were preparing the tender document. And then, once the tender document had been released and when they’re competing for a job, then the dialogues substantially stopped, because it was at the tender stage; it could be sensitive; it could be seen as favoring one particular vendor. I think that was how the feasibility study was done.

NBSP: Did the vulnerability assessment help you define your program requirements? Operational? Functional? Legal? Business/economic?

ATECH: The Hong Kong Government had considered these factors in their feasibility study. Their operational requirements were that in passenger handling capacity each eChannel (entry/exit Channel) had to be scalable up to 5,000 passengers per Channel per day; vehicle clearances scalable up to 3,000 per lane per day; and the system had to be designed to handle 7 million passengers per day and be scalable beyond that. Additionally, so you have an appreciation for the scope of the project beyond just statistics, it had to operate and meet those performance parameters in the following areas: Environment varies from extremes of heavy rain to very sunny with humidity in the summer of 95% with illumination variable.

Demographics of the operation vary from very young to very old, both groups encountering degrees of difficulty in concentration and dexterity; all ethnicities and races with many Asians and westerners; and cultural differences as well.
Security and safety were fundamental concerns, so provisions had to be made for liveness tests to enhance security, CCTV monitoring (one camera for every six eChannels), reliable detection systems to prevent tailgating and intrusions, gate door safety interlocks, referral lights to summon immigration officers, and local and central emergency capabilities.

NBSP: Were legal considerations—forgive me for not being as familiar as I should be with law in Hong Kong—but in the US and some of the Western countries, legal considerations such as privacy become sometimes an issue in biometrics. Did that occur in this application?

ATECH: That’s very much an issue. And that issue has gone through our legislature in an extensive debate as to how information, can be protected. I think Hong Kong has about seven million people, and everyone of us has an ID card. When we register our ID card, that information that biometric and other personal information was kept in a vault more safe than the Fort Knox.

NBSP: Fort Knox?

ATECH: Yes, I think it is highly secured. Actually, people were surprised how this data was kept so, so secure. I think it is like a vault of a central bank, and anyone—I mean anyone, even the Director of the Immigration Department — who is the highest officer in Hong Kong looking after IDs and immigration letter -- has to go through a number of procedures such as, you have to use the key pad to get into the lobby. Then after that, you will go into a second chamber with the Director of Immigration, and his deputies, two of them go through both iris and fingerprint biometrics to verify if these two persons are responsible officers. Only after that they can access to the database. As far as I can understand, no false access has ever occurred made since database was established.

NBSP: When you speak of the ID card that you carry in Hong Kong, are you saying that their biometrics included in that card?

ATECH: Yes, biometrics are included - facial and fingerprints.

NBSP: Facial and fingerprint? So then, the population of Hong Kong is obviously very familiar with biometrics.

ATECH: Oh, yes. I think the Hong Kong government has done (and we helped them to do this), a very good promotion exercise on this. We have a number of gates at different crossing points at the airport, at the marine crossing points, the land crossing points. The database was only kept in a central location, what I called Fort Knox. Whenever someone puts in the ID card to go through the gate, the data will have to send a request to the database and ask them to send the biometric to the gate. That takes a couple of seconds. Those databases are not installed at the closing points for security reasons.
NBSP: Okay, so help me understand. Each of the citizens of Hong Kong has an ID card, and the ID card has a facial and a fingerprint biometric imbedded in that, and that’s the card that they use at both the border crossings and at the airport?

ATECH: Yes.

NBSP: All right, so they had this card prior to this application being developed?

ATECH: Oh, yes. I think everything was planned before. Every person in Hong Kong was required by law to get a new ID card—I think about five years ago—and those ID cards—people understand those ID cards—will have their biometric on the card, embedded into the card.

NBSP: So this particular application at the airport and the border crossings was really designed to accommodate the ID cards that had already been distributed to the population.

ATECH: That’s right, but more than that. The gates have been enhanced to read ePassports. Any passport that has embedded biometrics, and when someone, say a frequent flyer into Hong Kong, registers with the Hong Kong government, then they can walk through [using the ePassport] just like an ID card.

NBSP: The application will accept registered ePassports as well as Hong Kong ID cards?

ATECH: That’s correct.

NBSP: Had you focused on biometrics as a solution from the beginning or were other technologies investigated...i.e.: did you evaluate the strengths/weaknesses of solutions other than biometrics?

ATECH: The Hong Kong Government had focused on biometrics as a solution from the beginning.

NBSP: I’m assuming that this was because of Hong Kong’s prior experience with biometrics in that their national ID cards already contained biometrics.

ATECH: The Hong Kong government has worked together with two or three universities in Hong Kong to investigate the feasibility of a security system which can automatically process people at the airport and at the crossing points … that must be a standard. We started about probably ten years ago. After looking at different options, I think the iris, the fingerprint, the facial, that sort of thing. Eventually, I think the government has come to conclusion in terms of level of security, in terms of the cost and in terms of efficiency of the system or the processing time. The government finalized on fingerprint as a choice. I think it has gone through not government only, but they have gone through with the universities, because a couple of universities have been doing a research on iris and others on fingerprint. One of the university professors is a world-recognized biometric expert, and the government is getting advice from them.
If you did evaluate the strengths/weaknesses of solutions other than biometrics what led you to decide on biometrics?

The Hong Kong Government specified biometric technology and we concurred that it was the most appropriate technology at that time.

Can you describe the selection process you went through to determine which modality (finger, face, iris, etc) was the best for your application?

The choice on applying fingerprint was made in the 2002-2003 time frame. At that time fingerprint technology appeared to be the most mature and most economical technology choice.

Once you settled on a modality how did you evaluate potential providers? i.e.: was it an internal evaluation or did you bring on a third party to help? In either case, can you describe the process you went through?

We searched through internet and/or local contacts and did the evaluation internally. We selected based on the technical characteristics, compatibility with other parts of the system, maintainability, and costs. Overall, for our purposes on this particular application, Lumidigm fit the fingerprint requirements best.

Let’s discuss potential quantifiable and non-quantifiable benefits of your application solution. What would you say were the quantifiable benefits to your business i.e.: cost savings, reduced risk of fraud, operational costs etc.?

Increased throughput rate and redeployment/reduction of staff (hence operating costs). In the old manual system one immigration officer was required for each entry/exit channel (eChannel), and with the new biometric-based system, one officer can monitor and control six echannels. In the last three years, the Hong Kong Government because of budget constraints has been under pressure to downsize, and this system has contributed much to the reduction of employees of Immigration Department of Hong Kong. It satisfies the high security requirements of passenger verification. The system has high availability and works 24 x 7 with minimum maintenance. In addition, the space required for eChannels is less, so the lanes can be narrower and we can put eight lanes in the same area that could only accommodate six lanes, thus increasing the capacity of our control points.

How about non-quantifiable benefits that you realized i.e.: added ease or convenience for your customers and/or employees? Or a heightened sense of identity protection?

The public can enjoy more convenience and privacy because of the use of the automated process. There’s also an improved image of using hi-technology at Hong Kong border.
NBSP: How was the installation process handled? Did you use an integrator or other third party consultant?

ATECH: We were the prime contractor to integrate and implement the system so we had the expertise in-house if you will. We knew that detailed planning was the key to a smooth implementation so we emphasized that before installation. It was also critical that current operations were not affected before, during, or after installation, so a great deal of coordination with operational units was carried out to ensure problems were addressed before installation commenced. We also developed and coordinated contingency, fallback and work-around procedures to ensure there was no disturbance to current operation.

NBSP: How did you prepare those who would be using the system for the application?

ATECH: Use of biometrics had been well accepted by the public of Hong Kong. Additionally the Immigration Office emphasized the increased convenience of the automated system: previously passing through customs manually averaged about three minutes, and with the automated system there should be no more than three persons in the queue at any time with a maximum acceptable processing time of 10 seconds each (in practice, it actually averages 6 – 7 seconds. So a 30 second processing time (and in practice, usually significantly less), was a vast improvement. And despite a propensity for bad press on anything new like this, there has been nothing but praise. We feel very satisfied that we have managed and met the expectations of both the client and the public.

NBSP: Can you subjectively assess how the application has benefited your organization operationally, financially, or competitively?

ATECH: It was not a financially rewarding project, initially, but because we shall maintain the system for 10 years, it will generate recurring income. It certainly showed that a professional, well thought-out program could result in deployment of a high tech solution to moving millions of passengers and cargo through borders in a safe, convenient and secure manner. The Hong Kong Government can be proud of this implementation, and frankly, it elevated ATAL to be a key player in this field.

NBSP: Were there any surprises along the way, and can you elaborate on how you dealt with the issues?

ATECH: The APVCS system called for high degree of reliability (99.8%) which could be delivered by individual components but initially not as a system. Hence, we had to have extensive discussions with component manufacturers to improve on the reliability of the components. We eventually achieved performance that satisfied the Immigration Department of Hong Kong and the community in general.

NBSP: Let’s discuss some of the lessons you learned from this experience and what you would pass on to others who are contemplating biometrics in their business. What aspects of the project went well?
ATECH: The most fundamental of all … the project was completed according to plan. We also thought the installation phase of the program went well even though there were some tough times during the middle of the project.

There were a series of national and international awards to the project including 1) the Hong Kong Information and Communication Technology (ICT) eGovernment Grand Award, 2) the Hong Kong Information and Communication Technology (ICT) eGovernment (Most Popular ePublic Service) Gold Award, 3) APICTA (Macau) Top prize in the category of eGovernment and services, and 4) the Hong Kong Occupational Safety and Health, Safety Technological Achievement Award - Immigration Department and ATAL Technologies Ltd.

The most rewarding is truly the acceptance of the community. As I travel through the Hong Kong border system or airport, I ask the people sitting next to me, or immigration officers I encounter, how they feel about the system and they universally are enthusiastic supporters of it.

NBSP: What aspects of the problem did not go well?

ATECH: Change of vendor (autogate) at the middle of the project.

NBSP: Can you elaborate on this a bit?

ATECH: Yes, I think the government demanded a really high reliability of the system. They are demanding a 99.8% success rate. When we were designing the system, we talked to component suppliers like card readers, like fingerprint scanners, and a number of other components. Each one of the suppliers of all these components told us that yes they can do 100%; they can do a 99.9% or whatever, which is true at the component level. But when you put 99.9 together with another 99.9 going down ten times, you are probably down to 98%. The error compounds and during the development stage and during the early implementation stage we cannot deliver the level of success, or the reliability of the system is not as high as what the Immigration Department would like to see. So we had to go back to vendors and talk to them, and some of them enhanced on their performance. Other says I can’t, that’s the limit, that’s the best we can do. Actually one or two vendors, they over claim on their performance, so they are not delivering us a 99.9; they are delivering us only 99% sort of performance. So at that stage, we have to search for other alternative suppliers of higher quality, higher reliability, and higher performance than had been taking place. And that’s a very painful process because quite often we have to change the mechanical mounting, the design of the gate, and also the interface and the software. Anyway, we secured a contract in April, and we got the first rollout in December in the same year by putting in millions of man-hours. I mean it was very painful to look in hindsight.

NBSP: Can you give us an example of what components you had a problem with on the autogate?
ATECH: Well, the fingerprint reader for one. It was one of those components that did not perform as well as we would like to see them perform. So eventually we changed them to Lumidign. There were a number of devices in the system which we tested. Some of the vendors enhanced their performance, some did not and that’s when where we had to change vendors.

NBSP: Was a formal “after-action” analysis performed to identify lessons learned?

ATECH: Yes, there was a post-implementation review.

NBSP: Can you describe the process for us...and were any changes to your application made as a result.

ATECH: We implemented a few enhancements to improve the application in terms of speed of operation and user friendliness.

NBSP: Can you elaborate on the enhancements made?

ATECH: Yes, I think anyway, my previous answer is part of this answer. But more than that, I think we’re also looking at ergonomics of the gate. For example, just take the case of the fingerprint scanner. I think how or where to locate this fingerprint scanner, and the angle of the inclination, and the position relative to the entrance of the gate, all these affects the user friendliness of the gate. I think we made a few changes on that sort of thing. I mean, it’s not the system change, but it’s just making the use of the reader more ergonomic.

NBSP: In other words, if you put the reader too flat, people approaching can’t see where to place their finger. If you put it on a wall, sometimes it’s too high for people to reach up and touch?

ATECH: I mean, assuming that the fingerprint scanner is mounted totally vertical, people will have difficulty in putting finger on a vertical surface. But the angle itself is also another issue — you know it’s the trial and error thing.

NBSP: Earlier in the interview questions, we talked about some of the benefits of the application, and your response was, from a financial standpoint, it was not initially a financially rewarding project. But as you will maintain the system for ten years, it will be. That’s from your perspective as the provider. From the Hong Kong government’s perspective, were they looking for a system that would provide them with a reduction in financial cost? Or were they looking more for enhanced security?

ATECH: I think the answer is that security must be the top priority, number one. There’s no question about it. I think when the government wants to push this system through our legislative council, like your House or Senate, the government receives a lot of questions on personal security, privacy, and all sorts of things before the legislative council will give the government the money to build the system. So it went through, probably, six months of intensive questioning and debate between the legislature and the
government to get the funding approved. Most of the discussion was centered on security and the reliability of the system. I think that’s it from a government’s perspective. All government projects go to open tender, so they cannot negotiate on this one particular supplier, and when the government, after talking to the vendors, finalized the specification, we have to submit a technically and financially complying proposal. But there were four companies bidding for it, for the contract on this system. The three others are multinationals, and we are the only Hong Kong local company before this job. I think the government evaluated the tender based on the two-envelop tender system. The first envelope is on technical performance. After they selected on paper the best performing system, we have to do a prototype to demonstrate to the government that we can deliver what we sent in our submission. After they’re satisfied with that, then they’ll open the second envelope, which is the price sheet. It’s the most competitive of these two combined that matters to get the job.

NBSP: How long has this system been in operation?

ATED: Oh, I think it is 2004.

NBSP: How would the Hong Kong government, if someone were to ask them, what are the benefits of this system versus what you had before. How would they define the success of the system?

ATED: I think that any automatic system or automated system will eliminate any abuse from the individuals. The immigration officer, he has a friend, he want to get him through in the old system, he can always get him through. But in here, the system does not know anybody. If the biometric is incorrect, he will not be allowed to enter, number one. Number two, in terms of efficiency, I think previously we have those immigration booths, and what work can happen for four immigration or four men in booths, we can put in six gates. So that will help to increase the number of channels that people can walk through. Number three, is that the time is faster. Then fourthly, it’s safe. A lot of men—officers—we don’t need that number of officers to man the entrance point.

So financially, economically the government benefited; the community benefited. More than that, I think sometimes people can be sentimental. When the immigration officer questioned somebody, it’s always people do not feel well. They say, you know, I’m being insulted; you don’t respect me as an individual, that feeling. But for machine, the machine is neutral. They treat whether President Clinton or anybody the same. So actually, the system is extremely well received in Hong Kong by the community as a whole.

NBSP: Let me ask you one last question. You had mentioned earlier that you have the responsibility or the contract for maintaining the system for ten years. Are you, and/or the Hong Kong government looking at any enhancements to the system?

ATED: It is always unknown. I think our government is already looking at the next generation of systems which probably we need to implement in ten, five years time from
now, that’s number one. Number two is that, I think if the government, the people, we, ourselves identify new devices that can work faster, better, more accurate, I think we can always make a proposal to the government for them to make a change, of course at a cost.

**NBSP:** Then - and I know I said one last question probably three times, but here’s one more. If a representative from another country, whether it be Kuala Lumpur or Japan or what have you, were to come to you and say, “We have been approached by the government to implement a system similar to yours.” What kind of advice would you give them in terms of what was the most difficult aspect of all process that you had to deal with that you would try to explain to somebody else who is asking you for some advice?

**ATECH:** I think based on my experience, managing the expectation from the government and from the community is the most difficult part.

**NBSP:** Managing customer expectations?

**ATECH:** Yes, for example, the biometric and fingerprint reader, I think some people have very fine fingerprints that will never work on the system. They have very dry fingers you know that sort of thing, and again we have to provide a sort of a little device to wet their finger a little bit before they use the gate. So I think initially, we have people manning the gates and tell the people how to use it, and I think it’s all to do with telling the people how the system works, how to use it, and if there’s any, if they can get to explain to them what they need to do, I think now after four or five years, people will accept it quite readily because people do use that to go to China. Between Hong Kong and the mainland China, everyday we have about half a million people go through, so on the average, every citizen of Hong Kong use it probably three or four times a year. So after this once or twice, they know what to do and they accept it readily.

**NBSP:** Mr. Poon, I know you are a very, very busy man, and I know we’ve gone round and round on this for a while. So I really do appreciate the time that you afforded us.

---

**Union Pacific Railroad:**

The following is a transcription of NBSP’s interview with Mr. Andre Johnson of Universal Biometric Systems and Tim Meyerhoff, Director, North American Sales, LG
Iris. Universal Biometric Systems was the integrator responsible for the deployment of Union Pacific Railroad’s LG Iris-based time and attendance system.

**NBSP:** Good morning. This is Jerry Williams.

**Andre Johnson:** Hi, this is Andre Johnson from Universal Biometric Systems.

**NBSP:** I think Tim just joined us.

**Tim Myer:** Yes, I did.

**NBSP:** Okay, glad to have you on board. Before we discuss the details of the application, perhaps you’ll take a few minutes describing the industry that Union Pacific is in and Union Pacific position within that industry.

**Andre Johnson:** I’ll give a little bit history about Union Pacific.

**NBSP:** Okay.

**Andre Johnson:** Union Pacific is a railroad. It’s one of the largest railroads in the United States and the application we presented to them was the time usage or time and attendance application -- basically a time clock for their remote employees. The employees are moving throughout the United States working on the road tracks. They are called a gang and Union Pacific had a need to get a better handle on who’s on site, and how long they’re there. That was the initial reason they needed this. That is also a part of a larger process then that their implementing within the company.

**NBSP:** Okay. Given that as a background, what got them to research biometrics for a solution?

**Tim Myer:** Well, they considered a variety of biometrics to automate their work gang time and attendance record keeping, and they were primarily concerned with eliminating worker fraud and leveraging their investment in workforce optimization. They ruled out fingerprints and hand based biometrics due to both union concerns and environmental and work condition issues. Work conditions in the field can alter a laborer’s biometric identity to some extent and/or prevent him from being identified. For example, fingerprint, when you have a laborer workforce, sometimes presents a lot of challenges with respect to getting a good image because they’re dirty or oily. There are a number of different reasons that a contact biometric doesn’t work well for that type of environment, so they wanted a non-contact biometric. Also, Union Pacific does have a significant history with respect to biometrics. Many years ago, they employed one of the first commercial voice recognition systems for managing the switches and related equipment in their rail yards. So, there’s the thumbnail summary of the Union Pacific position.

**NBSP:** All right.
Jerry Williams: Did Union Pacific create or provide you with any sort of documentation about any risk or vulnerability assessment or some people call it a feasibility assessment or did they just come to you and say, “Here’s what we want to do and here’s the reasons,” and that’s it.

Andre Johnson: Oh, it was the latter. They knew they needed a biometric solution for the process that they were creating. They didn’t give us any sort of documentation on the full process, just our part. One of the things that—and, you know, we did actually go up against fingerprint and hand geometry biometrics, and we won out for several reasons; those that Tim mentioned. But also, the speed of the search engines of fingerprints was slower than iris and it (the fingerprint reader) required physical touching and a PIN. Union Pacific also had some sanitary and safety concerns. Those two issues sold the system to Union Pacific management.

NBSP: Okay. Andre, I thought you almost implied that there was some kind of a formal, I don’t want to say formal competition, but you said, “We went up against fingerprints in other modalities.”

Andre Johnson: Yes, we did. Yeah, they invited several companies in to demonstrate their biometric technologies. In fact, these were companies that had biometric front-ends to their time and attendance packages, but we went out without a time-and-attendance software because ours was actually plug and play. But what, overall, won the day was the sanitary issue and the speed of the search engines for the iris.

NBSP: And lack of a PIN and non-contact of course.

Andre Johnson: Exactly. Yes.

Tim Myer: Jerry, the other thing, you know, I visited—where did I come, Andre? That was Kansas City?

Andre Johnson: Kansas City, yeah.

Tim Myer: The way that they did, attendance was, you know, imagine like 150 guys standing out there in the fields, doing roll call—

Andre Johnson: In the dark.

Tim Myer: Yeah, in the dark too, that’s right, and they’re calling out peoples’ names and then you just hear, “Here,” from somewhere in the crowd. It was pretty loose with respect to identification for your punch in process. Really, anybody’s voice could be saying, “Here.” So, that was something that they really wanted to eliminate.

Andre Johnson: In fact, as a surprise we did the roll call and the iris capture twice and we actually found eight people that were not there.
Tim Myer: You found eight?

Andre Johnson: Yeah. Well, there were people calling out for other guys, so we did find those guys immediately.

NBSP: Was that part of the pre-project competition?

Andre Johnson: No, no. The competition had already been won.

NBSP: Okay.

Andre Johnson: And we were demonstrating the software for their largest railroad gang for the first time and they were really surprised by the speed of the iris matching. The gang didn’t know we were going to do that and some of them had people who were going to punch in for them. Well, we did find that people who were actually buddy punching...and they weren’t too happy about that.

NBSP: Oh, boy.

Tim Myer: And some of that trial Jerry, was to validate the usability of the technology in the fields.

NBSP: Okay.

Tim Myer: Once you get people to used to the system it doesn’t take long for someone to become habituated with a particular sensor once you expose them to it and provide a little bit of education. This is how it works, you know. Look into the mirror and wait until you hear the shutter click from the camera.

NBSP: Okay.

Tim Myer: It’s a relatively simple process but you’ve got a large group of people that have no idea. What we saw on that particular evaluation day and we see regularly in other deployments is that with the LG Iris imager platform it takes only a minute of training, to habituate a person with that device, that sensor. “Just look here and wait for the shutter click because the imager will give you an audio prompt that says, ‘Please move back,’ or ‘please come closer to the camera.’ ”

NBSP: Okay.

Tim Myer: And we noticed that the enrollment speed—well, enrollment speed and recognition speed are basically the same give or take a few seconds for iris recognition, particularly with the imager that they use in that deployment. It’s very easy to use.

Tim Myer: Yeah, Andre, do you have any data on throughput like how many recognitions per minute or per hour when you utilize this.
Andre Johnson: Yeah, I have logs back at work where the guys were coming in behind each other like I can give numbers from that.

NBSP: That would be great.

Andre Johnson: For example, we were beta testing the equipment one time in Kansas City and we had poor power...it would come on and off. We were using two cameras, but there’s chaos because of the power situation, and these guys are new to the system, but we had 150 some guys, a little extra over 150 guys, but we got them all in that chaos through in 11 minutes.

Tim Myer: Really?

Andre Johnson: Yes.

NBSP: Okay. Can we discuss potential quantifiable and non-quantifiable benefits of the application and I’ll ask you first, what would you say would quantifiable benefits to Union Pacific?

Tim Myer: Well, first off, they get the guys logged in a lot faster than taking roll call, so there’s labor savings. Productivity goes up because they’re not taking the 45 minutes it took to do the roll call previously. With the new system they could cut a half hour off the previous time. So now the gang is working 30 minutes more during the course of the day, so that’s ROI right there, you know, higher productivity.

Andre Johnson: I also have instant recording backup to the home office. There are reports of who’s on what site.

NBSP: Okay.

Andre Johnson: And, as said earlier, there is no more buddy punching, so that’s an immediate benefit as well.

NBSP: So, what would you say are some of the non-quantifiable benefits? Any ancillary things such as fraud avoidance?

Andre Johnson: I was going to mention that. The employees will most likely come in because of the new systems. So, they can’t defraud now.

Tim Myer: Then you have the benefit that now this attendance report is generated automatically, so accuracy goes up and the amount of time that it takes someone to manually record the results of the roll call. You’re saving labor there as well.

NBSP: Yes.
Andre Johnson: The union has timekeepers that kept track of all the stuff we’re mentioning, and there was a lot of concern that the new system would put the timekeepers out of a job, although, it didn’t. They were given the responsibility to keep the system going. It was an efficient way of handling it.

NBSP: Great. How was the installation process handled? And maybe installation isn’t the right term because it looks like you didn’t really install stuff but you created mobile units or something?

Andre Johnson: Exactly. It was expected that we would go out to each one of their gangs throughout the country. We would just travel and implement the whole thing, do an enrollment process and then do a some training. Well, after the very first one, they realized that this was something that it was easy enough for them to do themselves. It was that easy to implement. So, yeah, implementation now is just shipping the hardware and software to them.

NBSP: Okay.

Tim Myer: And that’s a laptop configured in a case with an eye cam that’s like a durable case, I’m not sure what’s exactly your shipping right now, Andre, but—

Andre Johnson: It’s the little hard egg or most people know them as pelican cases but just a hard plastic case that holds the camera. In fact, the size of the case has changed because, in Union Pacific’s case, they weren’t actually carrying the laptops in the cases. They were always outside because it is use for other things.

Tim Myer: Oh, okay.

NBSP: Okay. Kind of touching on the similar subject, how did Union Pacific prepare their employees, those that’d be using the system, for the application?

Andre Johnson: They actually have management go around the country doing town hall meetings with the gangs, and they explain what is coming down the line. They were just getting prepared that way. And, of course, we did the administration for the management to show them how easy it was, and we had a lot of discussions with the unions.

Tim Myer: There’s another thing that helped Union Pacific a little bit with personnel concerns is that they already had a policy for biometric use. They indicated that when they deployed the voice recognition system for the railcar release program it sort of put a stake in the ground with respect to policy for the use of biometrics within the organization.

NBSP: It sounds like you’re saying they already had an adequate privacy policy in place.

Tim Myer: Yes.
**NBSP:** Was there any reaction by the people enrolling in this system? How did they initially react to the idea of having a biometric taken and being identified that way, I guess on a personal level?

**Andre Johnson:** I talked to a few of the guys and they didn’t know that I was the one implementing this application. They didn’t have a problem with the technology, it created the perception that management didn’t trust them. That was their beef.

**Tim Myer:** That’s what they’re saying.

**Andre Johnson:** But as far as them getting up to the technology, there were no problems at all, you know. They didn’t know who I was and I’d listen to them talk. In fact, a few weeks ago, made a new release and we’re on site with some guys who were new to the system. And I actually heard one guy say: “What is this phone doing?” Another replies: “It’s taken the picture of your irises. That’s how we’re going to do time cards now.” The first guy just says, “Okay, no more buddy punches.”

**NBSP:** Okay, let’s discuss lessons learned from the experience, and they can be yours or they can be things you’ve heard from Union Pacific management. First of all, what aspects of the project went well?

**Andre Johnson:** The speed in which we got them both enrolled and identified. I think, you know, again, I guess we’re sort of summarizing everything that we said, but also the acceptance of the workers themselves in using this, adapting to the hardware and, you know, figuring out after the first time. Actually, once you got them enrolled, they understand the distance and the position they need to be in, so those are all good thing.

**Tim Myer:** Also, the combination of a non-contact biometric and the fact that irises are very well protected, actually, they are internal organs that are exposed, the probability for them to get false rejects is extremely low as compared to other modalities. Union Pacific recognized that you’re going to have a better performance with this system. Of course, it’s going to cost a little bit more than a fingerprint, but it’s going to be extremely reliable.

**Andre Johnson:** Right. And they had a lot of problems with the fingerprints. They had already tested them and they just didn’t work for them because of the environment and working conditions that we discussed earlier.

**NBSP:** Okay. On the other side of the coin, were there any aspects of the implementation that did not go quite as well?

**Andre Johnson:** In the first release of this software, it was the integrator’s fault here, there were some things that weren’t in place to recognize whether we had good qualities or not of the enrolled iris. You know, the camera has the ability to tell you how good the iris capture is. We didn’t have that in the first release, we didn’t have that, so we were having to go back through this and identify it, and it couldn’t identify them because we
had captured them in the sunlight, and the sun was just too much. The sun is going into
the camera and the camera did not like too much sun coming from behind the head of the
person being enrolled. The quality of the iris was affected as it was captured, but those
are things we did not realize at the time and weren’t written into the code. The second
release accounted for all of that. Once we determined what the acceptable quality was
from 0% to 100% on each side of each eye, so you got four markers there from which we
made the determination what would be the best qualities or acceptable qualities. In most
cases, they’re usually around 100% especially since we know that you can’t have direct
sunlight to the camera. That was actually, you know, the only con that we have.

NBSP: Okay. Just out of curiosity, did you enroll a single eye of the person or did you
enroll both eyes?

Andre Johnson: Both eyes.

NBSP: Both eyes, and one was sufficient for identification. You didn’t require them to
do both, right?

Andre Johnson: Right. Right.

Tim Myer: Jerry, recent research in the iris community—this is like a kind of side
note—a good quality enrollment using the Daugman in two-pi algorithm which is what
we use commercially in the LG system, if you have a good quality enrollment, false
reject, even in kind of stressful environments like Andre mentioned, let’s say we have
significant sunlight in the image or area if it’s a good quality enrollment, false reject at
recognition time is extremely low, less than 1%. But if you don’t watch that quality
metric during enrollment, you know, for example, the imager that was deployed for
Union Pacific will do over 200 pixels across the iris, 200, 220, 240 based a little bit on
the individual. Studies have been done where other imagers were used this were an
interoperability studies that were done by the government. With as little as 100 pixels
across the iris and/or a blur image, poorly illuminated, and they were still getting really
good hemming distance or matching scores on those images when they used a probe that
was high quality for enrollment against the poor recognition image, you get very good
results. But if you have a poor enrollment to begin with, and there are a number of
factors that can contribute to that, then down line, yes, indeed, it will contribute to a
higher false reject. That’s why Andre, they went back and they changed the application
to show the quality metrics during enrollment to warn the individual, “Hey, you’re below
70,” you know, “don’t enroll these images.” That type of thing, you know.

NBSP: Okay, now, does that require a Union Pacific person to be there and monitor
those numbers and say to the enrollee, you have to come back again; you were below 70
or something like that?

Andre Johnson: Oh, yes. During the enrollment process, there was someone there
actually selecting names from a list, and the application itself should either be manually
put in the name or we have employee list that they have from a dropdown and then it just
populates fields. So, there’s always someone there at enrollment time to identify that someone has to be there.

**Tim Myer:** The single attribute that contributes to quality, if you had to pick out one for iris recognition, is eye openness, you know, the amount of occlusion, so it is easy to measure that and easy to display on the screen for the operator that’s performing the enrollment. He can look at the image and say, “Oh, look at that guy’s eyes were half closed. That’s not good. Hit the button again and recapture them.”

**Andre Johnson:** And we do this by the images of the eyes on the screen.

**NBSP:** That’s great. I think this is probably my last question other than will you send me other additional info you think is appropriate. This should be it. Was a formal after action analysis performed to identify the lessons that were learned during the course of implementation?

**Andre Johnson:** I guess that’s question is for me. No, it wasn’t.

**NBSP:** Okay guys, you’ve been very helpful and I appreciate despite all the wrong numbers and such like that, going up.
Andre Johnson: Okay.

**NBSP:** In any case, be sure to take a look at it and have the final say so on what appears online.

**Andre Johnson:** Okay.

**Tim Myer:** Okay.

---

**BAYCARE HEALTH SYSTEM (BCHS)**

NBSP conducted a telephone interview with Mr. Jim Schwamb, Vice President of Patient Financial Services for BCHS, and Lynda Gorken, Director of Management support for the CBO (Central Business Office), and project leader for implementation of this system.
**NBSP:** Can you provide us a brief statement describing the BayCare Health System in the context of the health care industry?

**BCHS:** BayCare is a community-based health care system in the Tampa Bay area. We have nine not-for-profit hospitals, twenty-five outpatient and imaging centers and other types of outpatient services. Our goal is to provide patients with the health care services they need such as imaging lab, behavioral health, and home health and a continuum of services. We have 2,677 beds, 17,400 team members, 13,554 births annually, and 355,307 annual emergency room visits.

**NBSP:** Continuing the background, what economic or security or competitive factors lead you to research biometrics as a possible solution?

**BCHS:** We had two things going on pretty much at the same time. First, we had the voice of the customer. We had a number of patients who indicated to us that they were becoming uneasy giving personal demographic information, such as social security numbers, when they are in waiting rooms with other patients. And they were concerned with how that information was used. The second thing is we had begun installation of a very large electronic medical record project – we’re about two and a half years into a seven year project, and as a part of that project we would be gathering a lot of data and storing it for use when the patient comes in to any of our facilities. It would be used to give us a head start on the patient’s history - allergies, last lab results, x-ray results of things that would need to be immediately available to a care giver who would be treating that patient. We also knew that sometimes it is hard to correctly identify patients when they enter our facilities. They may be coming into an emergency room and they may be, as I call it, “off balance”. They might not be able to come up with their social security number and may seem confused or be unconscious. So we were looking for a way to identify all patients quickly and accurately.

**NBSP:** Did you formalize this thought process to the point where you documented the acceptability and efficacy of the biometrics solution? This question is based on a growing propensity within federal government to require formalized business cases and we’re just curious about whether or not the industry ever really went to the trouble to do that. There is no right or wrong answer to that, but did you ever formally document the acceptability and efficiency of a biometric solution?

**BCHS:** No. Obviously, our issue was patient care and safety. If we picked the wrong Mary Jones or if each time Mary Jones came in we started a new record, then our electronic medical record stored data is of no use to us. We researched the available tools out there, we did some research on finger printing, as an example, and determined that it would not work for us. We looked at smart cards and came to the same conclusion. After going through that process we then hit on the solution that we ended up choosing...vein pattern recognition. We researched that technology, conducted site visits, and concluded that it would work for us. We then took all that information and went to senior management and requested the funds.
NBSP: So presumably if you did not provide them a written report, you certainly put together some presentation where you had to document the things, which you had discovered in your investigation.

BCHS: Correct.

NBSP: Once you got the authorization to do that and the associated funding, did you formalize a requirements list as a forerunner to going out to a vendor or systems integrator or putting out a request or proposals for somebody to do this for you?

BCHS: Actually, for the solution we chose, there was really only one vendor for us to partner with. HT systems is the contractor so to speak with Fujitsu, and HT systems works with the health system to build the integration with the Fujitsu system.

NBSP: So they acted as your system integrator also?

BCHS: Yes.

NBSP: I imagine it was probably a marriage between your IT people and those people at HT Systems

BCHS: Yes.

NBSP: Were performance characteristics a central portion of your selection of the palmreader? In other words, were the false accept, false reject rate or false non-match rates a critical issue for you?

BCHS: Yes, we did research performance and the Fujitsu product is very impressive As with anything else, we don’t buy something without seeing it work and getting good references. We felt that the investigation we did told us that very definitely this product worked and much better than other biometric options

NBSP: Did you formally define the impact that this biometric system was going to have on your facilities or training programs to get people up to speed to use the equipment?

BCHS: Yes we control the training ourselves at the Central Business Office and have a very formal training program. Part of Lynda’s responsibility is training, so we knew that this was something we would be able to handle.

NBSP: How about legal considerations such as development of a privacy policy or privacy impact assessments?

BCHS: Well, we are already governed under the federal government’s HIPAA requirements with regard to privacy, which is very well documented and we have many policies already in place.
NBSP: Did you ever get any push back from any of the patients that all this information could be on record now and you control it and it is their personal information?

BCHS: Actually not. The patients responded very positively to this project and they saw it is something that they have been waiting for. In fact, we had number of comments like “What took you so long. This is exactly what we want.” I mean the compliance rate from patients is something like 99.8% or 99.9%.

The patients really like it. We were concerned that had we gone with something like finger printing the connotation with law enforcement would be a negative, but there’s nothing like that with vein pattern recognition at all. In fact, in the first hospital we brought live, one of the patients was so excited that she went to a television station, which called, came out and did a complete story on it. A very positive story.

NBSP: Did you make a case for the business or economic impact of this? You could go as far as to do a life cycle cost analysis, but normally it is tough. As a minimum, there may have been some estimate of current cost, existing cost to be displaced by a biometric solution here.

BCHS: We did not justify this on a financial basis and we know that the actual registration process itself is only going to be impacted by maybe two minutes. Mainly, we did this to enhance the safety of the patient and the patient’s information.

NBSP: Let’s move on into the evaluation and implementation process. How did you select the best modality or technology to be used? I know you touched on the fact that the fingerprints did not seem suitable because it had possible criminal connotations such as checking of criminal databases, but there must be a range of possible technologies you could have used.

BCHS: The other technology that looked promising was optical (iris recognition). When we checked into it we found that it was very expensive. We looked into fingerprints and felt some of our patients would not feel comfortable and others would not have readable prints. We also looked at smart cards but found that they had a very low carry-rate of 40%, which would not have worked for us.

NBSP: That carry-rate means that 60% of time people would not have the cards with them?

BCHS: Yes. Really, this was the by far the best option for us. And the site visit we went on was very impressive. We saw it work in the Carolinas Health System based in Charlotte.

NBSP: And they were using the Fujitsu unit?

BCHS: Yes.
NBSP: Is there a single model number that you use everywhere or do you have a variety of Fujitsu models depending on the application?

BCHS: It is actually a camera that sits in the bottom of a device for the hand to rest on and in a fashion to help with the camera angle. We needed it to be mobile, so we worked with HT to develop a hand guide that would work for us which ended up probably weighing less than half a pound.

A lot of what we do is on a mobile wheeled computer device (computer on wheels) in the emergency room moving around between patients, and we needed something light, so you can place the patient’s hand on it even if the patient is comatose and still get a reading.

NBSP: Does this mean that you might have multiple types of readers such as one type for a mobile application and another type for a more permanent, fixed location such as a registrar’s work station?

BCHS: No, we are using the same device in every location.

NBSP: Would it work for someone with Dupytren’s Contracture where one cannot straighten one’s fingers?

BCHS: Actually we had a patient who had no fingers and it worked fine. We’ve also had had some arthritic patients where we’ve been able to successfully guide their hands on to the reader.

NBSP: Did you consider any other manufacturer that could provide reading device other than Fujitsu?

BCHS: No. This is their technology.

NBSP: Okay last question in that area. How did the training go? Did it require repeated attempts to train people or did you train them just the next time they came in?

BCHS: What we like to do is completely train our registrars for new applications upfront. So we did an hour and a half training session prior to “go-live”. Usually we tried to do it three or four days before the “go-live”, so it was very fresh in their minds. We supported the training by having trainers from the Central Business Office on site 24/7 for three or four days to help them with any questions or any issues that would come up.

We have a very sophisticated training program. We have five full time trainers who train all our registrars and our patient accounting folks. It helps when you have employee trainers who can quickly pull a project like this together and get everybody started out in the right direction. The other thing that helps us is we are very standardized across
BayCare. We have all the same screens, the same systems, the same processes, same everything, and so training is much easier.

We also spent a good 30 minutes on the importance of the new system and the critical need to determine identity and why we are doing it so rigorously.

Actually, identifying patients properly has become even more important now because the FTC passed this new regulation, the Red Flag Rule,¹ that has more stringent requirements about identifying patients to alleviate identity theft and so this {new system} puts us way ahead of where most folks are at this point in time.

One of the smart things we did is kind of interesting, and this was Lynda’s idea. At the time we were getting ready to kick this project off, we had a very large routine BayCare management meeting - all director level and above. At that meeting, we presented this new project and then we went ahead and enrolled all these people right then and there, which showed them the technology – got them all on board – and then they all went back to their facilities excited and informed about the project.

There are two pieces to this identity process: first, when the patient comes in and they are not {enrolled} in our system, we will go ahead and enroll them. The patients have to provide picture ID, and other information. The next time they come in – and every time after that – all they have to do is put their hand on the reader device and give us their birth date, as an extra check, and that’s it. They don’t in the future have to present ID, give social security number, or any other identifying information.

The initial enrollment piece only adds one to two minutes, but the future authentication process when they re-present, is just seconds. This is quicker than our old process where they had to type in five data elements to search our database to see if the patient had registered before. So we’re very pleased that we’re getting a high enrollment rate and we’re headed in that direction.

**NBSP:** How many readers do you have to handle this throughout the system?

**BCHS:** Three hundred sixty.

**NBSP:** If a patient came in and registered, was treated and didn’t return for a prolonged period of time … nine months, a year, year and a half...and returned, have they experienced any difficulty in using the system again?

**BCHS:** No, the template is stored on the server and remains there indefinitely. The only exception to that might be children age 2 through 12. We re-enroll them yearly due to the

---

¹ The FTC stated that this rule is designed to reduce identity theft by requiring organizations to "implement a written Identity Theft Prevention Program designed to detect the warning signs – or ‘red flags’ – of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts." An organization’s Identity Theft Prevention Program, also known as a Red Flag..
growth of the hand. The pattern of the veins in the hand doesn’t change, but just to make sure we do that yearly until age 12.

**NBSP:** Just as an aside, have you ever come across a case in doing that from year or year where there was an actual change in the vein pattern?

**BCHS:** We wouldn’t know that. We are actually just coming up to a year in July and we have not experienced it yet.

**NBSP:** What’s been the impact of the new biometric application on operational, financial, and personal operations?

**BCHS:** I think the impact is that we’re able to accurately identify our patients and quicker, which gives us access to our demographic and electronic medical record data.

**NBSP:** Are there any “work-arounds”, if an individual comes in and they are in such bad shape that they can’t authenticate? Are there any manual work arounds that you can do to pull up the necessary medical records?

**BCHS:** Yes. If the palm is not useable, we would just resort to our previous process where they do a search by demographic data elements to locate the patient in our database. Or in the case of a John Doe where the patient has no ID and is unable to give you information, a new John Doe record would be started. And, for those rare instances where a patient does not want to be enrolled in the system for any reason, we enroll them in our legacy system which we have to maintain for that very purpose,

An interesting aspect of our implementation of biometrics is that it’s stirred the innovative juices for other areas within the Health System. We are also looking at vein pattern recognition technology to possibly identify patients who are having blood transfused. We are also looking to palm vein technology for allowing our team members’ access to computers and software in systems and those types of things. The technology has been so well received by the community and by the team members who have used it for our project, that people are thinking, “Gosh we can use this for other applications.”

**NBSP:** It’s probably feasible to control access to your controlled substance storage, amongst the staff.

**BCHS:** Yes, I just think there are a lot of different things that it could be used for solving security and access issues.

**NBSP:** There are a number of hospitals that we profiled in previous publications not necessarily using vascular, but using both palm and finger for ER access, for obstetrics access, for access to the facilities or the rooms where narcotics may be stored and indeed access to the actual cabinet or shelves so that they can have a record of everybody that drew a particular drug or prescription out of the cabinets.
**BCHS:** Yes, Fujitsu invented this technology for access to the vault, at a bank or something needing security. I understand that there is an application relative to the GMAT\(^2\) tests for graduate education, where they are using it to make sure somebody is not taking the test for somebody else. It just opens up wide range of possibilities.

One of the things about fingerprints that’s kind of interesting is that a number of people – I don’t know what the percentages are – that don’t have readable fingerprints, because they have worn them down. I heard from a group of cardiologists that some physicians don’t have good prints because they are constantly scrubbing their fingers with harsh detergents and it wears them down over time.

**NBSP:** Okay, let’s touch on the last subject and that’s lessons learned. Can you think of what aspects of the project went well? For example, the preliminary planning phase.

**BCHS:** The implementation phase went extremely well. Lynda has talked about the short time frame for such a huge project affecting our entire System, yet it went unbelievably smooth. It was pretty amazing.

We did a site visit to Charlotte in October 2007 and when we came back, we got the project approved. We had our first kick off meeting of the project May 1\(^{st}\) and our first facility actually went live July 15. Following that, we were bringing up additional facilities about every three weeks. We have a large outreach lab that we did last in the first week of October 2008. With the outreach lab up, we had 24 sites throughout our health care system, -across three counties - that were implemented. And we were completely done one year from our site visit.

**NBSP:** That’s incredible.

**BCHS:** HT Systems was exemplary. I mean they are probably the best vendor we have ever dealt with. They stuck right with us and when we said we want to re-design this or do this different, they were right there, helped us with it, and they didn’t slow us down one bit. We integrated the new system with our hospital mainframe system and ambulatory mainframe system both during that timeframe.

**NBSP:** Did you do any initial, very upfront, pilot test in any smaller section?

**BCHS:** We did quite a lot of testing here at the Central Business Office prior to rolling it out to the first hospital and the first ambulatory site. One of our first efforts was enrolling employees that were here in the Central Business Office. The system worked well before going out to the first facility.

**NBSP:** Did you learn any lessons from that first facility - any things that you were able to apply to second, third, fourth, fifth facilities?

\(^2\)The Graduate Management Admission Test is a computer adaptive standardized test in Mathematics and the English language for measuring aptitude to succeed academically in graduate business studies.
**BCHS:** I think the one thing that’s surprised me was the amount of media coverage this received. I knew we were doing something a little different and but I didn’t realize the interest in the community was so high, and every one of the articles was very positive. We had a lot of national news stories - Scripts-Howard picked us up, the Washington Times .... we were all over the country in one newspaper or another. We had the Department of Justice, contact us, they wanted to benchmark this, and Mass General called us, they too, wanted to benchmark, as well. We had a lot of different folks around the county call and want to know how we were doing. We knew we wanted to have some PR with this, but we just didn’t realize that we would almost be doing this every week.

**NBSP:** So we interviewers are adding to your problems.

**BCHS:** Well you are not adding to our problems, it’s just that we have to be careful what we say to reporters. We wanted to be accurate in all dealings and make sure we were understood.

I guess the one thing that would be a lesson learned is we were so focused on the first facility “go-live” of the enrollment, actually getting those people put in the system, that we didn’t pay enough attention to the authentication when the already enrolled patient returns. We obviously didn’t see much of that the first week we were out there. We might have seen one or two, and we got excited because someone came back and we authenticated him. But the volume of authentications wasn’t high until we got to the outreach lab with lots of repeaters, then we really saw it. So we did do some additional training after we got a significant enrollment in our database. We then went back to every site just to heighten awareness of the authentication process, because we had so many enrollments, we wanted to make sure that we weren’t just enrolling people, but that they were authenticating properly as well.

Certain areas within BayCare have a lot of repeat patients and the outreach lab is one of them. So they might have a patient come once a week for lab draws and it has been very positive for them, because it did speed up their process a little bit. But there are some areas where they don’t have that many repeat patients, and so we had to double back and reinforce the importance of authenticating patients each time they came in.

**NBSP:** Does the system just provide you the name of the individual or does it actually call up the medical records?

**BCHS:** It actually integrates and calls up the demographics and medical records. It is integrated so that the registrar does not realize they are going to another system. You do the actual enrolment or authentication, and then it pulls the patient to the registration screens.

**NBSP:** I think you kind of lost me on that one. I don’t understand exactly what you said.
**BCHS**: In the past, under the old system, we entered five data elements and did a search. We got a list of patients that came up and the registrar would have to say “yes, this is my patient” and choose him/her. The old system would give you a percentage and say for example, there is an 80% percent chance that it’s this Mary Jones, it’s a 20% chance that it’s that Mary Jones, so that the registrar would have to say, “I don’t think it’s either one of these Mary Jones and I am going have to go ask this patient more questions to make sure I have the right Mary Jones.”

With this system, they hit a button that just asks them to have their patient place their hand on the reader, they put the date of birth in, and instead of bringing up a list of names it just takes you right into that patient’s master medical records and lets you go on to registering the patient. So it selects the right Mary Jones automatically and they don’t have to do any investigation. That’s the part they really like.

It takes away the whole decision making for the registrar.

**NBSP**: That’s quite a contrast.

**BCHS**: And visualize what would happen in a really busy emergency room, (and we have one that has a hundred and twenty thousand visits a year – a trauma center), the employee sometimes might take the easy way out and just start a new record. Says, “Well, I can’t figure out if this is the right Mary Jones so I am going to start a new Mary Jones because I haven’t got the time to try to find her relative.” Then you’ve got the same Mary Jones in there duplicated and you are going to have to merge these two files at a later date.

We have one corporate identifying number across all our facilities. You’ve got one number no matter where you go. If you are in there twice, then we must do research and merge them on the backend. That’s a lot of rework and takes a lot of time to do, because you have to make sure you are merging the correct patients.

**NBSP**: You have so many positive aspects of your installation and application there that you probably wouldn’t mind sharing with us what few aspects of the project did not go so well. Is that’s a sneaky way to say what didn’t go so well, without scaring you?

**BCHS**: Quite honestly, we did not have any problems I can think of. I know Lynda feels that it went smoothly and was well received by everybody. It wasn’t one of those projects where “Gosh we have a major problem we have to fix before we can proceed,” or we have to back up and start over, or the software was not working, or its response time is poor. We didn’t have any of those issues.

Normally when we install systems, after we put the first one in, we are tweaking things, and we are making some changes and modifications for the system. We didn’t make any changes after the first install.
**NBSP:** Well, let me try and ask you the question one more way. If you were doing it all over again, is there anything that you would do differently?

**BCHS:** Probably bring outreach lab up first. The outreach area is where we have the most volume. That way we would have seen more authentications the first time around. The more patients we get enrolled, the more authentications we can do and the registrars get very excited when they authenticate patients even today.

The patients also get excited. They think it’s really cool. Put your hand on the device and boy, that information pops up. We are in a part of the country where we have a lot of international visitors because of the Clearwater beaches and those types of vacation things and so our data base tends to be larger, much larger than what the population of the Tampa Bay area is. So they might come back 3 years from now, and we would still be able to authenticate them.

**NBSP:** This system must do nearly an exhaustive search. It does not sound to me like its what we call a one to one search where you have to claim to be somebody, you have to have a pin number that you put in, then it goes and compares the biometric with that single file, It sounds to me like this one searches the entire data base and determines who the individual is. Is that an accurate description?

**BCHS:** Yes, The only thing we do is enter the date of birth, which helps narrow the search.

**NBSP:** That narrows it, okay. What kind of a retrieval time do you have then?

**BCHS:** Seconds. If we don’t have the date of birth or if they can’t get it, we can take the last name, or something very minimal to speed the search up. Most people give an accurate date of birth.

**NBSP:** Does each facility maintain its own data base or is there one general data base for all of the facilities.

**BCHS:** One single data base.

**NBSP:** Okay, so if I register in facility A and for some reason or other I am traveling and I have to go to facility B in another area, I can still authenticate myself there.

**BCHS:** Absolutely.

**NBSP:** Is that data base redundant in some other physical location?

**BCHS:** Yes, it is redundant.

**NBSP:** Okay, and this data base is maintained by your own IT department?
**BCHS:** Yes. We have it on our sequel server.

**NBSP:** I am going to ask one question that isn’t on my list here and you can answer or not, or you can expunge it once you look at it in transcript. Can you give me an estimate of what that cost you on a one time shot to have the system implemented and what you think the annual cost has been recurring year by year there after?

**BCHS:** We are not multiple years yet but what I tell folks -because everybody wants to know the number - I tell them that I can’t really say what we paid for this because we did it in a bit of a partnership with HT Systems. We were the number two health system in the country to do this and we did do some development with them to make things a bit better, but I would think a health system of our size probably is close to a million dollars.

**NBSP:** Okay, the estimate is fine. And no one ever has the time to sit down afterwards and say “How much was the old system costing us on an annual basis and how much is this new system costing us on an annual basis”? I imagine that sort of analysis was difficult and time consuming.

**BCHS:** But we still have to maintain the old system as I mentioned earlier. So there was no financial benefit there.

We have had a few skeptical people. We had one person take the brochure and say, “No, I’m not going to do it”, get to the car, read all the benefits, and then turn around and walk back in and say ”Yes, I do want to do that”.

**NBSP:** Well certainly it must have reduced your staff member’s time a lot because they wouldn’t have to input these five values and then look at a list and try to figure out who was who … that must have saved a lot of time.

**BCHS:** We think it might be one or two minutes of registration. The total registration process probably only takes 7-8 minutes. The real savings in time is for those patients that are difficult to identify and in the old process would have required much research.

**NBSP:** Well we have gone through our list and what a great story you guys have to tell.

**BCHS:** We have been telling it a lot.

**NBSP:** Let me formally thank you both for sharing your time with us and all this information as I said , we will transcribe it, as best as it is professionally possible and we will do some editing, one thought occurs to me that I might move your last comments about training up on to the section on training but that is neither here nor there and then we will give it to you as quickly as we can, and let you take a look at it, you can redact what you want, add what you want. We will have something ready for the rest of the world to see.
**BCHS:** It was a pleasure sharing our experience and we hope it helps others with their identity projects.

**Technology Credit Union**

The following is a composite of responses to NBSP’s written questions, and a Biometric Summit conference presentation by Guri Walia, President, IDMatrixx, Inc.

**NBSP:** Before we discuss details of the application, perhaps, you would spend a
Few minutes describing your industry and your company’s position within the industry.

**TCU:** Technology Credit Union provides financial services to end customers serving over 80,000 members with over $1.3 Billion in assets. Tech CU is among the top 1% of the nation’s credit unions with nine full service branches with close to 30,000 online banking users and about 10,000 bill pay users.

**NBSP:** Given that as background, what led you to research biometrics in respect to your business? Were you trying to solve a business problem or trying to capitalize on a business opportunity? Were there economic, security, or competitive factors that may have spurred the investigation of biometrics?

**TCU:** Tech CU used to rely on traditional forms of authentication such as drivers’ licenses and passports when members visited branch tellers and conducted account-specific transactions. Branches also had on file cards with members’ signatures, called signature cards, which tellers compared with the signatures of individuals visiting a branch to identify them. Not only was this manual process prone to human error, but a signature card was only held at one branch, so if an individual visited another branch, that branch would have to request the signature card to be faxed from the original branch, a process that could take up to 10 minutes. Later Tech CU imaged all signature cards so that they could be accessed electronically, but comparison by teller still took up to one minute.

Tech CU’s Delivery Systems Division, led by SVP Mike Luckin and R&D Manager Barbara Cure, needed to implement an alternate method of identification at its branches in order to authenticate members more quickly and accurately, especially given the growing concern over identity theft and fraud. The new system also needed to provide members with a better customer experience.

**NBSP:** Can you describe the pre-acquisition process for me...i.e.: did you undertake a risk/vulnerability assessment...and if yes, can you describe how it was done and what the results were...obviously, without giving up proprietary information?

**TCU:** Whenever you are trying to increase security, as well as provide added convenience to your customers, you first have to focus on what it is you are trying to protect. In the credit union’s case, it was customer financial data that we were holding. Next, you need to understand where the data is housed...centrally or in a decentralized environment. Then you must define your threats. What are they and where are they? Are they external, internal or both? Having defined the problem you must next define the solution. Are you trying to be on the cutting edge of technology or are you fulfilling a strategic company goal...in this case a goal of improving security and enhancing the customer experience? Finally, how will you know if you are successful? What are the criteria for success? They must be real, attainable and measurable.

There are a number of solutions available to the financial industry including document signing, customer and staff identification, network login/SSO, and biometrics among
others and we evaluated a number of them. Integrating biometrics with a PIN and smart card seemed to be the best approach for us. There were, however, concerns about how well the biometrics technology would work and so we tested several solutions thoroughly for six months in house before making our final decision to implement it in a customer-facing environment.

**NBSP:** Can you describe the various solutions tested and the decision process you went through to land on a particular modality and device manufacturer?

**TCU:** There were solutions tested including network login, physical access and customer identification. The decision was made to focus on customer identification first as that was the most compelling issue for the credit union. We decided on fingerprint biometrics due to the accuracy, price and customer awareness in using the technology. We tried several fingerprint devices recommended by our solutions provider and had the flexibility to use any of them since the software was agnostic to the device used.

**NBSP:** Had you focused on biometrics as a solution from the beginning or were other technologies investigated...i.e.: did you evaluate the strengths/weaknesses of solutions other than biometrics?

**TCU:** As mentioned earlier, various authentication technologies were investigated, however the bank decided to incorporate biometrics as they, based on the technologies evaluated, provided an enhanced security, speed and convenience for the credit union’s customers. Now when members visit a branch teller, they have the option to authenticate themselves by entering a PIN (something you know), swiping a debit card (something you have), or placing their finger on a sensor (something you are) using a device with a numeric keypad, a card reader, and a fingerprint sensor. IDMatrixx provided a software solution, which was integrated with the core banking system thereby enabling a comprehensive authentication solution.

**NBSP:** Is it one factor authentication? PIN, card or biometric...or is it two of these?

**TCU:** The system uses two-factor authentication and gives the user a choice to enter any two inputs from a finger-scan, an ATM card or a pin.

**NBSP:** If you did evaluate the strengths/weaknesses of solutions other than biometrics what led you to decide on biometrics?

**TCU:** We felt the accuracy and reliability of biometrics, at least for our application, exceeded that provided by other technologies. And, given that we are dealing with clients’ money, in our case well over a billion dollars, accuracy and reliability were critical. We conducted a cost/benefit analysis on the proposed solution, which fit our business model; but the key was that the software solution provided by our integrator, IDMatrixx, could readily be integrated with our core banking system.

**NBSP:** Can you explain why this is important?
TCU: The integration incorporated biometrics into our existing solution and made it a seamless transaction for the bank employees as once the person was authenticated, the system would open the appropriate screen to continue the banking transaction.

NBSP: Can you describe the selection process you went through to determine which modality (finger, face, iris, etc) was the best for your application?

TCU: After evaluating a number of modalities we landed on fingerprint technology for a couple of reasons. First, despite the negative connotation fingerprints might have had at one time, they are becoming much more mainstream now. Go into any bank and you will see the little fingerprint pads at each teller station for those clients who do not have an account at the bank. Fingerprint sensors are pretty much the modality of choice for laptop access as well. So, there was the familiarity factor. Total cost of deployment was much more favorable with fingerprint and the accuracy, which, as I stated before is so critical to a financial institution, met all our thresholds for false accept, false reject and throughput.

NBSP: Once you settled on a modality how did you evaluate potential providers? i.e.: was it an internal evaluation or did you bring on a third party to help? In either case, can you describe the process you went through?

TCU: There were several vendors that we looked at internally to evaluate the strength of their respective technologies and the cost effectiveness of their proposed solution. We engaged an outside consultant to help with the process and to test out the technology and the vendor’s claims. Based on evaluation results we selected the IDMatrixx solution because of the robustness of the technology.... it had been deployed at several police stations as an AFIS system... the speed at which it could be integrated with our banking system -- and total cost.

NBSP: How was the installation process handled? Did you use an integrator or other third party consultant?

TCU: A system integrator that was familiar with our core-banking system was used to integrate the authentication system into the core banking application and install the system. The installation of a central authentication server at headquarters was done in four hours. Then, the software installation and activation of the biometric units averaged about an hour per branch. Each new branch opens with the new system fully operational.

NBSP: How did you prepare your employees/customers – (those who would be using the system) - for the application? i.e.: was there any formal training before the system was implemented? How did the system users initially react to the idea of having a biometric taken and then having that biometric matched (for the application)? How well did the users come to accommodate and adapt to the biometric concept?
**TCU:** Credit union members were very receptive and voluntarily enrolled in the system. There were about 1% of the customers that were apprehensive, since enrollment was voluntary; they had the option to not enroll.

**NBSP:** If you had formal training before implementation, how did that assist in the transition?

**TCU:** All the Branch Tellers went through a 4 hour formal training on how to use the system and what questions to anticipate from the customers and how to answer them. There was a question and answer sheet that was passed out to the end consumers. The training was very important to make the Tellers comfortable with the system. Attention to training is as important as attention to technical detail in assuring a successful implementation. Members and tellers both have to feel comfortable with the new technology and misperceptions about it have to be cleared up. If you handle that upfront you greatly reduce the chance of any negative reaction.

**NBSP:** Can you describe how members were enrolled...were CU employees trained to do it? Is there a permanent enrollment station at each branch to accommodate new members?

**TCU:** Members were enrolled by the CU Branch Tellers within 30 seconds at the teller station when they would come in to do a banking transaction. New members were enrolled at the time they opened the bank account by the employee signing them up.

**NBSP:** Were there any surprises along the way, and can you elaborate on how you dealt with the issues?

**TCU:** The biggest surprise was how well the technology was received by our customers as we were initially not sure how our customers would react to using biometrics technology. Training the Tellers and making them very comfortable with the system helped sell it to our customers.

**NBSP:** Let’s discuss potential quantifiable and non-quantifiable benefits of your application solution. What would you say were the quantifiable benefits to your business i.e.: cost savings, reduced risk of fraud, operational costs etc.

**TCU:** Most importantly and based on client feedback we find that our members feel more secure knowing their accounts are protected from identity theft or fraud by a more technically advanced security system. We are able to offer them the same protection that the government is installing in passports and at airports. Members increasingly are replacing their PINs with their fingers and use biometrics as the preferred second ID for wire transfers.

**NBSP:** What is the first ID?
TCU: An ATM card (US Patriot Act requires banks to use two forms of IDs for any wire transfers, biometrics is stated as an acceptable ID). From an operational standpoint, we have lowered authentication time from the 1 minute it took to compare imaged signature cards to an average of 3-5 seconds using the biometric system. Both teller and member transaction times have been reduced and as have the number of fraudulent transactions.

NBSP: Can you quantify the reduction in fraudulent claims?

TCU: That is confidential information for any bank as you can imagine.

NBSP: How about non-quantifiable benefits that you realized i.e.: added ease or convenience for your customers and/or employees? Or a heightened sense of identity protection?

TCU: Less tangible, but of high importance is the fact that by deploying a biometric authentication solution we demonstrate to our members that they are our priority when it comes to protecting their financial assets and ensuring fast service when they visit our branches; and that we will stay current or even ahead of the technology curve to do so. A number of members view the biometrically-enabled system as much more secure than scanned facial images and our Branch Managers believe that the opportunity for fraud is lessened just by the visibility of the authentication devices....I mean, when they see the fingerprint scanner they are deterred from attempting a fraudulent transaction and will look elsewhere for a less secure facility.

Customers love the feeling of security as no one can steal their identity and access their life savings. This helps differentiate our credit union from other financial institutions especially with customers worrying about identity theft. Oh, there were some questions at first from some members. Like they saw something on TV about using gummy bears to capture a fingerprint or if their fingerprint scans could be stolen or sold. We were able to alleviate those fears by educating them on the technology...you know, like the fingerprint scanner had a liveness detection capability that wouldn’t be fooled by gummy bears.

One of my favorite customer quotes is “I’m comforted knowing my private financial information is protected by fingerprint biometrics. I can access my account even if I forget my wallet or my PIN, and I feel confident that the credit union will prevent a fraudster from accessing my life savings.”

In addition to the benefits we’ve already discussed there is another benefit, that being the ability to strategically differentiate your business from the competition though the use of an enhanced security technology. And, we feel we have done just that, and the feedback we get from new members seems to support that belief.

NBSP: Let’s discuss some of the lessons you learned from this experience and what you would pass on to others who are contemplating biometrics in their business. What aspects of the project went well?
TCU: I think as I mentioned earlier, the integration of the IDMatrixx software with the core banking system ...that was a real plus. The branch installations went very smoothly as did member enrollment. Bottom line --the end-customers applauded us for deploying the biometrics technology.

NBSP: What aspects of the problem did not go well

TCU: The hardware scanners we initially deployed went bad quickly due to low Electro Static Discharge ratings and had to be frequently replaced. Since the software solution we deployed was an open solution, we did not have any problem to switch to another hardware vendor’s scanners. The key lesson here is to always make sure you are not locked into a proprietary system and you work with a vendor that provides an open system which gives you the flexibility to switch hardware vendors so you don’t have to re-enroll your customers.

NBSP: Was a formal” after-action” analysis performed to identify lessons learned?

TCU: Yes.

NBSP: Can you describe the process for us...and were any changes to your application made as a result.

NBSP: Can you describe the after-action analysis in a bit more detail?

TCU: No changes were made to the customer authentication application but the bank decided that it wanted to deploy biometrics applications in other areas of the bank.

NBSP: Such as?

TCU: Network Login.

NBSP: Well, thank you very much for your time. We enjoyed speaking with you today and I’m sure our readers will find your application most interesting.

PARKVIEW ADVENTIST MEDICAL CENTER (PAMC)
Parkview Adventist Medical Center is a 55 bed hospital in Brunswick, Maine which implemented a fingerprint-based biometric system in 2006. The application was part of a larger project to develop a secure, paperless medical records system.

On April 3rd 2009, NBSP conducted a telephone interview with Mr. Bill McQuaid, Assistant Vice President and CIO of PAMC.

NBSP: Mr. McQuaid could you give us a brief statement describing the case study we’re about to review and a summary of the issues facing your hospital and the healthcare industry?

PAMC: Parkview Adventist Medical Center has been serving the healthcare needs of the residents of mid coast Maine since 1959. Affiliated with the Seventh-day Adventist Church, Parkview was founded by three Adventist doctors and is one of about 70 acute care Adventist hospitals in the United States. There are approximately 200 worldwide.

In 2008, Parkview was recognized as a national award winner in healthcare service quality by Avatar International Inc. and recently became the 23rd hospital in the country to achieve The Health Information Management System Society (HIMSS) Analytics stage 6 status (http://www.himssanalytics.org/general/about.asp).

Parkview found itself at the intersection of two of the biggest concerns in the healthcare industry today—namely, how to provide easy access to patient data and medical information while finding a way to keep it all secure. Any access or security system implemented would need to take into account how often staff needed to log in and out of applications to access patient data—and balance that with compliance with industry and government regulations.

NBSP: What economic/competitive factors led Parkview to research biometrics as a possible solution?

PAMC: The pressure to increase productivity and protect patient data—among end-users and IT administrators alike – is an ongoing challenge for healthcare facilities of all types and sizes. The abundance of on-line information available to clinicians today ultimately improves productivity and potentially provides a competitive advantage in the market. But, facilitating fast and secure access to that information – without security policy violations such as writing down or sharing passwords - can be complex and daunting. Further complicating matters, strict regulations like the Health Insurance Portability and Accountability Act (HIPAA) were put in place to improve and protect patient information. Under these regulations, Parkview was challenged to both protect patient information and at the same time, securely provide clinical staff the ability to walk up to any workstation and log into the network. They needed real-time access to applications and information that would enable them to provide timely care and service to patients. A biometric solution could also take care of my issues; 1) they never do log off, and 2) how do I make sure they are not sharing their passwords?
Parkview discovered that integrating finger biometrics with single sign-on (SSO) was the answer. The SSO technology allows each user to sign on to all applications using a single password. By incorporating finger biometric scanning into the solution, Parkview could enable each doctor or nurse to log on to any PC at the facility with a single fingertip swipe. Because finger biometrics is a strong form of authentication, which also strengthens IT security and helps, meet compliance guidelines. Users enroll one or more fingerprints via a scanner, which then records them in a file associated with each user’s identification information. Thereafter, when logging in, the user again scans the fingerprint, which is compared to the print on file to complete the authentication process.

**NBSP:** Was the acceptability and efficacy of a biometric solution documented?

**PAMC:** We really did not formalize our documentation on the biometric solution. The biometric implementation was part of an effort to implement a 100% paperless environment. We were doing a lot of implementation with nursing documentation and physicians doing their own orders. It was all documented as part of a solution to get the nurses on the same page and get positive reinforcement. We were listening to a lot of their issues. I went to a lot of meetings documenting what I heard from physicians and nurses and a lot of it was “How do you expect us to keep logging in and logging off? So we started thinking that a biometric solution could also take care of my issues; 1) they never do log off, and 2) how do I make sure they are not sharing their passwords? We kind of used it as a tool, a mechanism of “We have listened to your concerns, this [biometrically-enabled single sign-on] is our solution, what do you think? And then we further structured it so that they could not participate in the biometric single sign-on until they went to training. So we kind of used it as a way to solve a lot of our issues. We did not formally document the acceptability and efficacy of a biometric solution before implementation. We had, however, documented a series of SWOT (Strengths, Weaknesses, Opportunities and Threat) analyses in our area and we have always had a security issue with our multiple systems. So it just kind of blended in and became obvious. By listening at all of these meetings, myself and the CFO began to realize that this was a no-brainer. If for no other reason, the cost of this product to do this initiative would be less than going to all these meetings. Now that we are successful and we are live, the value of a biometric solution is certainly documented.

**NBSP:** When you talk about integrating finger biometrics with single sign-on where did you actually first hear about biometrics and how did the idea of biometrics arise as opposed to some other type of technology?

**PMAC:** You know at the time we were researching vendors [for the total project], we were thinking wouldn’t it be great if you could just come up with some sort of single sign-on. Well, let us go one step farther - let us go zero sign-on, so we started researching and calling around. I was actually at a local HIMSS (Healthcare Information and Management Systems Society) conference once and I saw this – I found some other solutions at the time that might have worked, but they were not hardware based and they required a lot of software. I did not want to deal with that because we were so small.
Then at this local HIMSS conference, I saw Imprivata which was all hardware based and we started researching. They said, “You know what? We already have a hospital that has done this in your environment,” and we went from there as you said we have been on it since 2006.

**NBSP:** So, you really did not have to make a business case how non-biometric solutions A, B, C, D, E were less viable than biometrics?

**PAMC:** No, I didn’t – I finally gave them my plan of what we wanted to do. They saw the demos, brought doctors to evaluate, then they saw the excitement and said this is a no-brainer, go for it.

**NBSP:** Okay.

**PAMC:** Because we are a 55-bed hospital we know all the major players in the area and we know the board. I can present right to the board myself. And now they are seeing what all the benefits are. They are seeing that we are one of only 24 organizations in the country at a stage 6 status for EMR (Electronic Medical Records) adoption.

**NBSP:** So you did not do a formalized analysis?

**PAMC:** No, not at all. It was more like you said; we were getting ready to go live with nursing documentation. I went out to the units a lot, explained, showed demos, and then heard what the issues were and tried to come up with solutions before we went live … and the big one was security, people not logging off, and [secondarily] people having to keep logging in and logging out of each of multiple applications in the hospital.

**NBSP:** Okay. While you were making these pitches you mentioned, did you have to get into any of the details of operational issues such as the biometrics’ performance, reliability, changes that have to be made to the facility, amounts of training, issues like that?

**PAMC:** No, because I sold it as being part of a bigger project the training that they had already approved for all of nursing. It is actually what I used to make them sign up for training.

And what I did was put the technology on the medical-surgery unit and gave a couple of my super-users access so people saw them using it and they all wanted it. We told them “Well, you have not signed up for training yet” and the training sessions just filled right up.

**NBSP:** Very clever.

**PAMC:** So when they are seeing this thing, it was kind of like the cheese on the mousetrap. We put some bait out there and then reeled them in. What I did not want to do is use a treble hook and a fishing pole and snag them.
**NBSP:** How about the legal aspect of your implementation? Did you have to deal with a lot of privacy considerations, development of a Privacy Policy, and privacy impact assessments?

**PAMC:** Well, what is it for me, and I did not even realized at the time – we have the state surveys come in now and they walk by and see the biometric and inquire, “What’s this?” I explain that we use biometrics so people do not even know what their password is because their finger never changes and need no password. Same inquiries about the proximity detectors, and I explain that these proximity detectors automatically log the user off the system when they back away. The net result is that people are coming here now just to look at what we are doing so they can try to adopt those models.

**NBSP:** So you didn’t have to make any privacy assessments then?

**PAMC:** As mentioned, I have done SWOT “Strength Weaknesses, Opportunities and Threats” analyses on our department to identify weaknesses and I always highlight security. So this was a way for me to pitch this to Administration to improve the overall security of the organization and also relieve some clinician frustration.

**NBSP:** Did you ever have to formalize these issues in any sort of documentation, or did you make the presentations to the board and once they gave you their blessing you could go ahead?

**PAMC:** I think it was a lot more streamlined because I report directly to the CEO and CFO. And they report to the board and we are having such great success with our implementation that they say keep doing it. To be honest I did not spend much money to do this at all. It costs me $10,000 a year to keep this up. So when you were ask about documenting costs I don’t think people know how reasonable this stuff is.

**NBSP:** And you have got a pretty good feeling for $10,000 a year cost of operation and you probably do not have a documented cost previous to the biometric application do you?

**PAMC:** Well no. Before we did this, this hospital used to be what they call “Best of Breed”. Every single department had its own software with different vendors running on a different platforms. But back in 2005 it was not working for us. Key areas were unsupported as you probably read in the article. We opted to go with a single vendor for everything; Clinical, finance, H.R., payroll, everything is one vendor. So, I rolled this solution into that cost, so my cost now to run the whole hospital is the same as it was before but now we are paperless.

**NBSP:** Oh, that’s excellent.

**PAMC:** So I bundled [the SSO-biometric solution] into the overall upgrade project to one single HCIS (HealthCare Information System)solution. My thought was that I am only going to get a chance to do this once.
NBSP: That sounds pretty effective.

PAMC: So I threw the cost of the biometric SSO implementation into the cost of redoing the whole hospital HCIS. Like I was saying before, if we would have upgraded everything we had, it would have cost more than what we are doing now but we would not be able to meet any of the standards that we have now like HIPPA and HIMSS Analytics Stage 6. We would also not be a paperless environment. We have also rolled this technology into our physician practices.

NBSP: And can you explain rolling the technology into our physician practices, Bill?

PAMC: What that means is that our physician practices also utilize an EMR (Electronic Medical Record), and our doctors and nurses in the physician practices are documenting in the computer. They are also tied to the hospital so when they go into their exam rooms and offices they just stick their finger on [the reader] and that logs them right in, they get the same information they do if they are in the hospital.

NBSP: So they have fingerprint access in their laptops?

PAMC: And all the exam rooms and any PC’s that are in the open.

NBSP: Are patients ever enrolled in this system?

PAMC: Never.

NBSP: Never?

PAMC: It is tied to our active directory and our users. We have not gotten that far because this opens up all other aspects of security concerns.

NBSP: Has there been any thought to taking that a step further in terms of let us say physical access to narcotic cabinets or access to other areas?

PAMC: It is definitely something that we are looking at in the future

NBSP: You are formalizing that then?

PAMC: That documentation would actually come from the pharmacy and they already have a solution that works and converting my not be cost effective.

NBSP: Well, it would be interesting to see how that develops.

NBSP: Can we talk for a minute about the evaluation/implementation process? For example, why did you choose fingerprint as a biometric technology, or modality?
PAMC: Parkview selected finger biometrics as the biometric modality best suited because it enabled its more than 300 clinicians/staff to quickly and easily gain access to authorized applications.

NBSP: Would not other biometrics have done the same thing?

PAMC: Possibly. While researching this implementation, we encountered a number of biometrics that might have performed the actual identification satisfactorily. There is nothing better however, than having a vendor that could offer me the biometric solution and single sign-on. I have seen many people and organizations fail by choosing a single sign-on vendor, then choosing a different biometrics vendor.

I like to keep it simple so I made it clear that what we wanted was a single sign-on so that for example when a doctor sticks their finger on to the screen of the “med-surg” [Medical-Surgical], unit, it does not matter which of the multiple hospital applications they need access to next. The system automatically logs them in.

NBSP: And there is a proximity detector there so if the doctor goes away, it automatically logs them off right?

PAMC: Yes, but I only do that on the units in the hallway, or other public areas where you definitely do not want the information left up on the screen. It’s like sonar. You back up and automatically in the background the system essentially hits Control, Alt, Delete, Log-off, in three seconds. So that is really the technology and it works great in that application.

NBSP: So nothing distinguished fingerprints from let us say facial, or iris recognition, or vascular biometrics except the fact that this single vendor supported fingerprints and single sign-on?

PAMC: Well they also provided proximity cards I just kind of thought to myself wow, when I worked at L.L. Bean and I followed these people around, they forget their card, they just used their friend’s card. I would like to see them start sharing their fingers. Well, everyone gets all excited about using just their I.D. badges. I just do not see it - It is a pretty easy thing to steal. Maybe I.D. badges with another form is good but alone, I just do not see it.

NBSP: So how did you select a biometric reader provider?

PAMC: At the recommendation of Imprivata, Parkview selected UPEK and deployed its TouchChip biometric readers. We found that it was easy to integrate UPEK’s TouchChip biometric readers with both OneSign and the hospital’s existing MEDITECH modules. And I’ll tell you what, in three years, I think we have only replaced two.

NBSP: Is that right? That is very good.
PAMC: I could not believe it. They are quite big but when you read the details of the technology – the way they do their algorithm …. They even have thermal sensors that search for heat so if you cut someone’s finger off, and the system does not sense heat it won’t operate - they are pretty amazing.

NBSP: So, they got liveness detection built in?

PAMC: Yes exactly.

NBSP: Did you use a systems integrator?

PAMC: Yes we did. We used Imprivata’s one sign-on solution, but I already had Forward Advantage as a vendor. They work directly with the vendor I chose for our computer system. So, instead of bringing on another vendor, they are actually the reseller of the product and I already had a relationship with them that is why I bought that from them.

NBSP: Did they do your integration work for you?

PAMC: This is the cool part. They came up for two days and we were live before they left. Our approach was not to have the integrator do it all, but rather, to have them train me and my staff so we could do it ourselves. So like you said, they came up and did that, providing some oversight during startup. They asked for information that they would need and I sent it back to them. They brought us two devices that were preconfigured with the information I gave them. We plugged them in and we were live probably 12 hours later on med-surg. I mean it was ready to go in two hours but I actually rolled it out to all the units and had my whole department testing and using it on the unit.

NBSP: Extraordinary.

PAMC: But if you think about it we had the foundation built. I have about 70 applications in this hospital. About 60 of them are one vendor and one sign-in. So my windows log-in. my email, my fax, and my hospital information system were the only things that I had to build apps for. So it was sweet. It was like a year’s work done in eight hours.

NBSP: You talked about the training that you had built into this process. When it was first broached was there any push back at all in terms of biometric system?

PAMC: Actually not at all because our nursing staff had been using biometrics authentication already with our medication dispensary machines. Because of this, the technology did not intimidate staff in any way. We also made sure we did a good job of explaining the technology to the users.

NBSP: How many fingers do you use?
PAMC: Four, two on each hand.

NBSP: What has been the impact of the implementation of your biometrically-based single sign-on application?

PAMC: Nothing but positive. As a result of the SSO/finger biometrics project, the need for physicians and staff to memorize multiple passwords was eliminated. Parkview cut helpdesk costs and improved employee productivity because clinicians are now spending less time logging in and out of network applications—improving the security of patient data and overall patient care. By incorporating finger biometric scanning into the SSO solution, each doctor or nurse is able to log on to any PC at the facility with a single fingertip swipe. Key business results include:

- Three-day deployment with minimal resource requirements
- Single sign-on access to all critical applications
- Increased security through strong authentication with finger biometrics
- Faster, more convenient login/logout for users
- Lower Help Desk costs related to password resets
- Reduced IT support costs and resource requirements
- Easy adoption and consistent enforcement of security policy
- Compliance with data security requirements

NBSP: What aspects of this project went well?

PAMC: Well we’ve already mentioned some, but another was managing change in the organization. Recognizing we’d need the clinicians’ support to implement a new HCIS system, Parkview arranged a series of presentations during which we demonstrated to doctors how easy it would be for them to gain access to MEDITECH applications with SSO and finger biometrics -- and the clinicians were sold. When the clinicians learned that they would log on just once, using finger biometrics to access all the applications they needed, they started to become more interested in hearing about the project. With the use of SSO and finger biometrics, the IT team was able to deliver full access to all hospital information, with just one finger.

If I had to summarize “Lessons learned” I would probably say a couple of things:

- You can spend all you want on technology, but there’s nothing more powerful than education. Given the number of high-profile data breaches in the industry, healthcare organizations need to ensure patient data protection and comply with industry regulations such as HIPAA.

- Secondly, as I explained before, bringing your users on board early on is helpful in many ways. If they are impressed, and the value for them is obvious, they will make the overall adoption simpler and faster. Educating clinicians, staff, IT personnel, etc. is a critical step in protecting an organization and with the SSO/finger biometrics project, we learned that you have to do a comprehensive

60
and thorough review of available solutions and educate users on how to properly utilize them. In our evaluations, we discovered the importance of tying strong authentication with SSO and learned that combining finger biometrics with SSO was an easy and efficient way to strengthen security and improve productivity.

- Additionally, I’d point out that although Parkview initially invested in finger biometrics to solve its password problems and strengthen IT security, the technology has provided additional benefits, for the process, called “bedside medication verification,” which greatly reduces medication errors and ensures patient safety. Parkview now barcodes and scans every medication that enters the hospital and each patient is also identified by a barcode on their wristband. Scanning tells the nurse if the medication being administered was ordered for that patient and is being given at the right time. And as we mentioned, the medications are only accessible for dispensing after a nurse has authenticated using finger biometrics.

NBSP: Having it up and running and you have been through it, if you would be doing it all over again, would you do anything differently?

PAMC: It sounds bad but actually I think we did a pretty darn good job. It solved so many aspects that if we had to do it over again, we’d probably do it the exact same way. Part of that may be our underlying philosophy that everything we that we do here, we should do with our own staff. My motto is if we can’t do it on our own, we need to learn it because we should not be taking on stuff that we cannot handle by ourselves. The environment changes way too fast to be relying on other people and getting nickel and dimed to death.

NBSP: How big an IT staff do you have?

PAMC: Six including myself.

NBSP: Bill, we appreciate your cooperation and the help you’ve given us. You have given us a wealth of information and I am really, really pleased that your installation, your application went so well.

PAMC: You’re welcome.

NBSP: Bill you have been extremely helpful to us, both in the written material and the verbal interview and we appreciate it so much.

Pearson Vue

The following is a composite of responses to NBSP’s written questions, and a Biometric Summit conference presentation by Samir Nanavati.
Before we discuss details of the application, perhaps, you would spend a few minutes describing your industry and your company’s position within the industry.

Pearson VUE is the leading provider of global computer-based testing solutions for clients in the information technology, licensure, certification, academic admissions, regulatory, and government testing service markets. We provide a full suite of services from test development to data management and we deliver millions of high-stakes tests a year, primarily through our industry-leading network of over 5,000 test centers in 165 countries. 230 of these are fully-owned and -operated Pearson Professional Centers, utilizing a patent-winning design created specifically for high-stakes testing and offering a carefully controlled, consistent and secure testing environment.

We are a part of Pearson plc, an $8 billion corporation that is the largest commercial testing company and education publisher in the world. Pearson’s businesses include the Financial Times Group, Pearson Education and the Penguin Group. The primary Pearson VUE operations facilities are located in the United States, the United Kingdom, and India, with satellite operations in China and Japan.

Given that as background, what led you to research biometrics in respect to your business? Were you trying to solve a business problem or trying to capitalize on a business opportunity? Were there economic, security, or competitive factors that may have spurred the investigation of biometrics?

We deliver millions of high-stakes exams each year in over 5,000 test centers in 165 countries. We began utilizing fingerprint-based biometric technology in our high-end Pearson Professional Centers in 2001 as a means to ensure test integrity and to enhance the candidate management workflow. The primary benefit has been to deter and detect attempts at test taker impersonation, where someone hires another person (also known as a ‘proxy’) to take a test for them. However, our needs and those of our clients have evolved since 2001 and we were exploring opportunities to introduce a next-generation identity management system with greater flexibility and support for enhanced capabilities such as global one-to-many identification.

Can you describe the pre-acquisition process for me...i.e.: did you undertake a risk/vulnerability assessment...and if yes, can you describe how it was done and what the results were...obviously, without giving up proprietary information?

We were in the relatively unusual position of having outgrown our first-generation biometrics capability originally deployed in 2001. Therefore, as opposed to making a no/no-go decision on biometrics, we were interested in developing a next-generation identity management solution to meet our evolving needs. This led to a formal requirements analysis followed by a technology and vendor selection process.

Did the vulnerability assessment help you define your program requirements? Operational?
PVUE: One of the major factors in biometric technology selection and system design was an assessment of the core technology’s vulnerabilities to different types of attacks and threats. Our decision to select palm vein recognition technology in our test facilities was based on an evaluation of cost, performance, scalability, accuracy, usability, vendor support capabilities, privacy impact, acceptability to our client and candidate population and, of course, the competitive edge the solution would provide us. Our needs were somewhat unique and demanding, given that the solution needed to be tightly integrated with our existing test center software systems and deployed to a mix of company-owned and third party test centers in dispersed locations worldwide. The solution had to support over 700 devices operated by over a thousand personnel at more than 400 test centers in over 90 countries. It had to scale to efficiently process millions of biometric templates each year and to support enhanced services such as fast 1:N matching.

NBSP: Had you focused on biometrics as a solution from the beginning or were other technologies investigated...i.e.: did you evaluate the strengths/weaknesses of solutions other than biometrics?

PVUE: Because we have a strong interest in ensuring that candidates can only test under one identity, biometric identity management (coupled with stringent procedures for verification of original identity documents) has been an essential part of the Pearson VUE workflow for years. No other technology could be realistically used in place of biometrics for robust candidate verification and identification.

NBSP: If you did evaluate the strengths/weaknesses of solutions other than biometrics what led you to decide on biometrics?

NBSP: Can you describe the selection process you went through to determine which modality (finger, face, iris, etc) was the best for your application?

PVUE: We were an early adopter of digital fingerprint technology in our test facilities, starting in 2001. In 2006 and 2007, we began to examine alternatives; for both regulatory compliance and public perception reasons, collection of fingerprint data was becoming increasingly difficult in certain countries in which we operate. Features and capabilities that drove technology selection included the following:

- Usability without extensive training
- High enrollment rates
- Low unit cost
- Acceptability (from a privacy perspective) to candidates, clients and regulators
- Form factor (small footprint, suitable for desktop use)
- Accuracy - low false rejection and false acceptance rates
- Global support on the part of the vendor
**NBSP:** Once you settled on a modality how did you evaluate potential providers? i.e.: was it an internal evaluation or did you bring on a third party to help? In either case, can you describe the process you went through?

**PVUE:** We engaged International Biometric Group (IBG) to provide technical development services as well as consulting services including requirements definition, system design, and solution integration support. During the initial stages of technology assessment, IBG suggested that vascular pattern recognition technology warranted consideration, as the technology met several of our requirements for performance, usability, cost, and form factor. An in-depth evaluation of the technology itself and the vendors offering such products, conducted in conjunction with IBG, substantiated this initial recommendation and led to the selection of palm vein recognition.

**NBSP:** Let’s discuss potential quantifiable and non-quantifiable benefits of your application solution. For example, what would you say were the quantifiable benefits to your business i.e.: cost savings, reduced risk of fraud, operational costs etc.

**PVUE:** The primary quantifiable benefit to the business has been a reduction in various types of test-related fraud and malfeasance, including the use of impersonators (also known as ‘proxies’) and other misrepresentations of identity. We have also recognized operational efficiencies in terms of candidate management through the examination lifecycle.

**NBSP:** How about non-quantifiable benefits that you realized i.e.: added ease or convenience for your customers and/or employees? Or a heightened sense of identity protection?

**PVUE:** We are recognized as the industry leader in the application of advanced technologies for secure computer-based testing. Our successful implementation of next-generation biometric technology underscored that leadership.

**NBSP:** How was the installation process handled? Did you use an integrator or other third party consultant?

**PVUE:** We worked with IBG and the technology vendor to integrate the equipment into our systems. A fulfillment vendor handled logistics for shipping and delivery of the physical devices to locations worldwide for installation. The technology was integrated in such a way that the upgrade process required minimal direct involvement by central Pearson VUE personnel and was streamlined such that local test facilities were able to install and configure the devices on their own.

**NBSP:** How did you prepare your employees/customers – (those who would be using the system) - for the application? i.e.: was there any formal training before the system was implemented?
PVUE: We developed training material to familiarize test facility staff with device usage, best practices and related policies and procedures. Staff, in turn, guide each testing candidate on the use of the system. We also worked with the hardware vendor to develop a custom hand guide for the device that simplified and standardized usage on the part of operators and users. We created a strategy and supporting materials to inform and educate our clients about the features and benefits of the new system. We also worked with clients to develop informational videos, brochures and other materials to assist them in introducing their candidates to the new technology, provide assurance of security and privacy, and make the transition smooth and painless for them.

NBSP: How did the system users initially react to the idea of having a biometric taken and then having that biometric matched (for the application)? How well did the users come to accommodate and adapt to the biometric concept?

PVUE: Users (candidates) are by and large accustomed to the use of biometrics in this environment, and there is a general understanding across the candidate population that test integrity is an important element of high-stakes testing. During the early stages of deployment we conducted surveys of both candidates and test facility staff, who overwhelming reported satisfaction with the new technology.

NBSP: If you had formal training before implementation, how did that assist in the transition?

PVUE: All test facility staff were provided training prior to switching over to the new technology. The training program and early monitoring helped us to identify enhancements to both the training itself and the technology user interface that subsequently led to further improvements in usability and performance.

NBSP: Have you been able to quantify any operational, financial, or competitive benefits to your company as a result of the deployment of biometrics?

PVUE: There has been a direct impact on reducing identity fraud, in terms of both prevention and enhanced detection.

NBSP: If you didn’t formally quantify such benefits, can you subjectively assess how the application has benefited your organization operationally, financially, or competitively?

PVUE: The use of palm vein recognition technology underscores Pearson VUE's commitment to exam security. This has proven to be an important competitive differentiator for our clients and has laid the groundwork for additional services we intend offer clients.

NBSP: Were there any surprises along the way, and can you elaborate on how you dealt with the issues?
PVUE: Due to the evaluation and selection process described earlier, and a strong working partnership with IBG and the hardware vendor, we experienced few surprises.

NBSP: Let’s discuss some of the lessons you learned from this experience and what you would pass on to others who are contemplating biometrics in their business.
A. What aspects of the project went well?
B. What aspects of the problem did not go well
C. Was a formal” after-action” analysis performed to identify lessons learned?
D. If yes...can you describe the process for us...and were any changes to your application made as a result.

PVUE: The system was developed and continues to be managed through a formal software development life cycle process. This process is designed to ensure the right stakeholders are engaged at every step in the life cycle, from initial business case analysis and requirements gathering through design and development to deployment, training and maintenance. The system was deployed in phases, beginning with a three-month pilot during which we rolled it out to a limited set of locations for a single client’s program and monitored the system and end users for technical difficulties and training issues. This approach worked well and allowed us to tweak procedures and the technology itself prior to expanding the system to all locations and migrating additional clients to the new platform. We are now in the process of implementing additional modular capabilities (such as 1:N matching) that build upon this foundation.

NBSP: Thank you for your time.
Wood County School District is a public school system in West Virginia, whose main offices are in Parkersburg WV, with a total of 27 schools, grades K – 12. NBSP conducted a telephone interview with Mrs. Beverly Blough, Director of Food Services for the district.

**NBSP:** Mrs. Blough, could you give us a brief statement describing your school district’s case history along with a summary of the issues facing the educational sector in which you’re operating?

**WCSD:** We participate in the Federal Government Child Nutrition programs. So, first and foremost, we are guided by Federal Government regulations and in order to receive the reimbursement for the meals that we serve, we have to carefully identify the students who are receiving the meals.

In the Child Nutrition program, some students will qualify to receive the meals free of charge or at a reduced price if they meet the income guidelines that the Federal Government has established. So, they [the Government] are telling us, and rightfully so, that if they reimburse us for a meal for a child that gets a free benefit, we must make sure we carefully identify that child.

In our county school district we have 27 schools, and on an annual basis, at the time we began looking at Biometrics, we were serving 1.8 million meals. That meant that 1.8 millions times, we had to positively identify a student at the point that they received their meal. So, there was a large volume of students that had to be identified. That was one issue. Over the years, the school district created a two-system method for identifying students. One method required the student to actually have a card that they would present with their numbers on it and a bar code that would be scanned. The second method was for our younger children to have a bar code that was on a sheet of paper along with all the other students in that particular group such as the classroom and we found out both methods were unreliable.

The students that were issued cards would lose them, deface them, counterfeit them and that was a constant problem. The bar-coded sheets, or rather forms with the children’s’ names on them, were another on-going problem to keep current because some of our schools have very transient student populations. We were not able to produce the bar-coded sheet for the classroom, like a classroom roster in our department … that had to be done by our Information Systems Department. We were able to produce the cards here, however, so, we had two systems going at the same time.

The other issue that really became a change agent for us was when the State of West Virginia made a move to standardize the student’s identification number throughout the State so that they would be more portable. Students often may change school districts and in order to make sure that their records followed them without getting any other records and important information lost, the State of West Virginia introduced a nine-digit Id number.
So we were in essence going from a four or five digit number to nine digits and some of our students -- particularly the older students, when they lost their lunch card, would verbally give their student Id number. Our concern was when we went from four or five digits to nine digits, our problems would increase. The students might not remember their number, and if they did remember, the staff would have to type in nine digits, which increased the potential for errors. Our goal is to always be accurate with those numbers so that our Federal reimbursement claims accurately reflects what occurred when we were serving the meals.

Those were some of the driving factors that made us look into another method and at the time which -- when I think about it was only five years ago, there weren’t a lot of biometrics used in student or children identification. It was something more of an adult type of tool, so to speak. So, I felt that we needed to have some other method for identifying students and it was brought to my attention that there was the possibility of using biometrics. That is basically how we began our journey into using biometrics for our application here in the school district.

NBSP: Thank you … that was very clear and concise. Were there any other competitive or economic reasons to induce you into the area of biometrics?

WCSD: The cost of maintaining the manual identification system was a factor. We had the cost of the plastic cards, and I tried various thicknesses of cards that a student could not bend and break. We tried a variety, including something more of a credit card weight. Then there was the cost of the equipment we used to produce the card, and the cost of the printers that printed the cards, the printing cartridges that included not only the ink but also materials that overlaid that ink so that it would not be rubbed off and could withstand the frequent scanning. The latter items became an ongoing expense because the number of students who lost cards.

NBSP: And you were able to document those costs in some way?

WCSD: Right, we just looked at what our purchases were. Also, we even tried to assess the student’s family’s cost because the parents bore the cost of repetitive replacements. That was, from a volume standpoint, too difficult to track. Also, if students were receiving free meal benefits, they did not get a lunch bill in which we could tag on the $1 or whatever charge. So, it became an un-wieldy system to try to recover the expenses of frequent replacements.

Looking at what systems were out in the industry, there were other methods, such as having the child enter their own ID number on a touch keypad. But that didn’t meet the criteria for what I felt was a good method for identifying students because we already knew that students would borrow each other’s lunch cards and there was no assurance that they would not again use someone else’s, number if they were to have to type in or key in their number.
Another method in use was photo ID type of method. There are software programs out there that would display the students’ photograph. The problem with that program is that on the first day of school you don’t have a photograph of the student. Often in schools that were trying to use photo IDs, the photos were not available from a photographer until October. If we were to adopt such a system, there would have been a number of drawbacks: 1) it would have required purchasing specialized equipment again, 2) it would have required going to all the schools within a very short time period, 3) it was not a system that would be up and running and available on the first day of school, and 4) it would have required provisions for ongoing photos for new children enrolling in the school. So, I didn’t feel that it was a good option.

The other consideration was that we already had our POS or Point of Service program that had been developed by our own school district programmer. So, we felt that we had a good product for recording the meals and the other information that we needed and I was not interested in going out and purchasing a brand new program and any other identification software.

In researching the different methods and the use of biometrics, I did a good deal of online research, and also spoke to a school district that had implemented a biometric program using fingerprint scanning. They purchased both the scanners, but also the POS system at a tremendous cost and that was something that I didn’t want to do because again, we were satisfied with the program we had. I just needed to have a better way to accurately identify the student and as we refer to it, just reduce the hassle factor.

NBSP: So, it sounds like you did a lot of research on alternative ways to make your system better or to solve the problems that you saw. Did you have to pull these together in any sort of formal documentation, in a sense, have quantitative data to sell the idea, get the money, or to go ahead and move forward into a biometric application?

WCSD: I did put together a presentation with some numbers for the Board of Education, in which I documented the cost of producing the cards. There were things that were difficult to quantify such as the non-tangible, non-material expenses as well, but we focused on the cost of the lunch cards and other issues from the food service standpoint. I did not quantify, for example, the cost of our information system staff to create the list for the elementary schools that had the bar codes on them. I just focused mostly on what the impact was for the food service department.

NBSP: Let’s move on a little bit into the implementation process. Once, let’s say, you had the go-ahead to move forward toward biometrics, did you develop a formal requirements document to give to vendors or integrators, saying these are the things that our identification system must do?

WCSD: No, I did not, because I was looking for a company that would provide just the identification software and hardware and particularly, a company that was providing it for a student population. The company I was dealing with at the time was the only company that was selling, a stand-alone offering five years ago. It doesn’t seem like a
long time, but there were no other companies that were selling in the school market as a stand-alone product, not tied to POS software. So, there just weren’t many choices except the one company we ended up purchasing from.

**NBSP:** Can you identify that company for us?

**WCSD:** identiMetrics. I feel very strongly about our choice because as I did my homework and asked questions, I learned that biometrics, historically, had been designed for adult identification and the difference between the adult and the child was primarily the size of the field that the scanner was reading. Additionally, the scanners that had been developed and created at that time, did not easily allow for the change of resolution that the scanner had to make in order to properly read the features of the fingerprint that they used to identify a child. They had to magnify that image and when you magnify, you have to maintain your resolution, which most scanners did not account for. It was a technical issue that this particular company recognized and embraced and developed software that would effectively do that.

So, they were really the first in the field, so to speak to have a program and product that could read prints ranging from the very small finger of a child in kindergarten all the way to the big high school senior football player whose thumb will cover the whole scanner. It is really was a broad range and thus difficult.

**NBSP:** I can imagine the technical challenge in that.

**WCSD:** Right, and in the last five years, their program has increasingly improved. It is an evolving part of the technology in scanning children’s fingers.

**NBSP:** Did you specify or address the issue of performance of this biometric identification device in terms of false match or false non-match?

**WCSD:** We didn’t specify any false match rate, but we have never had any issues with false reads.

**NBSP:** I am assuming that this is what we in the business call a “One to N” application.

**WCSD:** Yes.

**NBSP:** Did you specify in any sort of requirements document the training that would be required by the vendor, identiMetrics?

**WCSD:** Yes. We required that they be there for the initial training, but would also be available to us in the initial enrollment of students. That was not particularly required but that was a part of the service that they were providing to us after we purchased their product. So, they were actually working alongside of us to enroll students to make sure that we felt comfortable with the product.
NBSP: And now I assume, your internal staff from the school district has reached the level of confidence that you don’t need identiMetrics there to do that enrollment for you?

WCSD: That’s correct. In essence, they trained the trainer and I became the county trainer and so I have been able to train my staff in the enrollment process.

NBSP: Did you address legal issues before you implemented the biometric system, such as privacy considerations? Or did you thereafter have to develop a privacy policy, and what were the impacts of those policies that you had or developed?

WCSD: At the time that we began this, it was decided that the software would reside on the local school machine(s) [server?]. So, the privacy issue was addressed mainly by the fact that one school’s server had only the biometric information for that school. We knew that down the road, we would want to put that data on our county server, which then would give us a different need for privacy. The way we addressed it when we first implemented the program, was that access to the local school machines was already controlled and that privacy had already been addressed with our existing data access program where there were sign-on codes. Personnel had to have their own sign-on codes to access the server. We concluded therefore that the existing privacy policies and security procedures were adequate if computers in the school were on the school’s intranet.

In addition, identiMetrics felt very comfortable that if someone had been able to breach the computer or server, the biometric information stored there would be of no use to them [in attempting to obtain a fingerprint image], because there were no images. The image was converted to a series of the numbers [templates], and it would have taken an expert in the field of biometrics many, many hours to recreate an image of a fingerprint from the template. And then even if they could accomplish that, it would not rise to the level of say a forensic fingerprint. There were just not enough points on there that were recorded, so if someone could breach it, they still could not create a full fingerprint image.

NBSP: There was a statement in an article that I read about your biometric implementation that said, "The main ingredient to a successful biometric system may be to get parents on board early."

WCSD: Correct.

NBSP: There are laws banning biometrics in Iowa, and Illinois schools, and I understand Arizona's has a current bill in work that was apparently the result of parental fury when learning, after-the-fact about biometric implementations in schools. How did you address that issue before actually implementing your biometric system?

WCSD: I knew from my research– particularly from the other school officials I spoke with - what kind of reaction they got from parents, and what we could expect. So I was prepared that there would be some negative reaction. Presenting it to the school board and getting their support was a real critical issue. If parents were speaking to someone on
the school board or speaking to an administrator, they would understand what we were
doing and why we were doing it. But we also provided to the parent who objected to
biometrics, the option to sign a statement that says, "We want our children to opt out of
this program," and they understood that if they wanted to opt out, their child would be
required to bring some form of ID with them to lunch.

Also we thought there might be people in the area that had religious objections, and this
was our way of accommodating them and saying in essence, “We are not going to force
you. If you object to this you may opt out.” And considering the number of students, we
really have a very, very small number of people that have chosen not to allow their
children to be scanned.

**NBSP:** Do you still have a cash register operation in the event that people want to pay
money?

**WCSD:** Yes, yes, we do. So there are different choices for the parents, and we thought
that that was a good compromise all the way around and it's been very workable for us.

**NBSP:** Let's move on to the next and last subject and that's evaluation or implementation
of your process. How did you select the biometric what you might call modality or
technology that was best suited to your application? In other words, you must have
considered other forms of biometrics such as perhaps vascular biometrics, iris
recognition, perhaps voice recognition.

**WCSD:** It was something that best fitted the environment that we operate in. You
mentioned voice recognition, we work in a very loud environment at times either with
equipment or just children and so trying to accomplish something like that would not be
feasible.

We were trying to do something that would be very quick and easy for any child and
would allow them to still have one hand on a tray and be able to present a finger for
identification. When you look at the process, the student simply presents his or her finger.
If we were to do some sort of eye scan, the student would have to get close to a piece of
equipment. You also have the fear-factor with children that, is this going to hurt, or is it
almost too sci-fi for some children. Some of the other technologies seemed a little bit too
invasive to their space so to speak, but it was easy to stick a finger out and put it down on
the reader. We didn't have to worry about the child being afraid of it because when we
went through in the normal process they saw that it didn't hurt, you just put your finger
there. So it had the least impact on the child and it was something again that was easy to
do. We approached it with the kids from the standpoint of you always are going to have
your finger with you - you can't leave it at home.

During the enrollment process we read both the right hand and the left hand index finger,
so even children who had a band-aid on one finger would have a back-up biometric
capability. If they didn't have a usable finger, we used the thumb. And in all of the
10,000 children that we have enrolled, we only had one situation where a child could not
enroll because, bless her heart, she had no arms and had no digits. We could have possibly done a toe-read for her, but that means she would have to take her shoes and socks off and we just felt like that was not a necessary thing to do.

**NBSP:** That’s a nice transition to the next issue and that is how did you train the user base, in this case your kids -- how did you structure it and how did it go?

**WCSD:** We trained as we did the enrolment process, by taking them in small groups, and (depending on the school and the setup), go into an actual classroom and set up our laptop computers. We show them what the scanner looks like, how to place their finger and have them do one finger three times on one hand and one finger three times on the other hand. So we walk them through the process. When they get up and see how it's done, we coach them, if they need to move their finger. We use the same process today in any large group enrollment. For example, right now we are enrolling our fifth grade students who are moving up into the sixth grade, which is now in our middle-school structure.

One other thing that identiMetrics has now developed which I have not had the opportunity to use, is an end-user video which actually features a child doing it. So that's another tool that I have available to use with children to say, here is what’s involved: It doesn’t hurt, your hair doesn't get curly, there is no electrical shock. We try to give the kids a kind of a fun approach to it so that they aren't scared by it or think that something is going to zap them or bite them. Unfortunately, our children are exposed to a lot of things on television and they come with wild imagination. So we try to make them feel comfortable that this is quick and easy. Then, when they see how easy it is and the fact that they can observe their fellow students using it, it, then it becomes just a nonchalant process and it's not a big deal for them.

**NBSP:** Can you assess the impact of a biometric system on operational, financial and personnel operations?

**WCSD:** In the personnel area, it really didn't impact us at all. It has not required any additional personnel. We have been very fortunate that it really did not put a demand on us. Financially, we obviously don't have the expense of the mass production printing cards at the beginning of the year. We don't have the cost of the special cartridges to produce the card, so that expense has been pretty much wiped off our budget.

Operationally, one of the key lessons learned was that if we are able to enroll the students who are going into our secondary schools or middle-schools, the year before they actually go there, such as this time of year, then that makes the start of school much easier. In the past we waited until school started before enrolling the children and were running from school to school to school. Now this way it's easier for us to do it over a time period of several weeks. I have a supervisor who schedules the schools and, depending on the number of the students in the school, we can go out with one or two people, or working with a large group, I have trained my secretary to go or to help so we can do four people and get in and out quickly.
The other thing we have learned is to make expectations known to the school staff when we are enrolling students. We need to specify to them our space needs. We need to make sure that we have electrical outlets to power the laptops. I don't want to rely on our laptop batteries always lasting. We need to be presented with all of the students at one time. We need someone from the school there to supervise the students, because we are focusing on the students we are enrolling and training and if the rest of the students who are waiting are running around getting in trouble then we become distracted.

In regard to the last point, I will share a funny story with you. When we do the enrolment, the scanner will give an audible sound, a beep so that the student knows that it read their digit. We were in a school in a cafeteria and we had most of the students of that grade level, and one of the teachers was trying to entertain them. So she did entertainment by having them clap loudly in a rhythmic fashion and that was a disaster, because we couldn't hear a thing.

So you learn to identify to the school the kind of setup we need. For example if we are going to all work in the same area; we need to be separated somewhat so that the student that's working with me is not thinking that the beep he hears from the next student is for him. So we try to isolate ourselves a little bit and we become very flexible with the school, we work within what they have, and thus have enrolled students in cafeterias, classrooms, hallways, wherever …. we are flexible.

**NBSP:** How many scanners do you have in your school district?

**WCSD:** Every one of the secondary schools will have one to two scanners depending on how many computers that they have at their [food service] line. High schools would typically have four.

**NBSP:** How many schools did you say you had in a district?

**WCSD:** We have 27 schools. Now, we are not integrated in the elementary. That's moved a little slower than what I would have liked to have done. The expectation initially for the Principals was that this was going to be very fast, and initially the scanning did not make things faster than the other methods. It was more accurate, but it took the students time to know where to place their finger, remember to wipe their hands off, etc. The first generation of scanners/readers were sensitive to dampness or to water, so if the child had sweaty palms or grabbed a bottle of milk that was wet it required extra time. The newer generation of scanners can read a wet fingerprint without hesitation. So they do begin to be faster as they go along but initially the Principals felt that it took too long. Well, it really didn't, they just had the expectation that it was going to be much faster.

**NBSP:** I am going to read a kind of an artificial list of some of the phases or aspects of typical biometric projects, and just have you react in terms of did you think these phases in your case went well.

**WCSD:** Ok
NBSP: Preliminary Planning Phase, Development and Presentation of the Business case, and selling a project to management?

WCSD: That went very well.

NBSP: Testing, pilot test, or installation?

WCSD: That went well, we did well, but at the same time learned.

NBSP: Training, did you feel that went well?

WCSD: Yes.

NBSP: Managing change within the organization?

WCSD: I would say that went pretty well.

NBSP: Cut-over or initial implementation?

WCSD: That went well.

NBSP: And finally, follow-up and problem resolution?

WCSD: That's been good. I temper my expectations with my knowledge about the evolution of child-focused biometrics. It is an evolving process and every reader gets better with improvements on a yearly basis. So, is it the top-of-the-line, 100% perfect? No, because I am always reaching and stretching and they are as well. But I am very pleased with the progress that I see that's being made with child biometrics.

NBSP: I think that's a very realistic perspective. People often times expect it to be the magic solution to everything and instantly be perfect and they don't factor in the evolutionary aspects of it.

WCSD: And I have got to say on a personal side, I have found myself to be fascinated by the subject, read a lot on it, and understand the software program and am becoming kind of a computer nerd as a result of this.

NBSP: Let's look at the other side of the story, were there aspects of the project that did not go well or did not go as well as you would like?

WCSD: We had hoped to have had the identiMetrics program with the database on a county server. That would have allowed for the portability of the data, at least within the county. Right now, when a student progresses to another school, I actually have to physically go out there, copy the data from one school, then transport that data and install it in the gaining school. That process would not be necessary if we had the program on a
A couple of years ago, the Child Nutrition Program in the state of West Virginia announced that they had made a commitment to purchase a POS program for all schools in the state. So at that time when I was ready to say in our own district, I want to get this biometric identification program on our county server, I stopped. I knew that within the year (now it's two years - it's a little slower process for the state to do this), that I will have a statewide POS, I will address the identification issue at the time that this occurs. So the one regret that I have is that we had not been able to get a more centralized database in administration of the biometric program. So right now I have to go physically from school to school to transfer information.

**NBSP:** Did anybody ever ask you for a formal after-action analysis and to provide lessons learned to them? Anybody on the board of education for example?

**WCSD:** Not in our particular board. I have been able to do that in talking to other school districts and other school district administrators, I actually went to another school district in the state of West Virginia and talked to them about our experiences. So that's something that I had not done here locally, but I took that information and went somewhere else with it. I give them the real honest story ... you know ... here's what's involved. I don't sugar coat anything. I tell them, you will be challenged by some people in the community and here is how we addressed this situation.

**NBSP:** A couple of things occurred to me as I was reviewing the article this morning. It said something about the fact that parents can now go online and find out what their children actually ate. Is that an ability to view records on a daily basis, weekly basis?

**WCSD:** That is not something that we have here in our school district. There are software programs that school districts can purchase that become part of their point of service in states that have a la carte meal programs. West Virginia is one of two states in the country that do not do a la carte business. Children have to purchase what we define as a reimbursable meal. In the application you are referring to, for example in the State of Ohio, a child could go into the lunch room and buy just as if they were walking into a fast food restaurant. They could pick and choose what they wanted to eat. In those schools the software programs record whatever is entered on the cash register and converts that information into a record so that the parent can access that and see, well gee, Johnny ate two servings of French fries today and five cookies and something along that line. So it is a service that some school districts offer.

**NBSP:** I am going to make an assumption here that the program that identiMetrics gave you has some algorithms in it to prevent repeaters from coming through the line or lines for the same meal.

**WCSD:** The identiMetrics does not, but our point of service program does. identiMetrics is only identifying whose fingers are on that scanner. So, if the child comes back again, our point of service system says, we have already recorded a meal for this student ID. So, that is built in, as there is a federal requirement again for Child Nutrition Program that you identify when a child gets more than one meal. It doesn’t prevent them, but it records
it in a different meal classification. It becomes a second meal and second meals do not receive any Federal reimbursement money.

**NBSP:** Sort of puts the onus on you to find out if Johnny did that on a particular day you have to correct that issue manually?

**WCSD:** We do allow children to charge the first meal and then pay cash for the second meal or vice versa. They can’t charge two meals and that is more of a county level and state level recommendation. If you allow a child to charge five meals and they are not paying their bills, then you are further in debt than you were if they only charged one meal. So, our system is saying, you can charge a meal and pay cash for the other, whichever way they want to do it. We do have some children that will get three or four meals and can charge for one and pay cash for three of them.

**NBSP:** Well, I’ll tell you, Ms. Blough, you have been extremely helpful and we appreciate it very much.

**WCSD:** It is always fun to share this information because I think it has just been fantastic for us.

**NBSP:** Well, I come from the user community myself, not the technical vendors and you have an excellent user’s perspective. I think you have looked at the right issues, you have done the right things and as a result, I think the program has moved the school district forward and so I doubly appreciate our conversation because of that perspective that you have.

**WCSD:** Well, thank you very much for asking me to participate with you. I appreciate the opportunity as well.
NBSP conducted a telephone interview with Mr. Rob Durwood, Director of Information Technology, and currently Director of Technical Programs for CATSA.

NBSP: Before we get into the actual details of the application, maybe you could just spend a few minutes giving a brief description of your industry and your agency’s position within that industry.

CATSA: Sure. CATSA is the Canadian Air Transport Security Authority. We were created right after 9/11 as the Government of Canada’s agency dedicated to aviation security. We report to our Parliament through the Minister of Transport. We’re governed by a Board of Directors, have a President, and Vice-presidents and Directors at my level. Part of our mandate is to manage the Restricted Area Identity Card (RAIC) program. We’re responsible for screening at 89 designated airports and for the RAIC program at the 29 largest airports, which handle roughly 92% of all the passenger traffic. The RAIC program is within the air terminal buildings now and moving forward, we’re looking to go outside of the air terminal buildings into the rest of the restricted areas and the perimeter fence around the airports. Our main areas of responsibility are 1) screening of passengers, 2) screening of baggage, and 3) control of non-passengers within the restricted area.

NBSP: We do have a bit of information from your presentation and it looks like you screened about 40 million passengers a year and 60 million pieces of luggage. It looks like you have 5,500 or more contract screening officers – is that a part of this?

CATSA: That’s correct. Our model is different from the TSA’s in the States. Your TSA uses federal employees, and we contract out that responsibility to different screening companies. Across the country we have 10 different companies handling different regions.

NBSP: You say that you were formed after 9/11?

CATSA: April 2002.

NBSP: As you started getting a sense of what your mission was, what led you to research biometrics with respect to increasing the security in the airport area?

CATSA: Well that’s a good question. Prior to CATSA, we had something called a Canada Pass System at the airports across the country and there were no biometrics on that card. Nor was there much restrictiveness in issuing the card; it was sort a trophy card and everybody had one and so it lost its original essence. Our Minister of Transport decided November 2002, that we were to develop a card with biometrics embedded in it, and that CATSA should take the lead.

CATSA formed working groups that interacted with the different stakeholders at the airports, other government agencies, the federal government, and Transport Canada, and
they did a lot of work and research on biometrics and what type of biometrics to use. I had been at CATSA since October 2002, but I didn’t get involved in this program until 2004. By then the iris and the fingerprint had been selected as the biometrics of choice. In exploring the background of the selection process, I learned that during this research and selection facial recognition was felt to be less accurate than fingerprint and iris technology. Certainly at the time, vascular had not been researched well and wasn’t a viable option. It looks like it has gained a little ground recently but it wasn’t even on the radar then, and the working groups chose fingerprints and iris.

**NBSP:** Can you explain what Transport Canada is?

**CATSA:** Sure, it’s the department within the Canadian government that is responsible for developing regulations, policies and services related to transportation in Canada. And unlike the TSA, in Canada the regulator (Transport Canada) is separate from the operator (CATSA).

**NBSP:** Thank you. Now getting back to your last point. Bottom line …. security was the key driver in the formation of your agency and the selection of the biometrics to further secure the airports? I mean it’s not like it was in the private sector where there are competitive factors or economic factors – it was primarily security.

**CATSA:** That’s a fair statement

**NBSP:** All right, so when you started the process – how did it start? Was there a vulnerability assessment done at the primary airports? Is that how you tried to define what the level of vulnerability was and what level of security that you would need to counteract that?

**CATSA:** No, not per se. Actually, we took our marching orders from our regulator, Transport Canada and specifically it was the Minister of Transport, who decided that this was going to happen. And he specified the 29 airports where the RAIC program would be implemented.

**NBSP:** Are the airports in Canada operated by the Canadian Federal government or are they operated by the province?

**CATSA:** Historically, they have been operated by the Federal government but probably 15 years ago they were privatized. Most if not all of the 89 designated airports we deal with are now not-for-profit corporations, guided by a local board of directors and generate revenue from their commercial interests.

**NBSP:** Okay. So they would obviously be concerned about the potential cost.

**CATSA:** Well, the first question the airports asked was “Why do we have to do this and how much is it going to cost?” So, it was obviously going to be a challenging process to
work with the airports to implement such a new, radically different, and very expensive security program.

**NBSP:** Okay, let’s move on. Can you help us understand, once you got the mandate, how you defined the requirements of the program? Such as operational requirements, functional requirements, legal requirements in terms of privacy concerns or what have you?

**CATSA:** Absolutely. Let’s begin with privacy. We took that one on first and met with the Office of the Privacy Commissioner prior to launching into all the other requirements because the privacy issues were fairly straightforward and codified.

In terms of the other more technically and operationally oriented requirements, they were going to vary greatly according to the individual airports. We had to identify somebody who was willing to work with us, point one. And we had a couple of airports that were willing to do that – you have to realize, by the way, that this was the first time ever that we would have two biometrics on a single card and we didn’t realize the technical impact of that at that time. We just sort of looked at it as a project that needed to be done, and tried to figure out the best way to do it.

Communication was a major, major, major portion of it, so we began by visiting the airports and having conversations with airport personnel. We made presentations, met with groups, and had one-on-ones at each of these airports. They wanted to know how was this going to impact their ability to make money, their ability to survive and, especially, their ability to maintain their distinctive relationship with Transport Canada, which comes in and says “The regulations require that you do this, this, this and this.”

We began with their IT folks. In hindsight, we should have involved senior management and made sure they had regular updates. We sent protocol updates to specific people, but we could have spread that out a bit more.

We also spoke to the security advisers and the security personnel at the airports and worked with those people. And they were our conduit into their organization. So where we had a relatively good relationship, things went well, while others took a little more time. We were able to make progress by being straightforward, genuine and honest, and they responded to that.

And most importantly we paid for all the equipment. So, although they did have some project management costs and some other expenses, CATSA paid for probably 95% to 98% of the project. And when we sat down and showed them what to do and they saw that it did work, we began to get some converts and make some progress.

We knew from the outset that we had to show some value in return for their support – in this case, their hard work, cooperation and “sweat-equity”. So when we put the prototype together we made sure that it worked well, each and every time we demonstrated it and that it integrated easily into their current existing Pass systems. We were honest and
admitted that it might be a bit of a pain, but we tried to show them that the process is new, but the results would be even better. We demonstrated that their security systems would be stronger and less vulnerable.

NBSP: Well I guess with you paying for all the equipment that pretty much resolved the economic concerns they may have then?

CATSA: It did. And they also realized how smart it was get on board early. When we brought in the equipment, if we ran into issues at that gate it was offset by the fact that we were able to find the bugs, address their concerns, work through different configurations and situations responsively – almost like having a team of designers and engineers custom building something to their specifications.

NBSP: Any operational or functional requirements that you had to take into consideration?

CATSA: I think the main objective was to enhance their current systems – because they all had Pass systems and they all work with Transport Canada to get those security clearances – that didn’t change. The issuing of the card changed and the enrollment and the accreditation portion changed a bit and that’s where we needed to sit down with them and work with them and provide guidance etc., etc. Then we had a couple of pilot sites at large and small airports and that proved extremely beneficial. We were able to test things out, look at any glitches, fix the system and move forward.

NBSP: Okay. Was biometrics considered as the primarily technology right from the beginning of the program or were smart cards looked at?

CATSA: Biometrics was focused on by the Minister right out the door.

NBSP: Could you comment on some of processes that you went through to land on the modality that you used - finger and iris. Did you evaluate others or what led you to land on those two?

CATSA: As I mentioned before, I wasn’t part of that early process, but by the time I arrived, the working groups had completed the formal analysis. They considered every modality that was viable at that time and then at the end of the day they agreed on the fingerprint and iris. A number of our people here in senior management have a police background with the RCMP and local police, and were very familiar with the fingerprint side of the house.

NBSP: This system with biometrics went online back around 2004?

CATSA: Yes.

NBSP: So iris was certainly not as pervasive as it is at today, five years later. So you were sort of ahead of the curve on that. Once you decided on the modalities of finger and
iris, do you have any idea of what kind of a selection process was used to determine who
the provider would be? Which fingerprint vendor did you select, which iris vendor did
you select?

**CATSA:** I can guarantee that there was a competitive process with multiple vendors
submitting specification-compliant bids. On the integration side there was a formal
competitive process where an integrator won and helped us with that.

**NBSP:** Describe the integration process. You’re talking integrating the biometrics into
the card?

**CATSA:** A company called Unicom, which is no longer with us, had teamed up with
IBM. They responded to the RFP and won the contract to start this process and worked
with us to get going on it.

**NBSP:** Can you tell us all the providers for both your iris and fingerprint devices?

**CATSA:** LG for the iris and Cross Match for the fingerprint portion and HID for our
card.

**NBSP:** All right let’s talk about benefits. How would you describe the most quantifiable
benefits and what would be some of the non-quantifiable or ad hoc type of benefits?

**CATSA:** From CATSA’s perspective I think the airports are the ones who most clearly
benefited from the new card, and the most singular benefit is, without a doubt, security.
As a byproduct, it helped them to clean up their database and their old system. What I
mean is, the new RAIC program ended the card-sharing era. For example, before this
system was in place, when somebody had to go to the bathroom they could borrow
someone else’s card to go. Now they have to have their own card, so it cut down on that
kind of stuff. It seems kind of minor, I know, but it goes to show you the vulnerability of
the Pass cards. And on the security side of the house, it reinforced what we had been
saying about enhanced security with biometrics. People being what they are, would try to
spoof the old system – not with things that people may try to spoof biometrics with – but
just by using somebody else’s card. But the integration of the biometric card into their
regular Pass system has provided enhanced security, as has the integration of the RAIC
into the rest of their security policies and those, I think, were the best benefits.

**NBSP:** Just to make sure that we understand and we’re not trying to be obtuse but –
explain the enrollment process to me.

**CATSA:** What happens is an airport would sponsor an individual and he or she would
apply for a transport security clearance that would allow the individual unescorted access
to restricted areas. By way of background, you cannot go into a restricted area of an
airport – be you a ramp worker or even a person from McDonald’s – without an escort.
To gain that clearance, you naturally have to fill out a lot paperwork, which is sent to
Transport Canada. Transport Canada would process this, and if all is well, the security
clearance is granted and the airport and CATSA are notified. At that point, the individual at the airport is eligible to enroll in the RAIC system. Before the physical enrollment, however, the RAIC system at the airport contacts our main CATSA database that checks and validates that there is a security clearance for a person X. and the physical part of the enrollment process would continue at the airport. They’ll be set to go within 10 minutes. That was one of our requirements actually, that the enrollment time, including both the clearance verification and the physical enrollment, would be under 10 minutes, on average.

**NBSP:** I’d like to think it includes the capture iris image and the fingerprint image?

**CATSA:** Yes sir it starts at the same time.

**NBSP:** Now are those images then integrated into the card?

**CATSA:** They're made into a template and the template is put on the card. Then when you go to the door, you insert the card and give your biometric sample, which is compared to what is on the card, and you’re in.

**NBSP:** Given the difficulty with some of the airports early on in terms of cost or as you say the sweat-equity that they have to put in to program, do you feel that they believe that all of that was worth it to now? Do you get feedback from some of the airport operators in terms of their reaction to the system?

**CATSA:** Nowadays, yes. To put it in context and be fair, most of the airports – especially those we had good relations with – supported the program. But I also understand why there were other ones that were a bit reluctant because there was no official deadline when the card was to go into effect.

**NBSP:** Right.

**CATSA:** So what happened to finally get these folks totally on board was, in December 2007, we got Transport Canada to say, “Okay that’s it. At the end of December this card goes into effect.” And when that happened, boom! Then everybody sort of got in line. While the people who’d been working with us were far ahead, there were a couple of airports, which experienced a bit of pain in that final month. But now that it’s done and it’s in, it’s an integral part of what they do every day.

**NBSP:** You mentioned Unicom earlier as an integrator that was with you during the initial install. Did they work with all of the airports with the installation of the process?

**CATSA:** Yes sir.

**NBSP:** Now the airports themselves have their own personnel that maintain the systems?
CATSA: No that’s still a CATSA responsibility. We work with the airports. Right now as a matter of fact, we’re in the process of redoing the application. When it was originally done it was in a language that was fixed at that point, and now we’re making it more of a robust application and we’re working with the airports and taking their suggestions on how we can improve the system a little bit more for them. Once they have some input, they can see the improvements right away and that makes things even better this time around.

NBSP: So their receptivity is higher than it was way back then?

CATSA: Yes for sure.

NBSP: I wonder if we could get a little bit of clarification. You talked about the enrollment and I think I understand that process. When an individual is now enrolled and has his card and he approaches a portal into a restricted area, does he insert the card somewhere and then give a fingerprint or an iris which is then compared against the information on the card?

CATSA: Exactly correct.

NBSP: So there’s no database at each portal?

CATSA: No and that was a conscious decision on our part to design the infrastructure that way. I didn’t want to be at the mercy of a network where there would be constant traffic going back and forth and if there was problem with the link, that area would be down. So our decision was to put that information on the card. During the enrollment process there certainly needs to be some kind of activity but after that there was no need for a huge and constant flow of electronic traffic between Ottawa and the rest of the country on that side of the house.

NBSP: It’s also a pretty good approach to address privacy issues and concerns that people have about giving their biometric and all of their data and having that controlled by someone else when it’s on the card they are controlling their own information all the time.

CATSA: That’s true. I didn’t finish up on the privacy question that came up earlier. And I’ll take two seconds to explain.

NBSP: Certainly

CATSA: Transport Canada has the main database with all of the security information on an individual. On our CATSA database we have only a couple of numbers. We have expiry, the date of the security documents, the Document Clearance (DC) number and a couple of other minor digits. We do not have names of individuals. We cannot reverse engineer if we got a RIN number (a RAIC Identification Number). We don’t have any of
that information. All the airport does is check with us to see if the DC number is legitimate and it ties into the same number that the individual has at the airport.

Given that background, I didn’t think that we had any personal data on our database. The Transport Canada privacy people disagreed with me because the document control number was the same on all three databases. We tried to impress upon the privacy office that CATSA doesn’t hold any data, Transport Canada does. They always have and it’s the airports’ data because the airports initiate these things, not us. So we said “Okay, how we handle this basically is that when the template is created at the airport, no information is kept on the airport database.” So that template is created, put on the card and that’s put on our database but not the airport’s. The reason it’s put on ours is because one of the checks done when the individual is enrolled is to see if those fingerprints exist already. So they check our database to see if they exist. If the answer is no, which is great, they go ahead and proceed with the enrollment. So that was, and is, how we protect our data, and that allowed us to continue.

**NBSP:** On your database there is no personal or biographic information?

**CATSA:** There are no names, no data other than the Document Control number.

**NBSP:** Now when an individual goes into a restricted area do they always match both the fingerprint and the iris?

**CATSA:** No, it’s either, or.

**NBSP:** Okay. We appreciate the explanation very much, but your last response makes me wonder what factors bear on what types of reader you put at a given door.

**CATSA:** That’s a very good question. Basically, the answer to your question is need. For example, I thought that the irises would be cool and awesome, but the pilots didn’t like them at all. They had problems with putting their eye near the device; they were afraid etc., etc., etc. They thought there might be some kind of damage. So they preferred fingerprints. That was one of the issues we had to deal with. So essentially we gave them a choice, because this was new at the time. We said, “Well, we don’t have enough money to give everybody an iris and a fingerprint reader, so why don’t you pick one, and if in 3 or 6 months we find that through the rhythm of the workload that’s going on that there’s a better way to do it, or a different reader, then we’ll be happy to change.” So that was okay.

A number of airports wanted two devices at every portal to start with and, again, we worked with them. Our rule was generally not to do that, but if they gave us a good reason we’d consider it. One of them was handicap access. There were a couple of people at airports who were in wheelchairs and as soon as we found that out we immediately went over and gave them a second reader at the appropriate height level.
**NBSP:** One other question on the process before we get into some of the training that may have taken place. You’ve mentioned that in the CATSA database all you keep would be the biometric template and the document control number and that’s to check in case anyone being enrolled in an airport has already been enrolled.

**CATSA:** That’s part of it. The other part is document control. The TSC - Transportation Security Clearance - has a Document Control number, and nobody can get into a restricted area without that number (and that’s from Transport Canada) So when the airport requests that number from Transport Canada and it’s granted, a valid number goes to the airport and it also goes to us in our database so that we can match when the airport enrolls. Because if we didn’t have that {DC number}, the airport could enroll anybody they want … without any auditing, or checks and balances.

**NBSP:** Oh okay I see what you’re saying. So they submit the template along with the document control number to you. You make sure that the document control number matches the one that you already have.

**CATSA:** Essentially, yes.

**NBSP:** Okay. Is there any case where an individual would be enrolled in an airport and you would already have their biometric in your database?

**CATSA:** No.

**NBSP:** Let me ask this question now. We’ve talked about the airports themselves and the costs and the sweat-equity … what about the users? What about all the people who were going to be enrolled into the RAIC card program? How did they react with their training ahead of time? How was all of it explained to them? Was there any pushback?

**CATSA:** We worked with the airports – but, again, we were very, very careful not to interfere with any of their day-to-day business. The Pass control office and the Pass control process procedures were on-going well before CATSA. That was a regular airport occurrence. What we did was to enhance the security of that Pass process. We worked with the airports but essentially, they manage their own people and work load. Where we ran into pushback was when a couple of airports waited a little too long to start processing these new cards and when the deadline came about there was a big rush in the last couple of months to get those people through. So we had to have a different number of enrollment stations and then monitor those situations very closely.

**NBSP:** The level of training of and the degree of training and the timing of it varied by airport to airport?

**CATSA:** Right.

**NBSP:** Okay.
CATSA: Again, it was our responsibility to go out and train them. Once everything was deployed I sort of sat back and said “Great”. But it didn’t take long for me to realize that we had to have constant communication with them. There was always some degree of turnover in their Pass offices, and if 2 or 3 of them left with their knowledge, people wouldn’t get the proper training. We realized that we needed to continue to provide training although technically it was an airport responsibility. We tried to work together with the airports on this.

NBSP: And after all of the users had been enrolled did it become sort of like second nature to them and there was no problem with it?

CATSA: Yeah.

NBSP: Well we’ve talked about some of the benefits you accrued, primarily the ones of the increased security aspects of the airport. Where there any surprises along the way that as you were going into process and doing the install and rolling it out, that you had not anticipated and would do differently now?

CATSA: Probably a ton of them because this was the first time we had done anything like this; more so at the airports. What kinds of surprises are you talking about? On the behavioral side, or the biometrics or?

NBSP: Primarily related to the biometric technology in terms of the roll out or the enrollment, the reactions of people that you just hadn’t anticipated or –

CATSA: Many Asian women turned out to be very difficult to enroll in a fingerprint system because they had tiny hands. Elderly people had some difficulty because their skin tended to be dry, which we tried to overcome with the use of emollients. A lot people were afraid of iris at first until we put out communications explaining that it’s just taking a photograph of your eye – there are no laser beams and no zapping that’s going on. So gradually they understood that. So, I was a little surprised by those things.

What I found was that people needed to see a person to communicate with each other. We would put out bulletins and everything else and think “Yeah that’s cool.” But unless people read the bulletins and flyers, etc., it’s not very cool at all. So we found the personal touch saved a ton of time. Any amount of money spent visiting the various airports was money well spent.

We also found people with a good IT program at the airports were the best, because they weren’t afraid and when we got right to it, being afraid of the new technology is what I’m talking about. For example, we had to deal with some union, the teamster’s union, and explain our situation. We had to get a hold of the D&B report to document for the union that the iris readers would not harm anybody. Once everything was in, and they could see there’s some value to it, then they sort of – I won’t say embraced it totally, but they were able to work with it with no problem and it goes from there.
All right. Let’s move on to lessons learned – I know we’ve touched on it a bit but maybe we have to look it this way. What aspects of the project do you think went the smoothest, went really, really well and what aspects of the project caused you some problems or issues?

CATSA: The communications were very good, but I think that we could have done a better job on the applications side of the house. I think we could have done a better job with some training, and then validating that the training they received was adequate. We certainly made sure that everybody was trained but I think we could have done a better job by going back and saying, “Hey, do you have any more questions?” We sort of assumed that everyone would find it very straightforward because we did and we’d been doing it for X amount of time. We didn’t take into account, as much as we should have, the vagaries of the individuals that were using the systems. So I think that was one.

I think we did a really good job putting the two biometrics on the one card with the technology that we had at that time. And that process was good and the lesson we learned is that both of those – the fingerprint and the iris were pretty good – fingerprint obviously has been around for a lot longer, but it was the first time that those two had been put together from what I understand. They were two good technologies, where one wasn’t brand new with a whole bunch of difficulty with the technology itself, so I think that was plus.

So that’s the short answer to lessons learned.

NBSP: Thank you for your time Mr. Durwood.

CATSA: You’re very welcome.
MASTER SUMMARY OF INTERVIEWS

Following is a summary of responses to the NBSP interviews. The responses below, however, have been edited from the preceding case studies for brevity and clarity.

Also, many details applicable to individual implementations were omitted from this summary. Readers are encouraged to refer to the individual case studies for such additional information

SUMMARY:

NBSP: What economic, security or competitive factors lead you to research biometrics as a possible solution?

ATECH: ATECH applied our biometrics expertise according to the customer’s requirements as specified in the contract. The Automated Passenger and Vehicle Systems were initiated by the Hong Kong Government to improve the throughput rates, efficiency and security at border control points.

BCHS: We had a number of patients who indicated to us that they were becoming uneasy giving personal demographic information, such as social security numbers, when they are in waiting rooms with other patients. And they were concerned with how that information was used.

The second thing is we had begun installation of a very large electronic medical record project, and as a part of that project we would be gathering a lot of data and storing it for use when the patient comes in to any of our facilities. It would be used to give us a head start on the patient’s history – allergies, last lab results, x-ray results of things that would need to be immediately available to a care giver who would be treating that patient.

We also knew that sometimes it is hard to correctly identify patients when they enter our facilities. They may be coming into an emergency room and they might not be able to come up with their social security number and may seem confused or be unconscious. So we were looking for a way to identify all patients quickly and accurately.

CATSA: Prior to CATSA, we had something called a Canada Pass System at the airports across the country and there were no biometrics on that card. Nor was there much restrictiveness in issuing the card; it was sort a trophy card and everybody had one and so it lost its original essence. Our Minister of Transport decided November 2002, that we were to develop a card with biometrics embedded in it, and that CATSA should take the lead.

PAMC: The pressure to increase productivity and protect patient data is an ongoing challenge for healthcare.
The abundance of on-line information available to clinicians today ultimately improves productivity and potentially provides a competitive advantage in the market. But, facilitating fast and secure access to that information – without security policy violations such as writing down or sharing passwords - can be complex and daunting.

Further complicating matters, strict regulations like the Health Insurance Portability and Accountability Act (HIPAA) were put in place to improve and protect patient information. Under these regulations, Parkview was challenged to both protect patient information and at the same time, securely provide clinical staff the ability to walk up to any workstation and log into the network. They needed real-time access to applications and information that would enable them to provide timely care and service to patients.

A biometric solution could also take care of my security issues; 1) they never do log off, and 2) how do I make sure they are not sharing their passwords?

Parkview discovered that integrating finger biometrics with single sign-on (SSO) was the answer. The SSO technology allows each user to sign on to all applications using a single password. By incorporating finger biometric scanning into the solution, Parkview could enable each doctor or nurse to log on to any PC at the facility with a single fingertip swipe.

**Pearson VUE:** We began utilizing fingerprint-based biometric technology in our high-end Pearson Professional Centers in 2001 as a means to ensure test integrity and to enhance the candidate management workflow. The primary benefit has been to deter and detect attempts at test taker impersonation, where someone hires another person (also known as a ‘proxy’) to take a test for them.

Because we have a strong interest in ensuring that candidates can only test under one identity, biometric identity management (coupled with stringent procedures for verification of original identity documents) has been an essential part of the Pearson VUE workflow for years. No other technology could be realistically used in place of biometrics for robust candidate verification and identification.

**TCU:** Tech CU used to rely on traditional forms of authentication such as drivers’ licenses and passports when members visited branch tellers and conducted account-specific transactions. Branches also had on file cards with members’ signatures, called signature cards, which tellers compared with the signatures of individuals visiting a branch to identify them. Not only was this manual process prone to human error, but a signature card was only held at one branch, so if an individual visited another branch, that branch would have to request the signature card to be faxed from the original branch, a process that could take up to 10 minutes. Later Tech CU imaged all signature cards so that they could be accessed electronically, but comparison by teller still took up to one minute.

Tech CU’s Delivery Systems Division, led by SVP Mike Luckin and R&D Manager Barbara Cure, needed to implement an alternate method of identification at its branches.
in order to authenticate members more quickly and accurately, especially given the growing concern over identity theft and fraud. The new system also needed to provide members with a better customer experience.

**Union Pacific:** Well, they considered a variety of biometrics to automate their work gang time and attendance record keeping, and they were primarily concerned with eliminating worker fraud and leveraging their investment in workforce optimization.

**WCSD:** The students that were issued cards would lose them, deface them, counterfeit them and that was a constant problem. The bar-coded sheets, or rather forms, with the children’s’ names on them were another on-going problem to keep current because some of our schools have very transient student populations. We were not able to produce the bar-coded sheet for the classroom, like a classroom roster, in our department … that had to be done by our Information Systems Department. We were able to produce the cards here, however, so, we had two systems going at the same time.

The other issue that really became a change agent for us was when the State of West Virginia made a move to standardize the student’s identification number throughout the State so that they would be more portable. Students often may change school districts and in order to make sure that their records followed them without getting any other records and important information lost, the State of West Virginia introduced a nine-digit ID number.

So we were in essence going from a four or five digit number to nine digits and some of our students -- particularly the older students, when they lost their lunch card, would verbally give their student ID number. Our concern was when we went from four or five digits to nine digits, our problems would increase. The students might not remember their number, and if they did remember, the staff would have to type in nine digits, which increased the potential for errors.

The cost of maintaining the manual identification system was a factor. We had the cost of the plastic cards, and I tried various thicknesses of cards that a student could not bend and break. We tried a variety, including something more of a credit card weight. Then there was the cost of the equipment we used to produce the card, and the cost of the printers that printed the cards, the printing cartridges which included not only the ink but materials that overlaid that ink so that it would not be rubbed off and could withstand the frequent scanning. The latter items became an ongoing expense because the number of students who lost cards.

Another consideration was that we already had our POS or Point of Service program that had been developed by our own school district programmer. So, we felt that we had a good product for recording the meals and the other information that we needed and I was not interested in going out and purchasing a brand new program and any other identification software.

In researching the different methods and the use of biometrics, I did a good deal of online research, and also spoke to a school district that had implemented a biometric program,
using fingerprint scanning. They purchased both the scanners, but also the POS system at a tremendous cost and that was something that I didn’t want to do because again, we were satisfied with the program we had. I just needed to have a better way to accurately identify the student and as we refer to it, just reduce the hassle factor.

**NBSP:** Where did you actually first hear about biometrics and how did the idea of biometrics arise as opposed to some other type of technology?

**ATECH:** The Hong Kong Government had focused on biometrics as a solution from the beginning. The Hong Kong government has worked together with two or three universities in Hong Kong to investigate the feasibility of a security system, which can automatically process people at the airport, and at the crossing points … that must be a standard. We started about probably ten years ago.

**CATSA:** Biometrics was focused on by the Minister right out the door.

**PMAC:** You know at the time we were researching vendors [for the total project], we were thinking wouldn’t it be great if you could just come up with some sort of single sign-on. Well, let us go one step farther - let us go zero sign-on, so we started researching and calling around. I was actually at a local HIMSS (Healthcare Information and Management Systems Society) conference once and I saw this – I found some other solutions at the time that might have worked, but they were not hardware based and they required a lot of software. I did not want to deal with that because we were so small. Then at this local HIMSS conference, I saw Imprivata which was all hardware based and we started researching. They said, “You know what? We already have a hospital that has done this in your environment,” and we went from there as you said we have been on it since 2006.

**TCU:** As mentioned earlier, various authentication technologies were investigated, however the bank decided to incorporate biometrics as they, based on the technologies evaluated, provided an enhanced security, speed and convenience for the credit union’s customers.

Now when members visit a branch teller, they have the option to authenticate themselves by entering a PIN (something you know), swiping a debit card (something you have), or placing their finger on a sensor (something you are), using a device with a numeric keypad, a card reader, and a fingerprint sensor. IDMatrixx provided a software solution which was integrated with the core banking system thereby enabling a comprehensive authentication solution.

**Union Pacific:** Also, Union Pacific does have a significant history with respect to biometrics. Many years ago, they employed one of the first commercial voice recognition systems for managing the switches and related equipment in their rail yards.

**WCSD:** Those were some of the driving factors that made us look into another method and at the time which -- when I think about it was only five years ago, there weren’t a lot
of biometrics used in student or children identification. It was something more of an adult type of tool, so to speak. So, I felt that we needed to have some other method for identifying students and it was brought to my attention that there was the possibility of using biometrics. That is basically how we began our journey into using biometrics for our application here in the school district.

**NBSP:** Did you formalize this thought process to the point where you documented the acceptability and efficacy of the biometrics solution?

**ATECH:** The Hong Kong Government had conducted a feasibility study before going ahead with the project, the bidding process and award of the contract. At the feasibility study phase, the Hong Kong Immigration Department consulted a number of potential vendors, we being one of the four. The government tried to get technical information and performance projections from different vendors, and we worked closely with the government at that stage when they were preparing the tender document.

**BCHS:** No. Obviously our issue was patient care and safety. If we picked the wrong Mary Jones or if each time Mary Jones came in we started a new record, then our electronic medical record stored data is of no use to us. We researched the available tools out there, we did some research on finger printing, as an example, and determined that it would not work for us. We looked at smart cards and came to the same conclusion. After going through that process we then hit on the solution that we ended up choosing...vein pattern recognition. We researched that technology, conducted site visits, and concluded that it would work for us. We then took all that information and went to senior management and requested the funds.

**PAMC:** We really did not formalize our documentation on the biometric solution. The biometric implementation was part of an effort to implement a 100% paperless environment. We were doing a lot of implementation with nursing documentation and physicians doing their own orders. It was all documented as part of a solution to get the nurses on the same page and get positive reinforcement. We were listening to a lot of their issues. I went to a lot of meetings documenting what I heard from physicians and nurses and a lot of it was “How do you expect us to keep logging in and logging off? So we started thinking that a biometric solution could also take care of my issues as well.

Although we did not formally document the acceptability and efficacy of a biometric solution before implementation, we documented a series of SWOT (Strengths, Weaknesses, Opportunities and Threat) analyses in our area and we have always had a security issue with our multiple systems. So it just kind of blended in and became obvious. By listening at all of these meetings, myself and the CFO began to realize that this was a no-brainer. If for no other reason, the cost of this product to do this initiative would be less than going to all these meetings. Now that we are successful and we are live, the value of a biometric solution is certainly documented.
**Pearson VUE:** We were in the relatively unusual position of having outgrown our first-generation biometrics capability originally deployed in 2001. Therefore, as opposed to making a no/no-go decision on biometrics, we were interested in developing a next-generation identity management solution to meet our evolving needs. This led to a formal requirements analysis followed by a technology and vendor selection process.

One of the major factors in biometric technology selection and system design was an assessment of the core technology’s vulnerabilities to different types of attacks and threats. Our decision to select palm vein recognition technology in our test facilities was based on an evaluation of cost, performance, scalability, accuracy, usability, vendor support capabilities, privacy impact, acceptability to our client and candidate population and, of course, the competitive edge the solution would provide us. Our needs were somewhat unique and demanding, given that the solution needed to be tightly integrated with our existing test center software systems and deployed to a mix of company-owned and third party test centers in dispersed locations worldwide. The solution had to support over 700 devices operated by over a thousand personnel at more than 400 test centers in over 90 countries. It had to scale to efficiently process millions of biometric templates each year and to support enhanced services such as fast 1:N matching.

**TCU:** You first have to focus on what it is you are trying to protect. Next, you need to understand where the data is housed...centrally or in a decentralized environment. Then you must define your threats. What are they and where are they? Are they external, internal or both? Having defined the problem you must next define the solution. Are you trying to be on the cutting edge of technology or are you fulfilling a strategic company goal...in this case a goal of improving security and enhancing the customer experience? Finally, how will you know if you are successful? What are the criteria for success? They must be real, attainable and measurable.

There are a number of solutions available to the financial industry including document signing, customer and staff identification, network login/SSO, and biometrics among others and we evaluated a number of them. Integrating biometrics with a PIN and smart card seemed to be the best approach for us. There were, however, concerns about how well the biometrics technology would work and so we tested several solutions thoroughly for six months in house before making our final decision to implement it in a customer-facing environment.

**NBSP:** Did you make a case for the business or economic impact of this? You could go as far as to do a life cycle cost analysis, or as a minimum, there may have been some estimate of current cost, existing cost to be displaced by a biometric solution here.

**BCHS:** We did not justify this on a financial basis and we know that the actual registration process itself is only going to be impacted by maybe two minutes. Mainly, we did this to enhance the safety of the patient and the patient’s information.
TCU: We conducted a cost/benefit analysis on the proposed solution, which fit our business model; but the key was that the software solution provided by our integrator, IDMatrixx, could readily be integrated with our core banking system.

WCSD: I did put together a presentation with some numbers for the Board of Education, in which I documented the cost of producing the cards. There were things that were difficult to quantify such as the non-tangible, non-material expenses as well, but we focused on the cost of the lunch cards and other issues from the food service standpoint.

NBSP: So presumably if you did not document your findings in a written report, you certainly put together some presentation where you had to document the things, which you had discovered in your investigation.

BCHS: Correct.

CATSA: No, not per se. Actually, we took our marching orders from our regulator, Transport Canada and specifically it was the Minister of Transport, who decided that this was going to happen. And he specified the 29 airports where the RAIC program would be implemented.

PAMC: Because we are a 55-bed hospital we know all the major players in the area and we know the board. I can present right to the board myself. I finally gave them my plan of what we wanted to do. They saw the demos, brought doctors to evaluate, then they saw the excitement and said this is a no-brainer, go for it.

WCDS: In the presentation I mentioned earlier, I did not quantify, for example, the cost of our information system staff to create the list for the elementary schools that had the bar codes on them. I just focused mostly on what the impact was for the food service department.

NBSP: Let’s move on into the evaluation and implementation process. How did you select the best modality (technology), to be used? There must be a range of possible technologies you could have used.

ATECH: The choice on applying fingerprint was made in the 2002-2003 time frame. At that time fingerprint technology appeared to be the most mature and most economical technology choice. The Hong Kong government has worked together with two or three universities in Hong Kong to investigate the feasibility of a security system which can automatically process people at the airport and at the crossing points … that must be a standard. We started about probably ten years ago. After looking at different options, I think the iris, the fingerprint, the facial, that sort of thing. Eventually, I think the government has come to conclusion in terms of level of security, in terms of the cost and in terms of efficiency of the system or the processing time. The government finalized on fingerprint as a choice. I think it has gone through not government only, but they have gone through with the universities, because a couple of universities have been doing a
research on iris and others on fingerprint. One of the university professors is a world-recognized biometric expert, and the government is getting advice from them.

**BCHS:** The other technology that looked promising was optical (iris recognition). When we checked into it we found that it was very expensive. We looked into fingerprints and felt some of our patients would not feel comfortable and others would not have readable prints. We also looked at smart cards but found that they had a very low carry-rate of 40%, which would not have worked for us.

**CATSA:** CATSA formed working groups that interacted with the different stakeholders at the airports, other government agencies, the federal government, and Transport Canada, and they did a lot of work and research on biometrics and what type of biometrics to use. I had been at CATSA since October 2002, but I didn’t get involved in this program until 2004. By then the iris and the fingerprint had been selected as the biometrics of choice. In exploring the background of the selection process, I learned that during this research and selection facial recognition was felt to be less accurate than fingerprint and iris technology. Certainly at the time, vascular had not been researched well and wasn’t a viable option. It looks like it has gained a little ground recently but it wasn’t even on the radar then, and the working groups chose fingerprints and iris.

As I mentioned before, I wasn’t part of that early process, but by the time I arrived, the working groups had completed the formal analysis. They considered every modality that was viable at that time and then at the end of the day they agreed on the fingerprint and iris. A number of our people here in senior management have a police background with the RCMP and local police, and were very familiar with the fingerprint side of the house.

**PAMC:** Parkview selected finger biometrics as the biometric modality best suited because it enabled its more than 300 clinicians/staff to quickly and easily gain access to authorized applications. While researching this implementation, we encountered a number of biometrics that might have performed the actual identification satisfactorily. There is nothing better however, than having a vendor that could offer me the biometric solution and single sign-on. I have seen many people and organizations fail by choosing a single sign-on vendor, then choosing a different biometrics vendor.

At the recommendation of Imprivata, Parkview selected UPEK and deployed its TouchChip biometric readers. We found that it was easy to integrate UPEK’s TouchChip biometric readers with both OneSign and the hospital’s existing MEDITECH modules. And I’ll tell you what, in three years, I think we have only replaced two.

**Pearson VUE:** We were an early adopter of digital fingerprint technology in our test facilities, starting in 2001. In 2006 and 2007, we began to examine alternatives; for both regulatory compliance and public perception reasons, collection of fingerprint data was becoming increasingly difficult in certain countries in which we operate. Features and capabilities that drove technology selection included the following:

- Usability without extensive training
- High enrollment rates
- Low unit cost
- Acceptability (from a privacy perspective) to candidates, clients and regulators
- Form factor (small footprint, suitable for desktop use)
- Accuracy - low false rejection and false acceptance rates
- Global support on the part of the vendor

TCU: There were solutions tested including network login, physical access and customer identification. The decision was made to focus on customer identification first as that was the most compelling issue for the credit union. We decided on fingerprint biometrics due to the accuracy, price and customer awareness in using the technology. We tried several fingerprint devices recommended by our solutions provider and had the flexibility to use any of them since the software was agnostic to the device used.

We felt the accuracy and reliability of biometrics, at least for our application, exceeded that provided by other technologies. And, given that we are dealing with clients’ money, in our case well over a billion dollars, accuracy and reliability were critical. We conducted a cost/benefit analysis on the proposed solution which fit our business model; but the key was that the software solution provided by our integrator, IDMatrixx, could readily be integrated with our core banking system. The integration was important because it incorporated biometrics into our existing solution and made it a seamless transaction for the bank employees. Once the person was authenticated, the system would open the appropriate screen to continue the banking transaction.

After evaluating a number of modalities we landed on fingerprint technology for a couple of reasons. First, despite the negative connotation fingerprints might have had at one time, they are becoming much more mainstream now. Go into any bank and you will see the little fingerprint pads at each teller station for those clients who do not have an account at the bank. Fingerprint sensors are pretty much the modality of choice for laptop access as well. So, there was the familiarity factor. Total cost of deployment was much more favorable with finger and the accuracy, which, as I stated before is so critical to a financial institution, met all our thresholds for false accept, false reject and throughput.

Union Pacific: Well, they considered a variety of biometrics to automate their work gang time and attendance record keeping, and they were primarily concerned with eliminating worker fraud and leveraging their investment in workforce optimization. They ruled out fingerprints and hand based biometrics due to both union concerns and environmental and work condition issues. Work conditions in the field can alter a laborer’s biometric identity to some extent and/or prevent him from being identified. For example, fingerprint, when you have a laborer workforce, sometimes presents a lot of challenges with respect to getting a good image because they’re dirty or oily. There are a number of different reasons that a contact biometric doesn’t work well for that type of environment, so they wanted a non-contact biometric.

WCSD: It was something that best fitted the environment that we operate in. You
mentioned voice recognition, we work in a very loud environment at times either with equipment or just children and so trying to accomplish something like that would not be feasible.

We were trying to do something that would be very quick and easy for any child and would allow them to still have one hand on a tray and be able to present a finger for identification. When you look at the process, the student simply presents his or her finger. If we were to do some sort of eye scan, the student would have to get close to a piece of equipment. You also have the fear-factor with children that, is this going to hurt, or is it almost too sci-fi for some children. Some of the other technologies seemed a little bit too invasive to their space so to speak, but it was easy to stick a finger out and put it down on the reader. We didn't have to worry about the child being afraid of it because when we went through in the normal process they saw that it didn't hurt, you just put your finger there. So it had the least impact on the child and it was something again that was easy to do. We approached it with the kids from the standpoint of you always are going to have your finger with you - you can't leave it at home.

I feel very strongly about our choice because as I did my homework and asked questions, I learned that biometrics, historically, had been designed for adult identification and the difference between the adult and the child was primarily the size of the field that the scanner was reading. Additionally, the scanners that had been developed and created at that time, did not easily allow for the change of resolution that the scanner had to make in order to properly read the features of the fingerprint that they used to identify a child. They had to magnify that image and when you magnify, you have to maintain your resolution, which most scanners did not account for. It was a technical issue that this particular company recognized and embraced and developed software that would effectively do that.
So, they were really the first in the field, so to speak to have a program and product that could read prints ranging from the very small finger of a child in kindergarten all the way to the big high school senior football player whose thumb will cover the whole scanner. So, it is really was a broad range and thus difficult.

**NBSP:** Did you formalize a requirements list as a forerunner to going out to a vendor or systems integrator or putting out a request or proposals for somebody to do this for you?

**ATECH:** The Hong Kong Government had considered these factors in their feasibility study. Their operational requirements were:
- Passenger handling capacity each eChannel (entry/exit Channel) had to be scalable up to 5,000 passengers per Channel per day;
- Vehicle clearances scalable up to 3,000 per lane per day;
- System had to be designed to handle 7 million passengers per day and be scalable beyond that.
- There should be no more than three persons in the queue at any time with a maximum acceptable processing time of 10 seconds each.
- System reliability 99.8%.
- The system had to operate and meet those performance parameters in the following areas:
- Environment varies from extremes of heavy rain to very sunny with humidity in the summer of 95% with illumination variable.
- Demographics of the operation vary from very young to very old, both groups encountering degrees of difficulty in concentration and dexterity; all ethnicities and races with many Asians and westerners; and cultural differences as well.
- Security and safety were fundamental concerns, so provisions had to be made for liveness tests to enhance security, CCTV monitoring (one camera for every six eChannels), reliable detection systems to prevent tailgating and intrusions, gate door safety interlocks, referral lights to summon immigration officers, and local and central emergency capabilities.

**BCHS:** Actually, for the solution we chose, there was really only one vendor for us to partner with. HT systems is the contractor so to speak with Fujitsu, and HT systems works with the health system to build the integration with the Fujitsu system.

**CATSA:** In terms of the other more technically and operationally oriented requirements, they were going to vary greatly according to the individual airports. We had to identify somebody who was willing to work with us, point one. And we had a couple of airports that were willing to do that – you have to realize, by the way, that this was the first time ever that we would have two biometrics on a single card and we didn’t realize the technical impact of that at that time. We just sort of looked at it as a project that needed to be done, and tried to figure out the best way to do it.

I think the main objective was to enhance their current systems – because they all had Pass systems and they all work with Transport Canada to get those security clearances – that didn’t change. The issuing of the card changed and the enrollment and the accreditation portion changed a bit and that’s where we needed to sit down with them and work with them and provide guidance etc., etc. Then we had a couple of pilot sites at large and small airports and that proved extremely beneficial. We were able to test things out, look at any glitches, fix the system and move forward.

**Pearson VUE:** Yes. As I mentioned before, we were interested in developing a next-generation identity management solution to meet our evolving needs. This led to a formal requirements analysis followed by a technology and vendor selection process.

**WCSD:** No, I did not, because I was looking for a company that would provide just the identification software and hardware and particularly, a company that was providing it for a student population. The company I was dealing with at the time was the only company that was selling, a stand-alone offering five years ago. It doesn’t seem like a long time, but there were no other companies that were selling in the school market as a stand-alone product, not tied to POS software. So, there just weren’t many choices except the one company we ended up purchasing from.
NBSP: Were performance characteristics a central portion of your selection of the biometric? In other words, were the false accept, false reject rate or false match, false non-match rates a critical issue for you?

BCHS: Yes, we did research performance and the Fujitsu product is very impressive. As with anything else, we don’t buy something without seeing it work and getting good references. We felt that the investigation we did told us that very definitely this product worked and much better than other biometric options.

Union Pacific: One of the things that—and, you know, we did actually go up against fingerprint and hand geometry biometrics, and we won out for several reasons; those that Tim mentioned. But also, the speed of the search engines of fingerprints was slower than iris and it (the fingerprint reader) required physical touching and a PIN. Union Pacific also had some sanitary and safety concerns. Those two issues sold the system to Union Pacific management.

WCSD: We didn’t specify any false match rate, but we have never had any issues with false reads.

NBSP: Did you formally define the impact that this biometric system was going to have on your facilities or training programs to get people up to speed to use the equipment?

BCHS: Yes we control the training ourselves at the Central Business Office (CBO) and have a very formal training program. Part of the CBO’s responsibility is training, so we knew that this was something we would be able to handle.

PAMC: No, because I sold it as being part of a bigger project the training that they had already approved for all of nursing. It is actually what I used to make them sign up for training. And what I did was put the technology on the medical-surgery unit and gave a couple of my super-users access so people saw them using it and they all wanted it. We told them “Well, you have not signed up for training yet” and the training sessions just filled right up.

NBSP: How about legal considerations such as development of a privacy policy or privacy impact assessments?

ATECH: That’s very much an issue. And that issue has gone through our legislature in an extensive debate as to how information, can be protected. I think Hong Kong has about seven million people, and everyone of us has an ID card. When we register our ID card, that information that biometric and other personal information was kept in a vault more safe than the Fort Knox.

BCHS: Well, we are already governed under the federal government’s HIPAA requirements with regard to privacy, which is very well documented and we have many policies already in place.
**CATSA:** Transport Canada has the main database with all of the security information on an individual. On our CATSA database we have only a couple of numbers. We have expiry, the date of the security documents, the Document Clearance (DC) number and a couple of other minor digits. We do not have names of individuals. We cannot reverse engineer if we got a RIN number (a RAIC Identification Number). We don’t have any of that information. All the airport does is check with us to see if the DC number is legitimate and it ties into the same number that the individual has at the airport.

Given that background, I didn’t think that we had any personal data on our database. The Transport Canada privacy people disagreed with me because the document control number was the same on all three databases. We tried to impress upon the privacy office that CATSA doesn’t hold any data, Transport Canada does. They always have and it’s the airports’ data because the airports initiate these things, not us. So we said “Okay, how we handle this basically is that when the template is created at the airport, no information is kept on the airport database.” So that template is created, put on the card and that’s put on our database but not the airport’s. The reason it’s put on ours is because one of the checks done when the individual is enrolled is to see if those fingerprints exist already. So they check our database to see if they exist. If the answer is no, which is great, they go ahead and proceed with the enrollment. There are no names, no data other than the Document Control number. So that was, and is, how we protect our data, and that allowed us to continue.

**WCSD:** At the time that we began this, it was decided that the software would reside on the local school’s [server]. So, the privacy issue was addressed mainly by the fact that one school’s server had only the biometric information for that school. We knew that down the road, we would want to put that data on our county server, which then would give us a different need for privacy.

The way we addressed it when we first implemented the program, was that access to the local school machines was already controlled and that privacy had already been addressed with our existing data access program where there were sign-on codes. Personnel had to have their own sign-on codes to access the server. We concluded therefore that the existing privacy policies and security procedures were adequate if computers in the school were on the school’s intranet.

**NBSP:** Did you ever get any push back from any of the users, patients, students, or parents, that all this information could be on record now and you control it and it is their personal information?

**ATECH:** I think the Hong Kong government has done (and we helped them to do this), a very good promotion exercise on this. We have a number of gates at different crossing points at the airport, at the marine crossing points, the land crossing points. The database was only kept in a central location, what I called Fort Knox. Whenever someone puts in the ID card to go through the gate, the data will have to send a request to the database and ask them to send the biometric to the gate. That takes a couple of seconds. Those databases are not installed at the closing points for security reasons.
Yes, I think it is highly secured. Actually, people were surprised how this data was kept so, so secure. I think it is like a vault of a central bank, and anyone—I mean anyone, even the Director of the Immigration Department — who is the highest officer in Hong Kong looking after IDs and immigration letter -- has to go through a number of procedures such as, you have to use the key pad to get into the lobby. Then after that, you will go into a second chamber with the Director of Immigration, and his deputies, two of them go through both iris and fingerprint biometrics to verify if these two persons are responsible officers. Only after that they can access to the database. As far as I can understand, no false access has ever occurred made since database was established.

**BCHS:** Actually not. The patients responded very positively to this project and they saw it is something that they have been waiting for. In fact, we had number of comments like “What took you so long. This is exactly what we want.” I mean the compliance rate from patients is something like 99.8% or 99.9%.

The patients really like it. We were concerned that had we gone with something like finger printing the connotation with law enforcement would be a negative, but there’s nothing like that with vein pattern recognition at all. In fact, in the first hospital we brought live, one of the patients was so excited that she went to a television station, which called, came out and did a complete story on it. A very positive story.

**CATSA:** We worked with the airports – but, again, we were very, very careful not to interfere with any of their day-to-day business. The Pass control office and the Pass control process procedures were on-going well before CATSA. That was a regular airport occurrence. What we did was to enhance the security of that Pass process. We worked with the airports but essentially they manage their own people and workload. Where we ran into pushback was when a couple of airports waited a little too long to start processing these new cards and when the deadline came about there was a big rush in the last couple of months to get those people through. So we had to have a different number of enrollment stations and then monitor those situations very closely.

**Union Pacific:** I talked to a few of the people and they didn’t know that I was the one implementing this application. They didn’t have a problem with the technology, it created the perception that management didn’t trust them. That was their beef. In fact, a few weeks ago, made a new release and we’re on site with some people who were new to the system. And I actually heard one guy say: “What is this phone doing?” Another replies: “It’s taken the picture of your irises. That’s how we’re going to do time cards now.” The first guy just says, “Okay, no more buddy punches.” There’s another thing that helped Union Pacific a little bit with personnel concerns is that they already had a policy for biometric use. They indicated that when they deployed the voice recognition system for the railcar release program it sort of put a stake in the ground with respect to policy for the use of biometrics within the organization.

**WCSD:** I knew from my research— particularly from the other school officials I spoke with - what kind of reaction they got from parents, and what we could expect. So I was
prepared that there would be some negative reaction. Presenting it to the school board and getting their support was a real critical issue. If parents were speaking to someone on the school board or speaking to an administrator, they would understand what we were doing and why we were doing it.

But we also provided to the parent who objected to biometrics, the option to sign a statement that says, "We want our children to opt out of this program," and they understood that if they wanted to opt out, their child would be required to bring some form of ID with them to lunch.

Also we thought there might be people in the area that had religious objections, and this was our way of accommodating them and saying in essence, “We are not going to force you. If you object to this you may opt out.” And considering the number of students, we really have a very, very small number of people that have chosen not to allow their children to be scanned.

**NBSP:** Once you settled on a modality how did you evaluate potential providers? i.e.: was it an internal evaluation or did you bring on a third party to help? In either case, can you describe the process you went through?

**ATECH:** We searched through internet and/or local contacts and did the evaluation internally. We selected based on the technical characteristics, compatibility with other parts of the system, maintainability, and costs. Overall, for our purposes on this particular application, Lumidign fit the fingerprint requirements best.

**CATSA:** I can guarantee that there was a competitive process with multiple vendors submitting specification-compliant bids. On the integration side there was a formal competitive process where an integrator won and helped us with that.

**Pearson VUE:** We engaged International Biometric Group (IBG) to provide technical development services as well as consulting services including requirements definition, system design, and solution integration support. During the initial stages of technology assessment, IBG suggested that vascular pattern recognition technology warranted consideration, as the technology met several of our requirements for performance, usability, cost, and form factor. An in-depth evaluation of the technology itself and the vendors offering such products, conducted in conjunction with IBG, substantiated this initial recommendation and led to the selection of palm vein recognition.

**TCU:** There were several vendors that we looked at internally to evaluate the strength of their respective technologies and the cost effectiveness of their proposed solution. We engaged an outside consultant to help with the process and to test out the technology and the vendor’s claims. Based on evaluation results we selected the IDMatrixx solution because of the robustness of the technology.... it had been deployed at several police stations as an AFIS system... the speed at which it could be integrated with our banking system -- and total cost.
**Union Pacific:** Yeah, they invited several companies in to demonstrate their biometric technologies. In fact, these were companies that had biometric front-ends to their time and attendance packages, but we went out without a time-and-attendance software because ours was actually plug and play. But what, overall, won the day was the sanitary issue and the speed of the search engines for the iris.

**WCSD:** No, I did not, because the company I was dealing with at the time was the only company that was selling, a stand-alone offering five years ago.

**NBSP:** Okay last question in that area. How did the training go? Did it require repeated attempts to train people or did you just train them the next time they came in?

**BCHS:** What we like to do is completely train our registrars for new applications upfront. So we did an hour and a half training session prior to “go-live”. Usually we tried to do it three or four days before the “go-live”, so it was very fresh in their minds. We supported the training by having trainers from the Central Business Office on site 24/7 for three or four days to help them with any questions or any issues that would come up. We also spent a good 30 minutes on the importance of the new system and the critical need to determine identity and why we are doing it so rigorously.

We have a very sophisticated training program. We have 5 full time trainers who train all our registrars and our patient accounting folks. It helps when you have employee trainers who can quickly pull a project like this together and get everybody started out in the right direction. The other thing that helps us is we are very standardized across BayCare. We have all the same screens, the same systems, the same processes, same everything, and so training is much easier.

The initial enrollment piece only adds one to two minutes, but the future authentication process when they re-present, is just seconds. This is quicker than our old process where they had to type in five data elements to search our database to see if the patient had registered before. So we’re very pleased that we’re getting a high enrollment rate and we are up to 160,000 enrolled currently. The goal is to get up to about a million, and we’re headed in that direction.

**PAMC:** We had an advantage because our nursing staff had been using biometrics authentication already with our medication dispensary machines. Because of this, the technology did not intimidate staff in any way. We also made sure we did a good job of explaining the technology to the users.

**Pearson VUE:** We developed training material to familiarize test facility staff with device usage, best practices and related policies and procedures. Staff, in turn, guide each testing candidate on the use of the system. We also worked with the hardware vendor to develop a custom hand guide for the device that simplified and standardized usage on the part of operators and users. We created a strategy and supporting materials to inform and educate our clients about the features and benefits of the new system. We also worked with clients to develop informational videos, brochures and other materials to assist them.
in introducing their candidates to the new technology, provide assurance of security and privacy, and make the transition smooth and painless for them.

All test facility staff were provided training prior to switching over to the new technology. The training program and early monitoring helped us to identify enhancements to both the training itself and the technology user interface that subsequently led to further improvements in usability and performance.

**Union Pacific:** It was expected that we would go out to each one of their gangs throughout the country. We would just travel and implement the whole thing, do an enrollment process and then do a some training. Well, after the very first one, they realized that this was something that it was easy enough for them to do themselves.

**WCSD:** We required that they (identiMetrics) be there for the initial training, but would also be available to us in the initial enrollment of students. That was not particularly required but that was a part of the service that they were providing to us after we purchased their product. So, they were actually working alongside of us to enroll students to make sure that we felt comfortable with the product. In essence, they trained the trainer and I became the county trainer and so I have been able to train my staff in the enrollment process.

We trained as we did the enrollment process, by taking them in small groups, and (depending on the school and the setup), go into an actual classroom and set up our laptop computers. We show them what the scanner looks like, how to place their finger and have them do one finger three times on one hand and one finger three times on the other hand. So we walk them through the process. When they get up and see how it's done, we coach them if they need to move their finger. We use the same process today in any large group enrollment. For example, right now we are enrolling our fifth grade students who are moving up into the sixth grade, which is now in our middle-school structure.

So you learn to identify to the school the kind of setup we need. For example if we are going to all work in the same area; we need to be separated somewhat so that the student that's working with me is not thinking that the beep he hears from the next student is for him. So we try to isolate ourselves a little bit and we become very flexible with the school, we work within what they have, and thus have enrolled students in cafeterias, classrooms, hallways, wherever …. we are flexible.

**NBSP:** What’s been the impact of the new biometric application on operational, financial, and personal operations?

**ATECH:** Increased through put rate and redeployment/reduction of staff (hence operating costs). In the old manual system one immigration officer was required for each entry/exit channel (eChannel), and with the new biometric-based system, one officer can monitor and control six echannels. In the last three years, the Hong Kong Government because of budget constraints has been under pressure to downsize, and this system has
contributed much to the reduction of employees of Immigration Department of Hong Kong. It satisfies the high security requirements of passenger verification. The system has high availability and works 24 x 7 with minimum maintenance. In addition, the space required for eChannels is less, so the lanes can be narrower and we can put eight lanes in the same area that could only accommodate six lanes, thus increasing the capacity of our control points.

The public can enjoy more convenience and privacy because of the use of the automated process. There’s also an improved image of using hi-technology at Hong Kong border

**BCHS:** I think the impact is that we’re able to accurately identify our patients and quicker, which gives us access to our demographic and electronic medical record data.

**CATSA:** From CATSA’s perspective I think the airports are the ones who most clearly benefited from the new card, and the most singular benefit is, without a doubt, security. As a byproduct, it helped them to clean up their database and their old system. What I mean is, the new RAIC program ended the card-sharing era. For example, before this system was in place, when somebody had to go to the bathroom they could borrow someone else’s card to go. Now they have to have their own card, so it cut down on that kind of stuff. It seems kind of minor, I know, but it goes to show you the vulnerability of the Pass cards. And on the security side of the house it reinforced what we had been saying about enhanced security with biometrics. People being what they are, would try to spoof the old system – not with things that people may try to spoof biometrics with – but just by using somebody else’s card. But the integration of the biometric card into their regular Pass system has provided enhanced security, as has the integration of the RAIC into the rest of their security policies and those, I think, were the best benefits.

**PAMC:** Nothing but positive. As a result of the SSO/finger biometrics project, the need for physicians and staff to memorize multiple passwords was eliminated. Parkview cut helpdesk costs and improved employee productivity because clinicians are now spending less time logging in and out of network applications—improving the security of patient data and overall patient care. By incorporating finger biometric scanning into the SSO solution, each doctor or nurse is able to log on to any PC at the facility with a single fingertip swipe.

Key business results include:

- Three-day deployment with minimal resource requirements
- Single sign-on access to all critical applications
- Increased security through strong authentication with finger biometrics
- Faster, more convenient login/logout for users
- Lower Help Desk costs related to password resets
- Reduced IT support costs and resource requirements
- Easy adoption and consistent enforcement of security policy
- Compliance with data security requirements
**Pearson VUE:** The primary quantifiable benefit to the business has been a reduction in various types of test-related fraud and malfeasance, including the use of impersonators (also known as ‘proxies’) and other misrepresentations of identity. We have also recognized operational efficiencies in terms of candidate management through the examination lifecycle.

We are recognized as the industry leader in the application of advanced technologies for secure computer-based testing. Our successful implementation of next-generation biometric technology underscored that leadership.

The use of palm vein recognition technology underscores Pearson VUE’s commitment to exam security. This has proven to be an important competitive differentiator for our clients and has laid the groundwork for additional services we intend offer clients.

**TCU:** Most importantly and based on client feedback, we find that our members feel more secure knowing their accounts are protected from identity theft or fraud by a more technically advanced security system. We are able to offer them the same protection that the government is installing in passports and at airports. Members increasingly are replacing their PINs with their fingers and use biometrics as the preferred second ID for wire transfers.

The U.S. Patriot Act requires banks to use two forms of IDs for any wire transfers, biometrics is stated as an acceptable ID. From an operational standpoint, we have lowered authentication time from the 1 minute it took to compare imaged signature cards to an average of 3-5 seconds using the biometric system. Both teller and member transaction times have been reduced and as have the number of fraudulent transactions.

Less tangible, but of high importance is the fact that by deploying a biometric authentication solution we demonstrate to our members that they are our priority when it comes to protecting their financial assets and ensuring fast service when they visit our branches; and that we will stay current or even ahead of the technology curve to do so. A number of members view the biometrically-enabled system as much more secure than scanned facial images and our Branch Managers believe that the opportunity for fraud is lessened just by the visibility of the authentication devices....I mean, when they see the fingerprint scanner they are deterred from attempting a fraudulent transaction and will look elsewhere for a less secure facility.

Customers love the feeling of security as no one can steal their identity and access their life savings. This helps differentiate our credit union from other financial institutions especially with customers worrying about identity theft. Oh, there were some questions at first from some members. Like they saw something on TV about using gummy bears to capture a fingerprint or if their fingerprint scans could be stolen or sold. We were able to alleviate those fears by educating them on the technology...you know, like the fingerprint scanner had a liveness detection capability that wouldn’t be fooled by gummy bears.
One of my favorite customer quotes is “I’m comforted knowing my private financial information is protected by fingerprint biometrics. I can access my account even if I forget my wallet or my PIN, and I feel confident that the credit union will prevent a fraudster from accessing my life savings.”

In addition to the benefits we’ve already discussed there is another benefit, that being the ability to strategically differentiate your business from the competition though the use of an enhanced security technology. And, we feel we have done just that, and the feedback we get from new members seems to support that belief.

**Union Pacific:** And, as said earlier, there is no more buddy punching, so that’s an immediate benefit as well. Then you have the benefit that now this attendance report is generated automatically, so accuracy goes up and the amount of time that it takes someone to manually record the results of the roll call. You’re saving labor there as well.

**WCSD:** In the personnel area, it really didn't impact us at all. It has not required any additional personnel. We have been very fortunate that it really did not put a demand on us.

Financially, we obviously don't have the expense of the mass production, printing cards at the beginning of the year. We don't have the cost of the special cartridges to produce the card, so that expense has been pretty much wiped off our budget.

Operationally, one of the key lessons learned was that if we are able to enroll the students who are going into our secondary schools or middle-schools, the year before they actually go there, such as this time of year, then that makes the start of school much easier. In the past we waited until school started before enrolling the children and were running from school to school to school. Now this way it's easier for us to do it over a time period of several weeks. I have a supervisor who schedules the schools and, depending on the number of the students in the school, we can go out with one or two people, or working with a large group, I have trained my secretary to go or to help so we can do four people and get in and out quickly.

The other thing we have learned is to make expectations known to the school staff when we are enrolling students. We need to specify to them our space needs. We need to make sure that we have electrical outlets to power the laptops. I don't want to rely on our laptop batteries always lasting. We need to be presented with all of the students at one time. We need someone from the school there to supervise the students, because we are focusing on the students we are enrolling and training and if the rest of the students who are waiting are running around getting in trouble then we become distracted.

**NBSP:** How was the installation process handled? Did you use an integrator or other third party consultant?
**BCHS:** As I mentioned earlier, there was really only one vendor for us to partner with. HT systems is the contractor with Fujitsu, and HT systems works with the health system to build the integration with the Fujitsu system.

**PAMC:** Yes we did. We used Imprivata’s one sign-on solution, but I already had Forward Advantage as a vendor. They work directly with the vendor I chose for our computer system. So, instead of bringing on another vendor, they are actually the reseller of the product and I already had a relationship with them that is why I bought that from them.

They (Forward Advantage), came up for two days and we were live before they left. Our approach was not to have the integrator do it all, but rather, to have them train me and my staff so we could do it ourselves. So like I said, they came up and did that, providing some oversight during startup. They asked for information that they would need and I sent it back to them. They brought us two devices that were preconfigured with the information I gave them. We plugged them in and we were live probably 12 hours later on med-surg. I mean it was ready to go in two hours but I actually rolled it out to all the units and had my whole department testing and using it on the unit.

But if you think about it we had the foundation built. I have about 70 applications in this hospital. About 60 of them are one vendor and one sign-in. So my windows log-in, my email, my fax, and my hospital information system were the only things that I had to build apps for. So it was sweet. It was like a year’s work done in eight hours.

**Pearson VUE:** We worked with IBG and the technology vendor to integrate the equipment into our systems. A fulfillment vendor handled logistics for shipping and delivery of the physical devices to locations worldwide for installation. The technology was integrated in such a way that the upgrade process required minimal direct involvement by central Pearson VUE personnel and was streamlined such that local test facilities were able to install and configure the devices on their own.

**TCU:** A system integrator that was familiar with our core-banking system was used to integrate the authentication system into the core banking application and install the system. The installation of a central authentication server at headquarters was done in four hours. Then, the software installation and activation of the biometric units averaged about an hour per branch. Each new branch opens with the new system fully operational.

**Union Pacific:** It was expected that we would go out to each one of their gangs throughout the country. We would just travel and implement the whole thing, do an enrollment process and then do a some training. Well, after the very first one, they realized that this was something that it was easy enough for them to do themselves. It was that easy to implement. So, yeah, implementation now is just shipping the hardware and software to them.

**NBSP:** How did you prepare your employees/customers – (those who would be using the system) - for the application? i.e.: was there any formal training before the system was
implemented? How did the system users initially react to the idea of having a biometric taken and then having that biometric matched (for the application)? How well did the users come to accommodate and adapt to the biometric concept?

**ATECH:** The Immigration Office emphasized the increased convenience of the automated system: previously passing through customs manually averaged about three minutes, and with the automated system there should be no more than three persons in the queue at any time with a maximum acceptable processing time of 10 seconds each (in practice, it actually averages 6 – 7 seconds. So a 30 second processing time (and in practice, usually significantly less), was a vast improvement.

**BCHS:** Expanding on my earlier answer, one of the smart things we did is kind of interesting. At the time we were getting ready to kick this project off, we had a very large routine BayCare management meeting – all director level and above. At that meeting, we presented this new project and then we went ahead and enrolled all these people right then and there, which showed them the technology – got them all on board – and then they all went back to their facilities excited and informed about the project.

**CATSA:** We worked with the airports – but, again, we were very, very careful not to interfere with any of their day-to-day business. We worked with the airports but essentially they manage their own people and work load. Where we ran into pushback was when a couple of airports waited a little too long to start processing these new cards and when the deadline came about there was a big rush in the last couple of months to get those people through. So we had to have a different number of enrollment stations and then monitor those situations very closely.

**PAMC:** As I mentioned before, I went to a lot of meetings documenting what I heard from physicians and nurses and a lot of it was “How do you expect us to keep logging in and logging off?

So we started thinking that a biometric solution could also take care of my issues; 1) they never do log off, and 2) how do I make sure they are not sharing their passwords?

We kind of used it as a tool, a mechanism of “We have listened to your concerns, this [biometrically-enabled single sign-on] is our solution, what do you think?

And then we further structured it so that they could not participate in the biometric single sign-on until they went to training. And what I did was put the technology on the medical-surgery unit and gave a couple of my super-users access so people saw them using it and they all wanted it. We told them “Well, you have not signed up for training yet” and the training sessions just filled right up. So when they are seeing this thing, it was kind of like the cheese on the mousetrap. We put some bait out there and then reeled them in. What I did not want to do is use a treble hook and a fishing pole and snap them.

**Pearson VUE:** Users (candidates) are by and large accustomed to the use of biometrics in this environment, and there is a general understanding across the candidate population
that test integrity is an important element of high-stakes testing. During the early stages of deployment we conducted surveys of both candidates and test facility staff, who overwhelmingly reported satisfaction with the new technology.

**TCU**: All the Branch Tellers went through a 4 hour formal training on how to use the system and what questions to anticipate from the customers and how to answer them. There was a question and answer sheet that was passed out to the end consumers. The training was very important to make the Tellers comfortable with the system. Attention to training is as important as attention to technical detail in assuring a successful implementation. Members and Tellers both have to feel comfortable with the new technology and misperceptions about it have to be cleared up. If you handle that upfront you greatly reduce the chance of any negative reaction. Members were enrolled by the CU Branch Tellers within 30 seconds at the teller station when they would come in to do a banking transaction. New members were enrolled at the time they opened the bank account by the employee signing them up.

Credit union members were very receptive and voluntarily enrolled in the system. There were about 1% of the customers that were apprehensive, since enrollment was voluntary; they had the option to not enroll.

**Union Pacific**: They actually have management go around the country doing town hall meetings with the gangs, and they explain what is coming down the line. They were just getting prepared that way. And, of course, we did the administration for the management to show them how easy it was, and we had a lot of discussions with the unions.

**WCSD**: I knew from my research—particularly from the other school officials I spoke with—what kind of reaction they got from parents, and what we could expect. So I was prepared that there would be some negative reaction. Presenting it to the school board and getting their support was a real critical issue. If parents were speaking to someone on the school board or speaking to an administrator, they would understand what we were doing and why we were doing it.

As I mentioned before, we also provided to the parent who objected to biometrics, the option to sign a statement that says, "We want our children to opt out of this program," and they understood that if they wanted to opt out, their child would be required to bring some form of ID with them to lunch.

Also we thought there might be people in the area that had religious objections, and this was our way of accommodating them and saying in essence, “We are not going to force you. If you object to this you may opt out.” And considering the number of students, we really have a very, very small number of people that have chosen not to allow their children to be scanned.

I mentioned the logistical and practical aspects of training before, but in addition we carefully convey to the children that the biometric process doesn’t hurt, your hair doesn’t get curly, there is no electrical shock. We try to give the kids a kind of a fun approach to
it so that they aren't scared by it or think that something is going to zap them or bite them. Unfortunately, our children are exposed to a lot of things on television and they come with wild imagination. So we try to make them feel comfortable that this is quick and easy. Then, when they see how easy it is and the fact that they can observe their fellow students using it, it, then becomes just a nonchalant process and it's not a big deal for them.

NBSP: Were there any surprises along the way, and can you elaborate on how you dealt with the issues?

ATECH: The APVCS system called for high degree of reliability (99.8%) which could be delivered by individual components but initially not as a system. Hence, we had to have extensive discussions with component manufacturers to improve on the reliability of the components. We eventually achieved performance that satisfied the Immigration Department of Hong Kong and the community in general.

BCHS: I think the one thing that’s surprised me was the amount of media coverage this received. I knew we were doing something a little different and but I didn’t realize the interest in the community was so high, and every one of the articles was very positive. We had a lot of national news stories - Scripts-Howard picked us up, the Washington Times …. we were all over the country in one newspaper or another. We had the Department of Justice, contact us, they wanted to benchmark this, and Mass General called us, they too, wanted to benchmark, as well. We had a lot of different folks around the county call and want to know how we were doing. We knew we wanted to have some PR with this, but we just didn’t realize that we would almost be doing this every week.

CATSA: Many Asian women turned out to be very difficult to enroll in a fingerprint system because they had tiny hands. Elderly people had some difficulty because their skin tended to be dry, which we tried to overcome with the use of emollients. A lot people were afraid of iris at first until we put out communications explaining that it’s just taking a photograph of your eye – there are no laser beams and no zapping that’s going on. So gradually they understood that. So, I was a little surprised by those things. What I found was that people needed to see a person to communicate with each other. We would put out bulletins and everything else and think “Yeah that’s cool.” But unless people read the bulletins and flyers, etc., it’s not very cool at all. So we found the personal touch saved a ton of time. Any amount of money spent visiting the various airports was money well spent.

We also found people with a good IT program at the airports were the best, because they weren’t afraid and when we got right to it, being afraid of the new technology is what I’m talking about. For example, we had to deal with some union, the teamster’s union, and explain our situation. We had to get a hold of the D&B report to document for the union that the iris readers would not harm anybody. Once everything was in, and they could see there’s some value to it, then they sort of – I won’t say embraced it totally, but they were able to work with it with no problem and it goes from there.
Pearson VUE: Due to the evaluation and selection process described earlier, and a strong working partnership with IBG and the hardware vendor, we experienced few surprises.

TCU: The biggest surprise was how well the technology was received by our customers as we were initially not sure how our customers would react to using biometrics technology. Training the Tellers and making them very comfortable with the system helped sell it to our customers.

WCSD: The expectation initially for the Principals was that this was going to be very fast, and initially the scanning did not make things faster than the other methods. It was more accurate, but it took the students time to know where to place their finger, remember to wipe their hands off, etc. The first generation of scanners/readers were sensitive to dampness or to water, so if the child had sweaty palms or grabbed a bottle of milk that was wet it required extra time. The newer generation of scanners can read a wet fingerprint without hesitation. So they do begin to be faster as they go along but initially the Principals felt that it took too long. Well, it really didn't, they just had the expectation that it was going to be much faster.

NBSP: Okay, let’s touch on the last subject and that’s lessons learned. Can you think of what aspects of the project went well? For example, the preliminary planning phase.

ATECH: The most fundamental of all … the project was completed according to plan. We also thought the installation phase of the program went well even though there were some tough times during the middle of the project.

The most rewarding is truly the acceptance of the community. As I travel through the Hong Kong border system or airport, I ask the people sitting next to me, or immigration officers I encounter, how they feel about the system and they universally are enthusiastic supporters of it. I think the answer is that security must be the top priority, number one. There’s no question about it. I think when the government wants to push this system through our legislative council, like your House or Senate, the government receives a lot of questions on personal security, privacy, and all sorts of things before the legislative council will give the government the money to build the system. So it went through, probably, six months of intensive questioning and debate between the legislature and the government to get the funding approved. Most of the discussion was centered on security and the reliability of the system. I think that any automatic system or automated system will eliminate any abuse from the individuals. The immigration officer, he has a friend, he want to get him through in the old system, he can always get him through. But in here, the system does not know anybody. If the biometric is incorrect, he will not be allowed to enter, number one. Number two, in terms of efficiency, I think previously we have those immigration booths, and what work can happen for four immigration or four men in booths, we can put in six gates. So that will help to increase the number of channels that people can walk through. Number three, is that the time is faster. Then
fourthly, it’s safe. A lot of men—officers—we don’t need that number of officers to man the entrance point.

So financially, economically the government benefited; the community benefited. More than that, I think sometimes people can be sentimental. When the immigration officer questioned somebody, it’s always people do not feel well. They say, you know, I’m being insulted; you don’t respect me as an individual, that feeling. But for machine, the machine is neutral. They treat whether President Clinton or anybody the same. So actually, the system is extremely well received in Hong Kong by the community as a whole.

**BCHS**: The implementation phase went extremely well. It was a very short time frame for such a huge project affecting our entire System, yet it went unbelievably smoothly. It was pretty amazing.

We did a site visit to Charlotte in October 2007 and when we came back, we got the project approved. We had our first kick off meeting of the project May 1st and our first facility actually went live July 15. Following that, we were bringing up additional facilities about every three weeks. We have a large outreach lab that we did last in the first week of October 2008. With the outreach lab up, we had 24 sites throughout our health care system, -across 3 counties - that were implemented. And we were completely done one year from our site visit.

I guess the one thing that would be a lesson learned is we were so focused on the first facility “go-live” of the enrollment, actually getting those people put in the system, that we didn’t pay enough attention to the authentication when the already enrolled patient returns. We obviously didn’t see much of that the first week we were out there … the volume of authentications wasn’t high until we got to the outreach lab with lots of repeaters, then we really saw it. So we did do some additional training after we got a significant enrollment in our database. We then went back to every site just to heighten awareness of the authentication process, because we had so many enrollments, we wanted to make sure that we weren’t just enrolling people, but that they were authenticating properly as well.

**CATSA**: The communications were very good, but I think that we could have done a better job on the applications side of the house. I think we could have done a better job with some training, and then validating that the training they received was adequate. We certainly made sure that everybody was trained but I think we could have done a better job by going back and saying, “Hey, do you have any more questions?” We sort of assumed that everyone would find it very straight forward because we did and we’d been doing it for X amount of time. We didn’t take into account, as much as we should have, the vagaries of the individuals that were using the systems. So I think that was one. I think we did a really good job putting the two biometrics on the one card with the technology that we had at that time. And that process was good and the lesson we learned is that both of those – the fingerprint and the iris were pretty good – fingerprint obviously has been around for a lot longer, but it was the first time that those two had
been put together from what I understand. They were two good technologies, where one wasn’t brand new with a whole bunch of difficulty with the technology itself, so I think that was plus. So that’s the short answer to lessons learned.

PAMC: Well we’ve already mentioned some, but another was managing change in the organization. Recognizing we’d need the clinicians’ support to implement a new HCIS system, Parkview arranged a series of presentations during which we demonstrated to doctors how easy it would be for them to gain access to MEDITECH applications with SSO and finger biometrics -- and the clinicians were sold. When the clinicians learned that they would log on just once, using finger biometrics to access all the applications they needed, they started to become more interested in hearing about the project. With the use of SSO and finger biometrics, the IT team was able to deliver full access to all hospital information, with just one finger.

If I had to summarize “Lessons learned” I would probably say a couple of things:

- You can spend all you want on technology, but there’s nothing more powerful than education. Given the number of high-profile data breaches in the industry, healthcare organizations need to ensure patient data protection and comply with industry regulations such as HIPAA.
- Secondly, as I explained before, bringing your users on board early on is helpful in many ways. If they are impressed, and the value for them is obvious, they will make the overall adoption simpler and faster. Educating clinicians, staff, IT personnel, etc. is a critical step in protecting an organization and with the SSO/finger biometrics project, we learned that you have to do a comprehensive and thorough review of available solutions and educate users on how to properly utilize them. In our evaluations, we discovered the importance of tying strong authentication with SSO and learned that combining finger biometrics with SSO was an easy and efficient way to strengthen security and improve productivity.
- Additionally, I’d point out that although Parkview initially invested in finger biometrics to solve its password problems and strengthen IT security, the technology has provided additional benefits, for the process, called “bedside medication verification,” which greatly reduces medication errors and ensures patient safety. Parkview now barcodes and scans every medication that enters the hospital and each patient is also identified by a barcode on their wristband. Scanning tells the nurse if the medication being administered was ordered for that patient and is being given at the right time. And as we mentioned, the medications are only accessible for dispensing after a nurse has authenticated using finger biometrics.

Pearson VUE: The system was developed and continues to be managed through a formal software development life cycle process. This process is designed to ensure the right stakeholders are engaged at every step in the life cycle, from initial business case analysis and requirements gathering through design and development to deployment, training and maintenance. The system was deployed in phases, beginning with a three-month pilot during which we rolled it out to a limited set of locations for a single client’s
program and monitored the system and end users for technical difficulties and training issues. This approach worked well and allowed us to tweak procedures and the technology itself prior to expanding the system to all locations and migrating additional clients to the new platform. We are now in the process of implementing additional modular capabilities (such as 1:N matching) that build upon this foundation.

**TCU:** I think as I mentioned earlier, the integration of the IDMatrixx software with the core banking system ...that was a real plus. The branch installations went very smoothly as did member enrollment. Bottom line --the end-customers applauded us for deploying the biometrics technology.

**Union Pacific:** The speed in which we got them both enrolled and identified. I think, you know, again, I guess we’re sort of summarizing everything that we said, but also the acceptance of the workers themselves in using this, adapting to the hardware and, you know, figuring out after the first time. Actually, once you got them enrolled, they understand the distance and the position they need to be in, so those are all good thing.

**WCSD:** Presentation of the Business case, and selling a project to management all went very well. Pilot testing, installation and training we did well, but at the same time learned. I would say that managing change within the organization went pretty well. Finally, follow-up and problem resolution … that's been good. I temper my expectations with my knowledge about the evolution of child-focused biometrics. It is an evolving process and every reader gets better with improvements on a yearly basis. So, is it the top-of-the-line, 100% perfect? No, because I am always reaching and stretching and they are as well. But I am very pleased with the progress that I see that's being made with child biometrics.

**NBSP:** You have so many positive aspects of your installation and application that you probably wouldn’t mind sharing with us what few aspects of the project did not go so well.

**ATECH:** Change of vendor (autogate) at the middle of the project. The government demanded a really high reliability of the system. They are demanding a 99.8% success rate. When we were designing the system, we talked to component suppliers like card readers, like fingerprint scanners, and a number of other components. Each one of the suppliers of all these components told us that yes they can do 100%; they can do a 99.9% or whatever, which is true at the component level. But when you put 99.9 together with another 99.9 going down ten times, you are probably down to 98%. The error compounds and during the development stage and during the early implementation stage we cannot deliver the level of success, or the reliability of the system is not as high as what the Immigration Department would like to see.

So we had to go back to vendors and talk to them, and some of them enhanced on their performance. Other says I can’t, that’s the limit, that’s the best we can do. Actually one or two vendors, they over claim on their performance, so they are not delivering us a 99.9; they are delivering us only 99% sort of performance. So at that stage, we have to
search for other alternative suppliers of higher quality, higher reliability, and higher performance than had been taking place. And that’s a very painful process because quite often we have to change the mechanical mounting, the design of the gate, and also the interface and the software. But anyway, we secured a contract in April, and we got the first rollout in December in the same year by putting in millions of man-hours. I mean it was very painful to look in hindsight.

**BCHS:** Quite honestly, we did not have any problems I can think of. I know Lynda (the Project Officer), feels that it went smoothly and was well received by everybody. It wasn’t one of those projects where “Gosh we have a major problem we have to fix before we can proceed,” or we have to back up and start over, or the software was not working, or its response time is poor. We didn’t have any of those issues. Normally when we install systems, after we put the first one in, we are tweaking things, and we are making some changes and modifications for the system. We didn’t make any changes after the first install.

**CATSA:** It was our responsibility to go out and train them. Once everything was deployed I sort of sat back and said “Great”. But it didn’t take long for me to realize that we had to have constant communication with them. There was always some degree of turnover in their Pass offices, and if 2 or 3 of them left with their knowledge, people wouldn’t get the proper training. We realized that we needed to continue to provide training although technically it was an airport responsibility. We tried to work together with the airports on this.

**TCU:** The hardware scanners we initially deployed went bad quickly due to low Electro Static Discharge ratings and had to be frequently replaced. Since the software solution we deployed was an open solution, we did not have any problem to switch to another hardware vendor’s scanners. The key lesson here is to always make sure you are not locked into a proprietary system and you work with a vendor that provides an open system, which gives you the flexibility to switch hardware vendors so you don’t have to re-enroll your customers.

**WCSD:** We had hoped to have had the identiMetrics program with the database on a county server. That would have allowed for the portability of the data, at least within the county. Right now, when a student progresses to another school, I actually have to physically go out there, copy the data from one school, then transport that data and install it in the gaining school. That process would not be necessary if we had the program on a [county] server.

A couple of years ago, the Child Nutrition Program in the state of West Virginia announced that they had made a commitment to purchase a POS program for all schools in the state. So at that time when I was ready to say in our own district, “I want to get this biometric identification program on our county server”, I stopped. I knew that within the year (now it's two years - it's a little slower process for the state to do this), that I will have a state-wide POS, I will address the identification issue at the time that this occurs. So the one regret that I have is that we had not been able to get a more centralized
database in administration of the biometric program. So right now I have to go physically from school to school to transfer information.

**NBSP:** Well, let me try and ask you the question one more way. If you were doing it all over again, is there anything that you would do differently?

**BCHS:** Probably bring outreach lab up first. The outreach area is where we have the most volume. That way we would have seen more authentications the first time around. The more patients we get enrolled, the more authentications we can do and the registrars get very excited when they authenticate patients even today.

**PAMC:** It sounds bad but actually I think we did a pretty darn good job. It solved so many aspects that if we had to do it over again, we’d probably do it the exact same way. Part of that may be our underlying philosophy that everything that we do here, we should do with our own staff. My motto is if we can’t do it on our own, we need to learn it because we should not be taking on stuff that we cannot handle by ourselves. The environment changes way too fast to be relying on other people and getting nickel and dimed to death.

**NBSP:** Was a formal” after-action” analysis performed to identify lessons learned?

**ATECH:** Yes, there was a post-implementation review. We implemented a few enhancements to improve the application in terms of speed of operation and user friendliness.

**TCU:** Yes, but no changes were made to the customer authentication application. The bank decided that it wanted to deploy biometrics applications in other areas of the bank such as Network Login.

**NBSP:** Mr. Poon, can you elaborate on the enhancements made to the Hong Kong system?

**ATECH:** Yes, I think my previous answer is part of this answer. But more than that, I think we’re also looking at ergonomics of the gate. For example, just take the case of the fingerprint scanner. I think how or where to locate this fingerprint scanner, and the angle of the inclination, and the position relative to the entrance of the gate, all these affects the user friendliness of the gate. I think we made a few changes on that sort of thing. I mean, it’s not the system change, but it’s just making the use of the reader more ergonomic. I mean that if the fingerprint scanner is mounted totally vertically, people will have difficulty in putting finger on a vertical surface. But the angle itself is also another issue — you know it’s the trial and error thing.

**TCU:** Yes, there was, but no changes were made to the customer authentication application. The bank decided that it wanted to deploy biometrics applications in other areas of the bank, such as Network Login, however.
**WCSD:** Not in our particular [school] board. I have been able to do that in talking to other school districts and other school district administrators. I actually went to another school district in the state of West Virginia and talked to them about our experiences. So that's something that I had not done here locally, but I took that information and went somewhere else with it. I give them the real honest story … you know … here's what's involved. I don't sugar coat anything. I tell them, you will be challenged by some people in the community and here is how we addressed this situation.
Update on Major Government Biometric Initiatives

Contents

1 Introduction ............................................................................................................. 123
  1.1 General ............................................................................................................. 123
  1.2 Policy Context................................................................................................. 123

2 Existing Programs.................................................................................................... 126
  2.1 US- VISIT ......................................................................................................... 126
    2.1.1 Background ............................................................................................... 127
    2.1.2 History and Inception ................................................................................ 128
    2.1.3 Program Description ................................................................................. 128
  2.2 TWIC ................................................................................................................ 132
    2.2.1 Background ............................................................................................... 132
    2.2.2 History and Inception ................................................................................ 132
    2.2.3 Program Description ................................................................................. 133
  2.3 Registered Traveler .......................................................................................... 138
    2.3.1 Background ............................................................................................... 138
    2.3.2 History and Inception ................................................................................ 138
    2.3.3 Program Description ................................................................................. 139
  2.4 Real ID ............................................................................................................. 141
  2.5 NEXUS ............................................................................................................. 143
  2.6 DOJ “Automated Fingerprint Identification System” (IAFIS) ......................... 143
    2.6.1 Background ............................................................................................... 143
    2.6.2 Program Description ................................................................................. 144
  2.7 Department of State ........................................................................................ 147
5.2.4 Voice Projects ................................................................. 167
5.2.5 Trends .................................................................................. 167
6 In Conclusion..................................................................................... 168
1 Introduction

In August 2008, the National Science and Technology Council released a seminal work entitled: “Biometrics in Government Post-9/11,” providing a comprehensive outline and discussion of biometric programs throughout the federal government. This Section, while not trying to replicate the basic document, neither in structure nor content, is meant to provide an update on a number of those major government programs and initiatives involving biometrics, past (but still vital and relevant), present, and emerging. It is not an exhaustive or encyclopedic account; the Department of Defense (DoD) subsection alone alludes to some 83 biometric programs, but since many are classified or sensitive short-term development efforts we will only discuss a few. The intent of this Section is to provide an overview of the major, government-wide programs currently underway and to provide a sense of the scope and intent of the federal government with respect to biometrics.

1.1 General

Parts 2 and 4 of this Section describe major federal civilian agency programs. Part 3 provides an overview of some known DoD programs. Each program summary attempts to provide as many of the following details to the extent we were able to recover the relevant information from public sources:

- Background
- History and Inception
- Program Description
- Development and history
- Configuration
- Operations
- Success Stories
- Problems encountered
- Future enhancements

In some cases, government agencies have been quite forthcoming and comprehensive in describing their programs in various public documents and conferences. In other cases the government sources have been quite circumspect and details are speculative at best. Many of the DoD programs are classified.

1.2 Policy Context

All of the programs reviewed in this Update are projects initiated by the Executive Branch of the Federal Government. While the Judicial Branch and Legislative Branch operate physical and cyber security programs, parts of which no doubt involve biometric devices and technology, details of these programs are not readily available to the public. For the most part, neither of these branches has implemented named biometric projects or programs but instead use conventional access control systems in which biometric devices may be included as necessary to serve special access functions.

The direction for the Executive Branch operational environment begins with the release, from time to time, of Presidential Directives. Such Directives are policy statements. They are not in themselves funded ‘programs’ or procurements. Funded programs or procurements based on such Directives will emerge in specific agencies over time as they best interpret the Directive. In

the current context of national security, these have become systematically designated “Homeland Security Presidential Directives (HSPD).” Some of these have been publically released while the full text of others has been classified “SECRET” or higher. Even the titles of some directives have not been mentioned publically. HSPDs typically lay out a high-level policy position, objectives, or policy desired by the President.

Unless the Directive contains a specific expiration date, the enforcement and the lifespan of a Presidential Directive will depend upon the interests of the current administration. A Directive issued by one administration will continue in force into a subsequent administration unless and until countermanded by a subsequent Directive. In many cases, enforcement of a Directive may lapse due to the press of higher, newer priorities if not explicitly countermanded or redirected.

HSPD-12, issued August 27, 2004 by President George W. Bush, lays out the objective for creating a common identification credential to be used by all federal agencies. The stated objectives4 are for a credential that:

- Is issued based on sound criteria for verifying an individual employee’s identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

The Directive lays out general guidelines regarding the credential and implementation milestones. It also assigns the responsibility for implementing the Directive to the GSA and the responsibility for monitoring compliance to the OMB. As is the case in many Presidential policy and guidance memoranda, the realities of managing hundreds of federal agencies, 14.6 million employees and government contractors5, and independent foundations, commissions, boards and administrations result in numerous negotiations tempering and modifying the details of the Directive. While HSPD-12 called for background investigations and the issuance of new credentials for all employees by October 27, 2007, the true magnitude of this task has overwhelmed the agencies and the deadlines have been negotiated between the agencies and OMB over a broader horizon, often depending on specific agency issues and operating requirements. Numerous agencies submitted requests for ‘grandfather’ clauses. The USDA, which employed more than 99,000 people in 2007, for example, asked for such a clause to grandfather employees with more than 15-years of employment.6

“USDA requests a ‘grandfather clause’ for employees (not contractors) who have been employed by the Department for greater than 15 years. USDA’s ‘average’ employee has

over 16 years of service - USDA requests OMB to reconsider the benefit of re-doing the [biometric identity] for these persons.\textsuperscript{7}

In establishing its HSPD-12 guidance, the National Institute of Standards and Technology (NIST) updated its FIPS-201 (Federal Information Processing Standard) “Personal Identity Verification (PIV) of Federal Employees and Contractors” document to be consistent with HSPD-12, the abstract of which states:

“This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.

The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.

This standard does not specify access control policies or requirements for Federal departments and agencies.”

While the Standard goes into great detail regarding the mechanics and physical details of PIV credentials and its interfaces, it does not speak to any user or operator performance factors such as the ease of use or the system reliability in an operational setting.

In addition to HSPD-12, but relevant to this Section, President Bush also directed the publication of HSPD-24, “Biometrics for Identification and Screening to Enhance National Security” on June 5, 2008.\textsuperscript{8} The Directive reads in part:

“This directive establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual

\textsuperscript{7} USDA HSPD-12 Compliance Report to OMB
\textsuperscript{8} \url{http://www.fas.org/irp/offdocs/nspd/nspd-59.html}
information of individuals in a lawful and appropriate manner, while respecting their
information privacy and other legal rights under United States law.”

“...Through integrated processes and interoperable systems, agencies shall, to the fullest
extent permitted by law, make available to other agencies all biometric and associated
biographic and contextual information associated with persons for whom there is an
articulable [sic] and reasonable basis for suspicion that they pose a threat to national
security,”

Essentially, the President wants federal agencies to coordinate the use of biometrics to
screen and identify individuals. HSPD-24 is a new order that will attempt to standardize
how the federal government shares biometrics and other biographical information. The
Directive called for an implementation plan by early September 2008. The Attorney
General is charged with leading this effort. By June 2009, the Directive calls for a report
from major agencies on their progress toward implementing a plan. Neither of these
major policies directs any specific procurement, but they will significantly influence the
language and terms of inevitable future procurements and program definitions for some
time to come.

2 Existing Programs
This subsection reviews existing federal (civilian) biometric programs. While not all-inclusive,
these are the major efforts that have appeared in the press and for which many millions of dollars
have been committed. Some of these programs, such as “Real ID”, while enthusiastically
announced initially, have met with political and/or budgetary issues and have not yet evolved
into completed efforts. Other programs such as US-VISIT have been in existence for several
years and will continue to be highly visible efforts for some time to come. This subsection will
review that program along with Registered Traveler, TWIC, Real ID, and IAFIS.

2.1 US-VISIT
The United States Visitor and Immigrant Status Indicator Technology (US-VISIT)
program has its roots in the “Illegal Immigration Reform and Immigrant Responsibility
Act” (IIRIRA), Section 110, September 1996 and subsequent legislation through the
Intelligence Reform and Terrorism Prevention Act of 2004. The primary focus of US-
VISIT is the establishment and operation of an automated monitoring of the entry and
exit of non-immigrants at border crossing points or ports of entry (POE). The program
falls within the jurisdiction of the Department of Homeland Security.

The US-VISIT program is a cornerstone of the United States government’s efforts to
transform the nation’s border management and immigration systems in a way that meets
the needs and challenges of the 21st century. US-VISIT is part of a continuum
of biometric-enhanced security measures that begins outside U.S. borders and continues
through a visitor’s arrival in and departure from the United States. US-VISIT currently
applies to all visitors (with limited exemptions) entering the United States, regardless of
country of origin or whether they are traveling on a visa or by air, sea or land. Most
visitors experience US-VISIT’s biometric procedures – digital, inkless fingerprints and
digital photograph – upon entry to the United States when being inspected by an officer of the Customs and Border Protection agency of DHS.

2.1.1 Background

US-VISIT is a large, complex government-wide program intended to achieve enhanced security of U.S. citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the U.S. immigration system, and protect the privacy of visitors. The program achieves these goals by:

- Collecting, maintaining, and sharing information on certain foreign nationals who enter and exit the United States

- Identifying foreign nationals who:
  - Have overstayed or violated the terms of their visit;
  - Can receive, extend, or adjust their immigration status; or
  - Should be apprehended or detained by law enforcement officials

- Detecting fraudulent travel documents, verifying visitor identity, and determining visitor admissibility through the use of biometrics (digital fingerprints and a digital photograph)

- Facilitating information sharing and coordination within the immigration and border management community

Currently, US-VISIT’s scope includes the pre-entry, entry, status, and exit of hundreds of millions of foreign national travelers who enter and leave the United States at over 300 air, sea, and land ports of entry. In practice, however, the complications involved with enabling departure control within the current infrastructure on the land border have thus far confined implementation efforts to air and sea ports of entry.

US-VISIT is designed to use biographic information (e.g., name, nationality, and date of birth) and biometric information (e.g., digital fingerprint scans and photographs) to verify the identity of those covered by the program. The program applies to visitors whether they hold a nonimmigrant visa or are traveling from a country that has a visa waiver agreement with the United States under the Visa Waiver Program. U.S. citizens, lawful permanent residents, and most Canadian and Mexican citizens are currently exempt from being processed under US-VISIT upon entering and exiting the country. Foreign nationals subject to US-VISIT who intend to enter the country encounter different inspection processes at different types of POEs depending on their mode of travel. Foreign nationals subject to US-VISIT who intend to enter the United States at an air or sea POE are to be processed, for purposes of US-VISIT, in the primary inspection area upon arrival.
2.1.2 History and Inception

Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) directed the then Immigration and Naturalization Service (INS) to implement an automated entry and exit system that would track the arrival to and the departure from the United States of every alien. The objective of this program was to track foreign travelers who had overstayed their visa authorization. Events of September 11, 2001 refocused this activity from tracking persons with expired visas to border security as a paramount concern.

The automated entry and exit data system began to be deployed in 2004 with the installation of two-finger fingerprint readers at major ports of entry. The system has since been supplemented by video cameras that capture the facial image of the entrant, and is now in the process of being upgraded to take advantage of “slap” readers that record images of all ten fingerprints. More problematic is the deployment of an effective exit tracking component of US-VISIT, as challenges surrounding the location of readers and the impact on airline procedures are being addressed and tested to arrive at a mutually satisfactory operational configuration.

2.1.3 Program Description

2.1.3.1 Development Details and history

As noted above, US-VIST is an evolutionary development of automated management of visitors and immigrants to and from the United States that was mandated by Congress in 1996 and has been significantly influenced with global terrorist events since then. Following September 11, 2001, modifications of the US Patriot Act and the Border Security Act accelerated the implementation of an automated entry and exit system as well as for some enhancements. Additional enhancements were added by the Intelligence Reform and Terrorism Prevention Act of 2004.

These tasks were not trivial. In FY08, for example, there were more than 400 million inspections at US ports of entry, including nearly 200 million foreign nationals. In addition to the huge workload, there were significant programmatic, political, budgetary, and process issues that emerged as well, thus delaying implementation of a number of the desired features of the program.

Between 2003 and 2007, Congress has appropriated and the DHS has spent approximately $1.7 billion on the US-VISIT program.\(^9\) In 2003, DHS also estimated the full implementation of the program would eventually cost $3 billion.\(^10\) In 2006, still struggling with the logistical details of the Exit component of US-VISIT, DHS estimated it would require another $3 billion to complete the Exit system.\(^11\) In addition to the

\(^11\) ---- page 41
\(^12\) ---- page 7
heavy price tag, DHS must address major operational barriers such as implementing effective exit control at land border ports of entry where no infrastructure currently exists for automating confirmations of departure from the U.S.

2.1.3.2 Configuration
US-VISIT is an extensive complex of databases, both internal to DHS and external connections to a number of federal agencies. Most notable of the internal databases is the IDENT program discussed below. US-VISIT also interfaces with U.S. Customs & Border Protection (CBP) systems that contain advance information on travelers that has been collected by airlines prior to their embarkation to the United States.

2.1.3.3 Operations
The scope of the US-VISIT program is immense. According to government records, in addition to more than 300 land border crossings with Canada and Mexico, there are 72 designated international airports13 and 34 deepwater seaports14, or more than 400 designated entry and exit points to the United States. While slightly less than half were US and Canadian citizens, 51% or 224,400,000 required US-VISIT processing. Presumably, at least 145,200,000 of these would have been required to exit the US at the expiration of their visa. No system is in place, however, to monitor these exits.

2.1.3.4 Success Stories
The border control system was able to count and process 440,000,000 entries into the United States in a year, making it the largest semi-automated border enforcement system in the world.

2.1.3.5 Problems encountered
Challenges to the US-VISIT program are technological, financial, and political. The sheer scope of the program (tens of millions of travelers entering and exiting the US at hundreds of POEs) calls for the installation and reliable operation of a standardized suite of equipment on a 24/7 basis year round. Technical solutions, therefore, need to be durable, industrial-grade biometric sensors and information processing machines that feed into massive databases. At the very basic workstation level, nothing is asked of the US-VISIT system that requires extraordinary technology or innovative breakthroughs. It is only when the requirement becomes one of providing tens of thousands of workstations worldwide and at several hundred POEs in the US, all working and demanding identity verifications in real time, that management of the system becomes unwieldy and expensive.

The large number of POEs where this technology must be installed and operators trained to use it adds up to hundreds of millions of dollars a year—and this is just for the Entry control component of the program. Yet to be solved and implemented are the details of the Exit control and monitoring part of the program, estimated to cost several billion dollars more. Understandably, challenges have been appearing in the media for years

13 http://aerospace.web.mtsu.edu/usinternational.htm
from both security experts and members of Congress questioning the value of the program from a cost-effectiveness perspective.

### 2.1.3.6 Statistics

In fiscal year 2007\(^\text{15}\)

- A total of 46,298,869 entries recorded at air and sea ports.
- Of these, 236,857 were identified as possible overstays.
- The manual vetting system led to 273 **U.S. Immigration and Customs Enforcement** arrests.
- The databases resulted in 25,552 hits for consular officers overseas adjudicating visa applications.
- There were 11,685 biometric watch-list hits at the port of entries, which included individuals with criminal histories.
- **United States Citizenship and Immigration Services** used the system to screen those who apply for immigration benefits, creating 31,324 hits.

### 2.1.3.7 IDENT

The DHS Automated Biometric Identification System (IDENT) is a legacy system of the INS that now uses automated fingerprint identification systems technology that is identical to the Department of Justice IAFIS. IDENT was originally designed to thwart illegal entry into the United States by criminal aliens and was first deployed at Border Patrol stations along the U.S. southern border to identify repeat offenders.\(^\text{16}\) The system originally used two-print technology that was incompatible with IAFIS standards. A significant upgrade performed after September 11 has made IDENT records interchangeable with IAFIS.

Launched on a trial basis by INS in 1994, the project was refined and enhanced, becoming operational in 1998. Today, IDENT is the largest fingerprint repository and the most efficient matching system in the world. It can process up to 300,000 transactions per day and has over 91 million individual fingerprint records. It contains watchlist data: information on known or suspected terrorists, criminals, sexual offenders, domestic and international fugitives, other safety threats, military detainees, other persons of interest, and other egregious offenders. IDENT receives a subject’s fingerprints and compares them against stored fingerprint records. Results are provided to end users to help determine identity on an average of 10 seconds or less against its highly actionable watchlist. IDENT has identified more that 60,000 criminals, immigration violators, and suspected or known terrorists. The IDENT system also provides basic identification information that allows access to several other security and law enforcement databases including, but not limited to, active and legacy systems that include the Central Index System (CIS), National Automated Immigration Lookout System II (NAILS), Deportable Alien Control System (DACS), National Crime Information Center (NCIC) database, and the Treasury Enforcement Communication System (TECS).

\(^{15}\) [http://www.cis.org/vaughan/USVISITNumbers](http://www.cis.org/vaughan/USVISITNumbers)

Figure 2 illustrates the relationships among these databases.

2.1.3.8 Future enhancements

As mentioned above, the final major keystone for the US-VISIT program is the implementation of the Exit component of the system. Accounting for who is entering the US with legitimate credentials is only half the problem. Equally important is to make sure that those who have entered on a time-limited visa exit the country on or before the expiration date of that visa. Of course, this begs the question of whom and what agency will be tasked to locate and apprehend those overstaying their visas. This aspect of visitor management has not been, in our opinion, adequately addressed in any related program in any systematic manner. The Exit component of US-VISIT is intended to facilitate the exit reporting, from a U.S. port, of visitors who entered under authority of a visa. By design, an examination of the database of persons who entered under visas, less those who have just departed, enables the identification of those who have remained in the U.S. beyond the terms of their admission.

Not unexpectedly, the cost and logistics of implementing a sound Exit program has been daunting and has become the major obstacle to implementation and US-VISIT has been hard-pressed to proceed. In mid-April, 2009, for example, The U.S. House of
Representatives Appropriations Subcommittee withheld funding for the US-VISIT Exit program. DHS wanted to have airlines collect the biometrics of those exiting the country. Naturally, airlines do not want to pay for it and the House is withholding DHS funding for the project until the agency figures out another way to implement the program. Rather than arguing the cost impact, the airlines have put forward an argument that DHS lacks the legal authority to collect fingerprints from those departing.17

2.2 TWIC18

2.2.1 Background
The Transportation Worker Identification Credential (TWIC) is a biometric-validated credential for use throughout all transportation modes. The TWIC enables unescorted physical or computer access to secure areas in the national transportation system. TWIC was developed in accordance with the legislative provisions of the Aviation and Transportation Security Act (ATSA) and the Maritime Transportation Security Act (MTSA). The program is administered by the Transportation Security Administration (TSA), under the guidance of the parent Department of Transportation (DOT). To date over 1.2 million people have been enrolled in TWIC at U.S. seaports. Each enrollee is required to pay a fee of $132.50 for a card that is valid for five years.

The TWIC program is a multi-phase program evolving both with technology and national security policy. Although its current focus rests on maritime operations, full deployment will eventually include workers in truck, rail, and air modes of transportation as well as sea.

The goals of the TWIC program are to:

- Positively identify authorized individuals who require unescorted access to secure areas of the nation's maritime transportation system
- Determine the eligibility of an individual to be authorized unescorted access
- Secure areas of the maritime transportation system
- Enhance security by ensuring that unauthorized individuals are denied unescorted access to secure areas of the nation's maritime transportation system
- Identify individuals who fail to maintain their eligibility qualifications after being permitted unescorted access to secure areas of the nation's maritime transportation system and revoke the individual's permissions

2.2.2 History and Inception
Immediately following the terrorist attacks of September 11, 2001 Congress passed the Aviation & Transportation Security Act. This comprehensive law prescribed steps to be taken to secure the nation’s transportation infrastructure, and authorized the Executive Branch to take strong action to ensure traveler safety and prevent further disruption to air

18 http://www.tsa.gov/what_we_do/layers/twic/index.shtm
transportation. The November 19, 2001 law specifically authorized the Under Secretary of Transportation to “provide for the use of biometric or other technology that positively verifies the identity or each employee and law enforcement officer who enters a secure area of an airport.”

Research on a program to use biometric identification at airports began immediately. By early 2002, DOT announced its intention to establish the Transportation Worker Identity Credential, which was to be issued to anyone who needs access to secure facilities in the performance of their job. In the aviation industry alone, this meant that every flight crew member, every airport vendor, mechanics, fuel and catering truck drivers, security staff, and law enforcement personnel would have to carry and present a valid TWIC before they would be authorized to enter the secure zone. Identity would be verified through biometric checks that would compare data stored on the card or a server against a live image acquired from the card holder.

Concerns were raised by airports, airlines and others about the feasibility of such a large program. Since the initial plan allowed flexibility on how the program was to be implemented at each location, airlines in particular were skeptical about the complexities that would be encountered by crews as they traveled from airport to airport. Questions were also raised about who would pay the costs to redesign and retrofit airports to accommodate the TWIC infrastructure.

While program development continued, immediate implementation was postponed due to these unresolved issues of procedure and cost. It was not until Congress passed further legislation in the form of the Maritime Transportation Security Act on November 25, 2002 that a program was specifically mandated. Congress laid down further requirements in the Security and Accountability for Every Port Act, resulting in a seaport security initiative that was to be administered jointly by TSA and the Coast Guard.

Rules for TWIC were described in federal regulations published in January 2007; late that year, implementation was under way as enrolment centers opened in cities across the U.S. A schedule was set for ports to start screening workers by late 2008 in some locations, with virtually all major seaports to be included by late spring 2009.

2.2.3 Program Description

2.2.3.1 Development Details
As envisioned in the notice of proposed rulemaking released by the Coast Guard in 2006, card readers enabled with biometric identification technology were envisioned as an integral part of the initial TWIC deployment at seaports. Agreeing with concerns by those who commented on the proposed rule, DHS decided to postpone the use of the readers until technology and procedural questions could be resolved. The TWIC would

---

19 U.S. Congress, Public Law 107-71
20 U.S. Congress, Public Law 107-295
21 U.S. Congress, Public Law 109-347
be enabled for biometric checks, but use of readers would be delayed pending further examination of these barriers. For now, the TWIC exists as a standardized identification badge with security features that make it difficult to forge or alter. In addition, the Coast Guard uses handheld readers to make unannounced checks of the biometrics on the card against that of the person presenting the card.

The technology issues identified in comments centered on the speed, accuracy and reliability of an identification process that would take place in a harsh environment. Concerns that resonated with Coast Guard regulators included:

- Compatibility with existing systems and standards
- Robustness of a data network that would have to be capable of supporting up to 700,000 transactions per second
- Reliability of readers that were constantly exposed to marine conditions yet required contact with the TWIC to acquire the necessary data
- The impact of high failure-to-read rates on port operations
- Dead zones in the wireless communications infrastructure

Facing these critiques, regulators decided that further testing was necessary before readers could be placed in the field. As a result, five areas were identified for additional study and research. These are:

1. **Environment.** Establish that the readers are fully functional outdoors and can withstand changing weather conditions. Demonstrate that sensors imbedded in the readers must demonstrate resistance to the effects of condensation, direct sunlight, static charges created by wind, and abrasion.

2. **Customer service and training.** Develop processes for ensuring that systems and devices are adequately maintained, and users are properly trained in the use of a relatively new technology. Determine that the readers are intuitive and can be used by following simple instructions.

3. **Reader type.** Examine the feasibility of using readers that can read the data on the TWIC-imbedded integrated circuit chip without having to physically contact the chip. Determine the effect of continued use on the durability of the card when using either contact- or contactless technology. Measure throughput rates when using either type of card reader.

4. **Biometric operation.** Determine how biometrics can be used in a real time, high volume identification process given the data storage limitations on the card and potentially poor read rates. Ascertain if there are ways to make routine biometric checks without compromising data security requirements.

5. **Standards compliance.** Ensure that the program is fully interoperable with other major federal credentialing programs, including the FIPS 201 guidelines for HSPD-12 implementation and the merchant mariner credential.
These questions are in the process of being examined in a pilot program involving seven seaports (see 2.2.3.6, Future Activities, below).

2.2.3.2 Configuration

Although configurations for biometric checks under operational conditions will not be set until the pilot programs have been concluded and key procedural concerns are resolved, the enrollment process is in place across the U.S. at 149 sites. Applicants are required to produce either one document from List A – primarily a U.S. passport or Merchant Mariner Document – or two documents from List B. The latter includes a state driver’s license, certified birth certificate, voter registration card, social security card, military ID card, military discharge papers, and seven other types of documentation. Foreigners who may be qualified to work based on their immigration status are subject to similar identification requirements. All applicants must be fingerprinted to facilitate checks of the FBI IAFIS system, and to capture the biometric data that is needed to establish a positive link between the individual and the card.

Aside from having to prove eligibility for TWIC on the basis of citizenship or immigration status, workers may be disqualified based on a serious criminal record. In many cases a denial may be appealed to an administrative law judge for adjudication. Once the enrollment process is complete an applicant may check on the status at a TSA-maintained website. If the application has been approved, the same website may be used to schedule a time to pick up the completed card. The latest statistics on number of enrolments, cards printed, average enrolment time, disqualifications, and other important program metrics may be viewed at http://www.tsa.gov/assets/pdf/twic_dashboard.pdf.

2.2.3.3 Operations

TWIC is in operation only as a uniform identity badge. The program will be expanded to validate identity using biometrics once the development questions discussed above have been resolved through field testing.

2.2.3.4 Success Stories

To date much has been learned in the process of ramping up enrolment and studying how the TWIC can be introduced as an identity tool at the port. Those key lessons cited by TSA and its contractors include:

• Developing a rapid and repeatable deployment process
• Learning to use mobile devices to make record checks and verify identity
• Modifying capture processes to accommodate oversize hands
• Adopting flexible staffing models to handle fluctuating enrolment demand
• Scheduling card activation and pick-up to avoid bottlenecks
• Adjusting systems requirements to comply with NIST standards
• Exploring self service options to streamline pre-enrolment data capture

22 For a list of TSA enrolment offices and hours, see: http://twicinformation.tsa.dhs.gov/twicinfo/schedule.jsp
23 https://twicprogram.tsa.dhs.gov/TWICWebApp/StatusCheckPrep.do
Eventually TWIC should become the largest real-time biometric identification system deployed to date. When biometric devices come into common use for operational purposes, TWIC should provide an unprecedented amount of data regarding the field use of the technology under some of the most demanding conditions found anywhere.

2.2.3.5 Problems encountered
The most apparent problem area that emerged from initial evaluations of the TWIC solution was the discontinuity between the nature of the credential and the operating environments in which it was expected to be used.

Administratively a decision was reached that the TWIC should be compatible and compliant with the FIPS-201 standard for federal identification credentials. This standard requires a contact credential used in combination with a PIN code. There are at least two key problems with this approach.

One problem is that the salt air common to all maritime facilities and ships at sea is highly corrosive to the delicate electronic components used in the contact readers. Not only were the contact points highly vulnerable, but the electronics within most commercial readers were not sealed and protected from the salt air and moisture. The obvious solution would be to use sealed and ruggedized contact-less readers designed to withstand the rigors of ocean air and the maritime environment. The problem with this solution was that the FIPS-201 standard called for the physical contact between the reader and the concurrent submission of a PIN.

The second problem lay with the administrative rules and procedures regarding the PIN code. If bearers of the TWIC forget their PIN, they are required to return to an official TWIC enrollment center where special equipment is required to reset the PIN. Additional problems encountered reflected the ‘failure-to-enroll’ (FTE) issue that can sometimes affect biometrics capture. Hard work and exposure the maritime environment often takes a toll on the hands of mariners, thus making it difficult, if not impossible, to capture usable fingerprint images. While the TWIC contractor (Lockheed Martin) was claiming FTE rates of 1-2%, the actual experience has often been in the FTE range of 3-8%. Without the fingerprints, the TWIC cannot be issued.

Another problem emerged as the number of credentials to be issued began to grow. Machines designated to print and create the TWIC were not designed to handle the volume of cards required. TSA also acknowledges that the adjudication of applications has proven to be far more complex than originally estimated, as nearly fifty percent of applications must be subjected to closer review before eligibility can be determined. And, as has been the case with many similar large-scale biometric-based identity programs, TSA has noted the importance of having initial biographic data captured in a

24 http://www.secureidnews.com/2008/08/28/council-twic-is-broken
26 http://www.secureidnews.com/2008/06/13/more-twic-problems
pre-enrolment scheme (e.g., web-based collection) to avoid unnecessary administrative burdens at time of enrolment.

Additional problems or issues associated with the TWIC are summarized in a National Maritime Security Advisory Committee, TWIC Working Group report amended and issued July 30, 2008.27

2.2.3.6 Future Activities28

As of mid-2009, TSA approved a number of contactless readers after subjecting them to laboratory tests and “live” trials at approximately 23 maritime facilities, vessels, and vessel operation centers. TSA is preparing a report to be submitted to Congress as required by the SAFE Port Act and will be used to support a second TWIC rulemaking that will establish long term requirements for TWIC readers.

The ongoing testing program examines contactless biometric card readers, including the credential authentication and validation process. The testing program includes an evaluation of the business processes, technologies, and operational impact of deploying readers to the maritime environment. Seven ports29 have been selected as pilot sites for the field portion of the tests. In accordance with the requirements of the SAFE Port Act, the trials will emphasize interactivity between multiple facilities and various vessels to evaluate reader functions and the impact on overall environmental and operational conditions.

The pilot program is taking place in three phases:

- Initial Technical Testing (ITT) Phase will provide information on the technical capability of the readers to function in the second phase.

- Early Operational Assessment (EOA) Phase will obtain data to support the rulemaking process, assess reader suitability and effectiveness, and support refinement of the reader specifications.

- System Test and Evaluation (ST&E) Phase will evaluate card reader effectiveness, suitability, and supportability; and will establish a test protocol that will be used by the sites and vessels to evaluate readers before they are acquired and used for broader TWIC implementation. ST&E will also evaluate the full impact of readers on facility and vessel operations and business process as operators conduct access control measures in accordance with various scenarios designed to provide data in crafting the final reader rule.

---

28 http://www.tsa.gov/what_we_do/layers/twic/pilot_test.shtm
29 Port Authority of Los Angeles (CA); Port Authority of Long Beach (CA); Port Authority of New York and New Jersey; Port Authority of Brownsville (TX); Watermark Cruises of Annapolis (MD); Magnolia Marine (MS); and Staten Island Ferry (NY)
2.3 Registered Traveler

2.3.1 Background
The Transportation Security Administration (TSA) developed the Registered Traveler Program as a way to address customer service concerns that resulted from the imposition of stronger passenger security screening measures in the wake of the September 11 attacks. Long lines at airport security checkpoints prompted pressure on TSA from Congress and consumer groups to implement a program that would allow low risk travelers to be expedited through screening procedures.

Tests of the concept resulted in the 2006 launch of a Registered Traveler Program that was to be a voluntary, market-driven initiative operated by the private sector but overseen by TSA. Participating companies would be authorized to enroll participants using biometric (fingerprint and iris) and biographic information and charge an annual fee for the service.

As of July 2009 the program is on life support. The company that provided services at 18 of 21 approved Registered Traveler sites is out of business, and customers who paid up to $200 annually to participate must now go back to using the standard TSA clearance process.

2.3.2 History and Inception
The Registered Traveler (RT) concept had its origins in legislation passed in late 2001. The Aviation and Transportation Security Act of November 2001 mandated many improvements in security, including the re-establishment of the air marshal program, more extensive screening of passengers and baggage, the installation of explosives detection equipment, and full federal (i.e., TSA) control over the checkpoints. At the same time, the Act authorized the newly created TSA to “establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.”

A year later, the Government Accountability Office completed a review of options for an RT program at the request of Congress. The resultant report identified key operational and policy issues that should be addressed before implementing a program, and made a series of recommendations for TSA to follow:

- Incorporate “lessons learned” from similar programs, including US and Canadian experience with automating border clearance
- Test the program on a small scale to determine feasibility and effectiveness
- Develop performance measures to assess if the program meets stated goals

30 Public Law 107-71, 107th Congress, November 19, 2001
- Use interoperable technologies, and select solutions that can be updated to take advantage of advancements in security, biometrics, and data sharing.

The report documented the benefits of an RT program but went on to list a number of concerns that were identified by stakeholder groups. These included questions about privacy and the use of data for purposes beyond aviation security, and about the distracting effect that an RT program could have on TSA’s security mission. In addition, the report raised the serious question of liability: would RT program providers have adequate protection against lawsuits arising from denied applications, or from security failures that resulted in a terrorist attack? Finally, the report summarized four biometric technologies that had potential for use in RT systems: fingerprints, iris recognition, hand geometry, and face recognition. The report drew no conclusions on which, or what combinations of, biometric technology should be used.

The Act, the GAO Report, and continuing public pressure for a viable alternative to long security lines set the stage for TSA to begin work in earnest on an RT solution.

2.3.3 Program Description

2.3.3.1 Development Details and history

TSA took to heart the lengthy list of GAO recommendations on policy and operational questions that needed to be resolved before a program could be implemented. By late spring of 2004, however, the agency rolled out six pilot programs that were designed to test market acceptance and operational performance. TSA-run sites included airports in Los Angeles, Minneapolis-St. Paul, Houston, Boston, and Washington, DC. An additional trial was authorized at Orlando, to be run by the private sector firm Verified Identity Pass (VIP). Up to 2,000 volunteers were authorized to participate at each of the TSA sites; participants were issued smart cards that were linked to a centralized database containing their biometric data. The trial, initially set for a ninety day period at the TSA sites, was not interoperable between the airports, i.e., a card issued for use at LAX could not be used at Boston Logan. The Orlando project was authorized for six months to one year, and was capped at 30,000 members.

By 2006 TSA was ready to implement RT using a public-private partnership model. Companies that agreed to comply with TSA requirements would negotiate with individual airports to set up special lanes adjacent to or near the regular TSA-operated security checkpoints. Fees charged to travelers would cover the costs of leasing space from airports, buying and installing equipment, paying TSA for screening services, and operating the RT lanes with staff provided by the private sector partner. Interoperability was an essential prerequisite, meaning that a card issued by one provider was valid for use at any other participating airport. Management of information on travelers and their biometrics would be provided by the Transportation Security Clearinghouse, operated by the American Association of Airport Executives using database technology provided by Daon.
By 2008 the RT process was in place at 21 airports,\textsuperscript{32} with VIP operating 18 of those sites under its brand name “Clear”. Two other companies were also authorized to participate: Flo, maintaining an RT site at Reno, Nevada; and Preferred Traveler, with installations at Jacksonville, Florida and Louisville, Kentucky. On June 22, 2009, however, the program ground to a halt when VIP announced it was going out of business and closed down all of its facilities. The prime benefit of multi-airport interoperability for more than 250,000 RT users had vanished, and the future of the program placed in serious jeopardy.

\textbf{2.3.3.2 Configuration}

Companies wishing to provide RT services are subject to a TSA review and approval process that examines the legitimacy and financial stability of the business. Service providers are divided into three categories: companies that provide enrollment services; companies that provide verification services; and those that provide both enrollment and verification. Approved providers would be allowed to collect and forward biographic and biometric information on applicants for the purpose of vetting prospective users against criminal and watch list databases. For such checks, called Security Threat Assessments, TSA requires payment of a $28 operating fee per applicant. Upon approval, smart cards are issued to participants by the service providers.

\textbf{2.3.3.3 Operations}

As noted above, RT facilities are usually collocated with TSA screening checkpoints. The RT user is directed by signage to a reserved queue. As with travelers using the standard clearance process, the RT participant produces government-issued identification that is verified by TSA staff. Once that step is complete, the traveler is turned over to the service provider staff who oversees the biometric identification phase. This is accomplished by having the user insert the smart card into the RT kiosk and face a special camera that captures the iris image. The “live” image is then compared against the database record associated with the smart card. If identity is verified the registrant then goes through the regular TSA screening procedures to which all air travelers are subjected. If no RT participants are in the service provider queue, nonparticipants are often shown to the area that has been set aside for enrollees to avoid idle time for TSA staff.

\textbf{2.3.3.4 Success Stories}

At its peak – June 22, 2009, when VIP ceased operations – the program claimed 260,000 members. This made RT the largest USA program of its kind to date, exceeding the size of the joint USA-Canada NEXUS program that claims about 225,000 participants. The program also established the operational viability of public-private partnership, and the robustness of the biometric technology in quickly matching the identity of the user against enrollment data.

\textsuperscript{32} Participating airports included Albany, Atlanta, Boston, Cincinnati-Northern Kentucky, Denver, Indianapolis, Jacksonville, New York LaGuardia, Little Rock, Louisville, New York JFK, Newark, Oakland, Orlando, Reno, Salt Lake City, San Francisco, San Jose, Washington Reagan National, Washington Dulles, and Westchester County (NY)
Since the smart card was standardized in format and content, it could also be used to facilitate other services. Tie-ins with airport parking and frequent traveler lounge access have been used to entice flyers to sign up for an RT card.

### 2.3.3.5 Problems encountered

At a macro level the demise of the RT program was due to several factors, including a recession-induced slowdown in business travel, the price of the service, the dominance of a single company, and the skepticism of key airports. The falloff in air traffic alone may have had profound effects, as service providers were unable to recruit enough travelers to make the service financially viable. While the list of participating airports was impressive, some of the biggest airports avoided making a commitment to RT: Los Angeles, Chicago, Baltimore-Washington, and Pittsburgh are top tier airports that did not institute a program and thus excluded huge segments of the traveling public from an RT system that relied on critical mass to succeed. Finally, the suspension of operations by a company that dominated the market effectively ended the program.

Beyond the financial problems that put VIP out of business, the Registered Traveler program also appears to have failed – for the time being, at least – due to the combination of high fees and relative lack of benefits. RT was originally conceived by leading advocates as a program in which travelers would submit to extensive vetting in exchange for an expedited screening process, perhaps one in which shoes and coats did not have to be removed or in which searches would be random rather than routine. Instead, travelers were paying up to $200 in annual fees simply for, as one wag put it, a “glorified ‘cut in front of the line’ system.”

Airlines also undermined the program by instituting lines that were dedicated to frequent flyers. This free service reduced the attractiveness of RT with its separate application process and significant fees. Put another way, travelers may pay high fees to avoid a twenty minute queue, but will not do so to save five minutes.

### 2.3.3.6 Future enhancements

As of this writing, the program has ceased to function as a national scale service. TSA has not announced plans to revive or restructure the program, and traveler data that had been held by VIP has been destroyed.

### 2.4 Real ID

REAL ID is a controversial nationwide effort to prevent terrorism and reduce fraud by improving the reliability and accuracy of identification documents that state governments issue. Enacted and signed by George W. Bush on May 11, 2005, as “REAL ID Act of 2005,” the Act does not use the term “biometric.” On March 1, 2007, DHS released a Notice of Proposed Rulemaking (NPRM) for the REAL ID act for a 60-day comment period. The NPRM did not include biometrics as a required feature on REAL ID compliant driver's licenses or identification cards, but solicited comments on the potential use of biometrics as an additional security feature for individual states or for

---

33 Danny Sullivan, The Huffington Post, July 9, 2009

authenticating individuals during renewals. It also points to the US-VISIT and other passport and visa related programs and their use of biometrics as a tool that states might use to enhance a person’s identity assurance level.

Discussions surrounding Real ID have, however, focused on the possibility to use the holder’s photograph as an input to a biometric identifier using facial imaging techniques. Opposition groups have picked up on this interpretation and have used it, along with unfounded references to other biometric modalities—including “retina scanning”—to drum up support for legislation to prevent implementation of the Real ID Act. Various provisions of the Act have struck a fundamental chord of opposition on several fronts, but it is not easy to determine what is really at the heart of the dissent. As of the date of the publication of this document, no real biometric application has been mandated or articulated for implementations of Real ID credentials and the editorial position of credible national media now speculate support for Real ID has eroded and that it will not be implemented.

Former DHS Secretary Michael Chertoff stated in testimony before Congress that the Act’s primary intent was to “[raise] the security standards on driver’s licenses [to establish] …another layer of protection to prevent terrorists from obtaining and using fake documents to plan or carry out an attack.” The Act has come under fire recently with many senators speaking out against it, and state legislatures passing resolutions against its implementation. The National Governors Association (NGA) issued a statement regarding the introduction of an amendment by Senator Susan Collins to delay implementation of Real ID. “This proposal would provide states a more workable time frame to comply with federal standards, ensure necessary systems are operational and enhance the input states and other stakeholders have in the implementation process,” said the NGA.

A major real impediment to the implementation of Real ID is the fact that the Act did not include any funding for the states to offset the cost of the new credentialing program. Congress only added about $40 million to assist the implementation while a Government Technology Report reflects an industry estimated cost of $11 billion for implementation. In December 2007, DHS announced it would permit states to use up to 20% (an estimated total of $35 million) of their State Homeland Security Grant Program (SHSGP) funds to help in the implementation of Real ID. As of this writing, however, many states have either announced their refusal to participate in Real ID or stated their inclination not to participate. As of March 2009, the American Financial Services Association announced: “Since 2007, at least 10 states have passed resolutions that urge Congress to amend or repeal REAL ID, or indicated their intent not to comply. At least 23 states have passed some sort of anti-Real ID legislation and 11 have successfully

---

36 http://www.govtech.com/gt/104173
37 http://www.govtech.com/gt/101128
changed state law to reject Real ID requirements…There are currently 26 bills pending in 18 states relating to REAL ID.\textsuperscript{38}

The final blow to Real ID came in April of 2009 when Homeland Security Secretary Janet Napolitano announced that she is working with governors to repeal the Real ID Act, which was passed in 2005 and went into effect last year. Napolitano, former governor of Arizona, said she has met with governors of both parties recently "to look at a way to repeal Real ID." She said she wants to substitute the federal law with "something else that pivots off the driver's license but accomplishes some of the same goals. And we hope to be able to announce something on that fairly soon."

2.5 NEXUS

NEXUS is a joint U.S./Canadian program, launched in 2002, designed to facilitate and expedite the movement of frequent travelers between these two countries by sea, land, or air. NEXUS travelers are initially screened for basic eligibility, which is limited to American and Canadian citizens and permanent residents, and subjected to criminal record checks. Iris and fingerprint biometrics are captured from successful registrants, who then receive government issued ID cards. The cost of the credential is $50 for US citizens and $80 (Canadian) for Canadian citizens and is good for five years.

As of September 2008, over 225,000 Canadian and US citizens were enrolled in NEXUS. It is currently in place at eleven land crossing points between the USA and Canada and eight Canadian airports that have U.S. pre-clearance facilities. NEXUS uses iris recognition biometrics to automate border clearance processes at the eight airports; on the land border, the U.S. version simply provides expedited access to special traffic lanes that are open only to travelers who are enrolled in the NEXUS system. As a traveler and vehicle approach the inspection point, radio frequency (RF) technology is used to preload a data file on the traveler. The inspector visually correlates the file information with the traveler and authorizes entry if there is a match.

2.6 DOJ “Automated Fingerprint Identification System” (IAFIS)

The Integrated Automated Fingerprint Identification System, more commonly known as IAFIS, is a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year.

2.6.1 Background

The predecessor AFIS system was developed over thirty years ago. In the early 1990s government managers recognized the necessity to improve the technology and accelerate the collection, transmission, and analysis of fingerprint data by the FBI in support of both federal and local law enforcement daily investigative activities. The resulting advanced system, IAFIS, became operational by 1999.

\textsuperscript{38} https://www.afsaonline.org/CMS/fileREPOSITORY/The%20REAL%20ID%20Act%20Final.pdf
2.6.2 Program Description

2.6.2.1 Configuration\(^{39}\)

The IAFIS comprises a central depository of millions of ten-print images and templates based on decades of law enforcement activity that has resulted in the capture of tens of thousands of automated fingerprint images using collection devices and systems located at various law enforcement facilities nationwide.

2.6.2.2 Operations

IAFIS provides five key services:

1. Ten-print Based Fingerprint Identification Services. Ten-print images are collected at various sites nationwide and comprise both criminal and civil databases.
   - Criminal Ten-print Fingerprints: This database comprises prints taken as the result of an arrest at any governmental level and electronically forwarded to the IAFIS. Fingerprints captured on paper media are mailed to IAFIS where they are converted to electronic images.
   - Civil or “Applicant” Ten-print Fingerprints: Fingerprints are acquired related to various background checks for employment, licensing and other non-criminal justice purposes.

2. Latent Fingerprint Services. In addition to fingerprints taken directly from subjects, IAFIS supports both electronic and paper submissions of latent fingerprints taken from objects of interest normally related to criminal investigations.

3. Subject Search and Criminal History Services. IAFIS supports the storage and exchange of criminal history records of individuals based on law enforcement and court record information provided by participating states.

4. Document and Imaging Services. These include non-analytic functions that support law enforcement operations.
   - Document Services: IAFIS processes documents associated with various criminal history records such as arrest dispositions, expungements, and other data updates.
   - Fingerprint Image Services: IAFIS supplies electronic images of fingerprints to authorized agencies on request.
   - Photo Services: The IAFIS has the capability to receive, store, and distribute photographic images.

\(^{39}\) http://www.fbi.gov/hq/cjisd/iafis.htm
Remote Ten-print and Latent Fingerprint Search Services. Using IAFIS-provided Remote Fingerprint Editing Software (RFES), local law enforcement activities search the both IAFIS ten-print and latent image databases as part of criminal investigations. Searches that used to take as much as three months to complete can now be accomplished in just a few minutes.

Table 1 - IAFIS Daily Capacity and Usage\(^{40}\) (2004)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TPRS queries (DHS)</td>
<td>8,000</td>
<td>2,200-3,000</td>
<td>3,182</td>
<td>-</td>
<td>6,059(^{(a)})</td>
<td></td>
</tr>
<tr>
<td>CAR bookings</td>
<td>30,000</td>
<td>20,500</td>
<td>60,000</td>
<td>35,000</td>
<td>up to 3,900(^{(b)})</td>
<td></td>
</tr>
<tr>
<td>IRQ</td>
<td>7,000</td>
<td>6,000</td>
<td>7,000</td>
<td>6,000</td>
<td>3,000</td>
<td></td>
</tr>
<tr>
<td>Latents</td>
<td>635(^{(d)})</td>
<td>350</td>
<td>25</td>
<td>635</td>
<td>450</td>
<td>up to 158(^{(e)})</td>
</tr>
<tr>
<td>Name checks/III/Criminal histories</td>
<td>850,000</td>
<td>425,000</td>
<td>187,000</td>
<td>850,000</td>
<td>470,000</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Source: CJIS Division, except where noted as from the DHS.

(a) Provided by the DHS. The DHS projection is based on workload data for January through April 2004.
(b) The FBI plans to support up to 1 million additional annual CAR bookings from the DHS after October 1, 2005.
(c) The CJIS Division limits the DHS to 3,000 IRQs per day to ensure that other entities have access to fingerprint image retrievals.
(d) All federal agencies except the FBI have been allocated 25 percent of IAFIS’s latent fingerprint search capacity.
(e) The DHS allocation is 158; in the past the DHS has not submitted latent requests up to its allocation.

2.6.2.3 Success Stories

Metrics on IAFIS are not available through public sources, but anecdotes indicate that to a large extent the FBI has achieved its goal of speeding up the fingerprint examination process and by doing so improving the effectiveness of law enforcement. Checks that used to take days now take minutes, enabling local law enforcement officials to quickly determine if a subject may be using a false identity or may be wanted in another jurisdiction.

\(^{40}\) [http://www.usdoj.gov/oig/reports/plus/e0501/results1.htm](http://www.usdoj.gov/oig/reports/plus/e0501/results1.htm)
In two instances cited in 2003, subjects who had been arrested for minor drug violations were wanted for murder in another part of the country. Because IAFIS response times in these cases\(^{41}\) had been reduced to 14-18 minutes, the subjects were identified before they may have been released on the lesser charges.\(^{42}\) The FBI notes that “these are just a few of the many IAFIS success stories every day — and why the FBI remains committed to providing this critical service to law enforcement.”

### 2.6.2.4 Problems encountered

The FBI acknowledges an error rate of 2 percent on IAFIS checks.\(^{43}\) While this may not seem high, volume now exceeds 100,000 checks per day,\(^{44}\) meaning up to 2,000 of those checks either failing to match existing records or erroneously pairing an identity to someone else. With a database that now exceeds 63,000,000 records, the FBI has been actively seeking system improvements that will reduce the error rate and improve the accuracy of the identification process.

### 2.6.2.5 Future enhancements

The FBI’s Next Generation Identification System program is a multi-year effort 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 within the existing IAFIS environment.

Preceded by the activation of the IAFIS in 1999 and its subsequent successes (Section 2.6), the NGI is a natural evolution from the single dimension of the IAFIS fingerprint-oriented system to a multi-modal system embracing iris, facial, and other resources for identification. The IAFIS system had been experiencing occasional embarrassing instances of missed or erroneous identifications using fingerprints only;\(^{45}\) incorporating newer biometrics in the IAFIS database is expected to reduce or eliminate this problem. Although the procurement action for NGI initially anticipated a 2006 or 2007 award, the program was not formally awarded until February 2008. Due to bidder protests the procurement action was not resolved until May 2008\(^{46}\) when IBM agreed to join the winning Lockheed Martin team. Initially thought to be worth “…hundreds of millions of dollars…,” NGI was finally awarded the 10-year contract worth nearly of $1 billion. In development since at least 2004, the NGI is expected to reach an initial operating capability (IOC) with enhanced fingerprint capabilities by late 2010/early 2011.\(^{47}\) The NGI will be an integrated system using open standards to give it flexibility to adapt to changing requirements. The program is to be implemented in a multi-phase, 6-year development effort. The first phase or increment, now underway, is the Design Phase resulting in an initial capability for advanced fingerprint matching. In addition to improved accuracy, the FBI also hopes to reduce response times from two hours to ten

---

\(^{41}\) Officially, the FBI quotes a two hour response time for criminal record checks
\(^{42}\) [http://www.fbi.gov/page2/dec03/prints121603.htm](http://www.fbi.gov/page2/dec03/prints121603.htm)
\(^{44}\) On February 26, 2009, the FBI reported receiving over 188,000 IAFIS queries in one day
\(^{45}\) Ibid.
minutes on criminal checks, and from 24 hours to fifteen minutes on urgent civil or “applicant” checks. Increment 1 also includes a study and selection of a new fingerprint matching system. This study is expected to be complete by the end of 2009.48

Increment 2, to begin while Increment 1 is still underway, will start to integrate the new business systems surrounding the fingerprint capability. Also, this phase will develop new databases for “…individuals of special concern…”, i.e., known or suspected terrorists. The goal is to provide a 10-second response to local law enforcement officials in the field by using wireless fingerprinting devices mounted in police vehicles or stationed at remote locations.

Increment 3 will see the fully integrated business system implementation by the first quarter of 2012. A unique attribute of this phase will be to incorporate a palm print identification system as part of the IAFIS NGI structure. Increment 4, ending in mid-2013, will add the facial recognition modality as well as the addition of scars, marks, and tattoos as identifying features. Increment 5 will see the integration of iris recognition into the NGI system, leading to what the FBI hopes will be a 100 per cent identification solution. This phase is expected to be complete in early 2014. Increment 6 will be the project validation phase and will conclude the formal development aspect of the contract. The remaining 3-4 years of the NGI contract, into 2018, will comprise efforts to maintain and operate the system and to introduce improvements and other enhancements.

2.7 Department of State

2.7.1 Electronic Passport

The U.S. Electronic Passport is the same as a regular passport with the addition of a small contactless integrated circuit (computer chip) imbedded in the back cover. The chip securely stores the same data visually displayed on the photo page of the passport, and includes a digital photograph. The inclusion of the digital photograph in theory enables biometric comparison through the use of face recognition technology at international borders, although there are no such implementations to date.49 The U.S. “e-passport” also has a new look, and incorporates additional anti-fraud and security features. Although international standards50 for e-passports also permit on-chip storage of fingerprint and iris images, the U.S. has chosen not to, primarily because there is no easy way to collect the data from passport applicants. With few exceptions this is consistent with practice elsewhere in the world, establishing the face image as the default technology for future identity applications involving the new generation passport.

2.7.2 Secure Network Access

Secure network authentication is now possible through the use of smart cards and biometrics. Users simply insert their smart card into the biometric reader and place their finger on the reader surface for biometric authentication. This solution features tests for user “liveness” and match-on-card technology, in which all processing takes place at the

48 http://findarticles.com/p/articles/mi_6712/is_29_237/ai_n29416348/
49 The Australian Government has implemented an automated border crossing system that relies on face recognition, but that program is currently limited to Australian citizens who are e-Passport holders.
50 International Civil Aviation Organization; see http://www2.icao.int/en/mrtd/Pages/default.aspx
card reader. With on-board processing, the time required for user authentication is substantially reduced, since user information does not need to be verified on the workstation. The greatest benefits of this technology are ease of use, the reduction of fraud generated by password sharing, and the elimination of password resets.

3 DoD Programs

DoD presents a special bloc of biometric programs for evaluation and study. On one hand the DoD is much like any other government agency in that it is responsible for implementing biometric programs in a manner consistent with public policy and executive branch directives. A number of DoD programs (such as the Common Access Credential [CAC]) are recognizable, standard identity management and access control activities.

On the other hand the DoD is responsible for and is currently engaged in extraordinary, on-going combat operations in the Middle East against an unconventional terrorist adversary. Wearing no uniforms and observing no international standards for the conduct of war or protection of civilians, the terrorist slips in and out of native populations firing shots of opportunity, often using indiscriminate ordnance such as “improved explosive devices.” Tactics designed to counter an enemy of this nature need to be as flexible and creative as the adversary. The military Services have developed biometric technology solutions to help identify and maintain identity awareness of as many of these terrorists as possible. Some of these efforts are very highly classified and information regarding most is considered to be, at the very least, “unclassified, but sensitive.”

In 2005 the Armed Services reported that there were 83 deployed biometric systems or projects. Of these, some 27 were considered large (more than 200 enrollees, or more than $1 million budgeted system costs). The remaining 56 projects were classified as ‘small’. Of the “large” systems, the Army has deployed eight, the Air Force five, the Navy/Marine Corps five, and, at the DoD/Joint organizational level, nine.

In 2000 Congress designated the Department of the Army as the Executive Agent for Biometrics. The operational environment facing the DoD has changed significantly over the last two decades, starting with the fall of the Soviet Union and following the emergence of stateless terrorism as the unconventional, but primary aggressor force that is challenging DoD resources and strategies. In the biometric context a very real threat is the ability of terrorists to blend in with native populations. Biometric technologies are being used on an increasing basis to identity populations and to isolate terrorist elements. Indeed, the DoD believes biometric technologies are revolutionizing operations such as population control, counterintelligence screening, and detainee management and interrogation, and in business operations such as base access control to verify Common Access Card (CAC) credentials.

---

3.1 DoD Organization for Biometrics
Biometric activities—research, evaluation, applications, and adaptations—have been underway in various forms since at least 1980, but without centralized coordination. Most efforts were exploratory in nature and involved relatively small databases. Research focused on forensic applications (i.e., fingerprints) and access control methods. Increasing expenditures for research elevated the need for better coordination and management, culminating in a Congressional designation of the Army as the Executive Agent for Biometrics in 2000.

In July 2000, Congress designated the Secretary of the Army (SecArmy) as the Executive Agent (EA) for DoD biometrics information assurance programs. Under Chief Information Officer (CIO)/G-6 oversight, the Army established a Biometrics Management Office (BMO) charged with strategy, planning, and resourcing, as well as a Biometrics Fusion Center (BFC) responsible for technical operations. SecArmy later shifted organizational oversight from CIO/G-6 to the Deputy Chief of Staff (DCS)/G-3/5/7 in June 2006. Upon this transition, DCS/G-3/5/7 united the BMO and the BFC by establishing the Biometric Task Force (BTF) as a central taskforce responsible for DoD biometrics. On 23 March 2010, Department of the Army General Order (DAGO) 2010-06, signed by the Secretary of the Army (SecArmy), redesignated BTF as the Biometrics Identity Management Agency (BIMA) on 23 March 2010.

Unlike the BTF, BIMA is a permanent organization, rather than a temporary task force. This permanent status ensures that biometrics endures as an enabling capability for DoD. BIMA will continue to report to G-3/5/7, and the Director remains the Executive Manager for DoD Biometrics.

Biometrics enables IdM across four domains: Warfighter, Business, Intelligence, and Security & Law Enforcement. This redesignation has the broad effect of institutionalizing a formal organization type and reporting process for DoD biometrics. Through BIMA's assigned functions and responsibilities, the DoD achieves a biometrics program that is fully integrated Department-wide and synchronized across the Services and Combatant Commands.

The Biometrics Identity Management Agency leads Department of Defense activities to prioritize, integrate, and synchronize biometrics technologies and capabilities and to manage the Department of Defense’s authoritative biometrics database to support the National Security Strategy. Through the Biometric Identity Management Agency, the Department of Defense achieves a biometrics program that is fully integrated Department-wide and synchronized across the Services and combatant commands.

3.2 Automated Biometric Identification System (ABIS)

3.2.1 Background & History
In September 2004 the Army awarded a contract to Lockheed Martin for $5 million for the first year of a five year contract to development its Automated Biometric Identification System (ABIS). Patterned after the FBI’s “Integrated Automated Fingerprint Identification System (IAFIS)”, also developed by Lockheed Martin, ABIS and its fully deployable successor NG-ABIS (Next Generation) enable military agencies to conduct automated searches of biometric

data, store images electronically, and exchange fingerprints on a 24-hour daily basis. ABIS has been designed to support military forces in the field as they encounter unconventional warfare opponents who conceal their identities to avoid capture as an enemy combatant or terrorism suspect.

Field applications for biometrics have been in place since the mid-1990s. One of the first to be developed was the Biometric Automated Toolset (BAT), as DoD war planners recognized the value of a system that could detect persons of interest in a hostile environment. That system was not compatible with other U.S. Government databases, however, in particular the FBI’s library of 50 million fingerprints that are stored in its IAFIS system.

ABIS was launched to resolve this incompatibility problem, adapt more efficient ways of capturing biometrics in the war theater, and, under the Next Generation version, add additional biometrics that could improve accuracy of the identification process. ABIS is now considered to be one of the three major databases maintained by the Federal Government that contain information on known and suspected terrorists, along with IAFIS and the DHS IDENT system.

3.2.2 Program Description

3.2.2.1 Development Details and history
To work effectively on the battlefield and in hostile territory as a tool to detect enemies and terrorists, ABIS must be capable of performing fast one-to-many searches (i.e., scanning an entire biometric database for a match without using pointers to a particular record) across a very large number of records. Additionally, the system must be configured to facilitate matching attempts against non-DoD records held by the FBI and DHS.

With these goals in mind, the DoD Biometric Fusion Center in West Virginia launched the first phase of the ABIS development program. Identix Corporation, now a division of L-1 Identity Solutions, offered a scalable, standards-based, commercial off-the-shelf (COTS) solution also called ABIS®. The Identix ABIS platform was found to provide speed, matching accuracy, and the flexibility to incorporate other biometric data and not just fingerprints. The COTS approach paid off, as DoD moved quickly to deploy an ABIS system that is capable of handling thousands of queries per day from warfighters in Iraq.

An industry team led by Northrop Grumman oversaw the development of the Next Generation update. By June 2009 NG-ABIS was ready for field use. It improves on the first version by offering search times that are 14-28 times faster, interfacing with other collection and intelligence systems, and generating fewer questionable results. Most

54 Identically named, ABIS is a registered trademark now owned by L-1
significantly, NG-ABIS employs multi-modal fusion algorithms that enable records to be matched using fingerprint, face, or iris recognition technology.

3.2.2.2 Configuration
The AFIS platform is designed to interface with several existing systems. On the back end, the database is capable of querying other government databases such as IAFIS and IDENT. On the operational side, AFIS communicates with applications such as the previously deployed BAT and the Biometric Identification System for Access (BISA). The Identix ABIS® software provides the matching engine, and IBM supplies the blade-type servers that store the data.

3.2.2.3 Operations
NG-ABIS is able to provide identity management support during operational encounters, to control base access, and to manage detainees. In this scenario, U.S. forces capture biometric and biographic data using existing applications such as BAT and BISA. These systems are configured to forward data to ABIS for data storage and checks of external systems such as IAFIS and ABIS. The results are used to determine if the subject should be detained, granted permission to access a U.S. military base, or released from custody.

3.2.2.4 Success Stories
ABIS and its enhanced update, NG-ABIS, have been successfully deployed and fully integrated with legacy applications such as BAT and BISA. The system is routinely handling thousands of queries per day, and was developed very quickly by adapting COTS products for criticial data management and storage functions. The system was built to handle additional biometric information as existing technologies are improved and new technologies are introduced that can help U.S. ground forces improve upon friend-or-foe identity requirements. An example of how the system works in a practical sense is shown in the following diagram.⁵⁶

---

3.2.2.5 Problems Encountered

No documentation was found to indicate there have been major problems with the development and deployment of ABIS. This can be attributed to the classified nature of ABIS and, on the positive side, a system architecture that draws on COTS products to achieve system reliability.

3.2.2.5 Future enhancements

As noted above, NG-ABIS expands ABIS capabilities with multi-modal (fingerprint, palm, iris, and face) storage and matching, watch list capability, and improved integration with interagency repositories. Since it is based on adaptations of COTS products and utilizes open architecture to minimize development and speed deployment, NG-ABIS can be expanded and enhanced as new technologies are made available. The system also takes advantage of low-risk, cost-effective blade hardware to optimize system availability and scalability, and ensure Continuity of Operations (COOP). The system is currently designed to support up to 2.4 million finger, face, palm, and iris records, and a lesser
number of latent prints. The built-in scalability of NG-ABIS ensures that the system can be upgraded to meet operational demands.

3.3 CAC

The **Common Access Card (CAC)** is a United States Department of Defense (DoD) credential that is issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees and State Employees of the National Guard and eligible contractor personnel.\(^{57}\)

The CAC, a “smart card” containing a 64 kilobyte integrated circuit (IC) chip from which data is extracted, or “read,” by contact with or proximity to the chip surface, is used as a general identification card and for authentication to enable access to DoD computers, networks, and certain DoD facilities. It also serves as an identification card under the Geneva Conventions. The CAC is intended to enable military and civilian personnel to encrypt and cryptographically sign email, securely log on to sensitive systems and databases, and automate identification functions at gates and other access points. As of 2008 DoD has issued over 17 million CAC cards, (including reissues to accommodate changes in name, rank, or status and to replace lost or stolen cards). DoD has deployed an infrastructure at over 1000 sites in more than 25 countries around the world and is rolling out more than 1 million card readers and associated middleware.

The program used to issue CAC IDs is called the Real-Time Automated Personnel Identification System (RAPIDS). The system is secure and monitored by the DoD at all times. Users have to go through a special course and be certified to issue CACs. Different RAPIDS sites have been setup throughout military installations in and out of combat theater to issue new cards.

3.3.1 Background and History

The CAC program began with a November 10, 1999 memo from Dr. John Hamre, Deputy Secretary of Defense.\(^{58}\) While the CAC was not initially intended to incorporate biometric features or functions, the credential concept quickly evolved so that within a year or two the operating concept did include room for biometric authentication. The initial rollout was planned to cover four million participants, including active duty military, selected reserve personnel, civilian employees, and some contractors. By 2003 extensive plans had been developed for an evolution to a biometric-capable credential.\(^{59}\)


The potential population to be served by the program, including families, retirees, and those receiving medical or economic benefits, was placed at 13 million.

By 2006 DoD announced that an improved CAC met the HSPD-12 presidential directive and its related standards. \(^{60}\) DoD was thus the first executive branch department to adapt the FIPS-201 requirements and come into full compliance with the government-wide identity initiative.

### 3.3.2 Program Description

#### 3.3.2.1 Configuration

From program inception the CAC was envisioned as a smart card based identity management application. Along with its IC chip, the CAC incorporates a Code 39 barcode, two-dimensional barcode (PDF-417 standard), a magnetic stripe, and a digital photograph. The magnetic stripe is not encoded at time of issuance, but is intended for local use to assist with automated access control. By using COTS technology and following industry practices, the CAC card platform and architecture mirror the approach of the credit card industry.

Fingerprint biometric data and a digital face image are stored on the CAC chip as well as in DoD databases. This configuration allows for many different identity management applications that can draw on either fingerprint or face recognition biometrics to confirm identity, depending on the equipment available and the level of security needed. These include:

- Using the CAC as a “pointer” to the biometric template on a server and using that server to compare the live data against the template
- Using the same pointer process to look up a template on a workstation and perform the match operation on the workstation
- Extracting the biometric template from the CAC and using the main server to compare that template against the live data
- Storing the biometric template on the CAC and performing the match operation on the CAC (“match on card”)

In addition to setting up a global card issuance network, DoD has continued to develop subsystems that support and improve card management. These include a PIN reset application built by the Defense Manpower Data Center (DMDC), a web portal for adding applications to the CAC, a contractor verification system to improve management of DoD contractors, and automated tools for managing card inventories.

As noted above, cards are issued at many sites around the world using the RAPIDS network. The original version of RAPIDS has been updated to include Public Key Infrastructure certificate management, Java\(^{\text{™}}\) card applications,\(^{61}\) and a variety of card reader and personalization (i.e., printing) solutions.

---

\(^{60}\) [http://www.cac.mil/](http://www.cac.mil/)

\(^{61}\) Java is a trademark of Sun Systems; for further information see [http://www.java.com/en/](http://www.java.com/en/)
RAPIDS creates, modifies and uses data stored in the Defense Enrollment Eligibility Reporting System (DEERS), which offers accurate and timely information on all DoD uniformed services, family members, civilian employees, and guard/reserve personnel. The DEERS database, which contains records on over 23 million people, is closely integrated with the RAPIDS issuance infrastructure.

As of 2008, DoD has issued over 17 million smart cards. (This number includes reissues to accommodate changes in name, rank, or status and to replace lost or stolen cards.) As of the same date, approximately 3.5 million un-terminated or active CACs are in circulation. DoD has deployed an issuance infrastructure at over 1000 sites in more than 25 countries around the world and is rolling out more than 1 million card readers and associated middleware.

### 3.3.2.2 Operations: DBIDS

The CAC is in use throughout the DoD civilian and military organizations. Several applications have been developed at the field level to use the card’s inherent biometric identification capabilities with access control needs. The Defense Biometric Identification System (DBIDS) is the largest, relying on fingerprint identification technology to accurately identify staff entering military installations. In addition to identifying CAC holders, DBIDS also validates the identity of foreign nationals, U.S. embassy personnel, delivery drivers, children of DoD employees and others who have been issued a compatible card.

DBIDS predates the development of the CAC system by several years, having been created at the request of U.S. Forces Korea in 1998. Now fully compatible with the CAC, DBIDS facilitates the verification of identity through the use of wireless, handheld devices that can read fingerprints and barcodes. Within a few seconds personal information and a color photo of the card holder are displayed on a screen, enabling quick verification in high volume operational environments such as base gates and checkpoints.

### 3.3.2.3 Success Stories

The CAC infrastructure is the largest known internal identity management system in the world. The system includes all DoD military and civilian staff and provides a common platform on which to base a wide variety of physical and logical access control solutions. Deployment took place under challenging conditions, including unforeseen practical problems with establishing issuing stations in Afghanistan and Iraq. On an anecdotal basis it appears that having an architecture based on a common card format has provided a number of benefits, some of which have been achieved by using the card to improve local processes as well as on a DoD-wide basis:

- White Sands Missile Range integrated an electronic signature system with the CAC to securely eliminate paper, save postage costs, and reduce process time from days to seconds
Scott Air Force Base reported a savings of $400,000 in manpower costs by taking advantage of CAC biometric information to automate processing at the base’s access gates.

Air Force Pentagon officials have documented a 90 percent drop in username-password help desk calls by using the CAC for logical access, thus reducing administrative costs.

An Army base in Korea has used the CAC to detect fraudulent attempts to enter the facility by imposters.

3.3.2.4 Problems encountered

There are several issues that have evolved with the use of the CAC. These include:

- **Mission capability:** While most CAC users remain at the same workstation, an ever-increasing number of government websites are requiring the use of the CAC for authentication. The problem with this approach is that many people who have a legitimate requirement to access these websites, are, by the very nature of their duties, required to access those sites from non-CAC enabled workstations. This occurs most frequently when users are on temporary duty elsewhere at workstations over which they have no administrative control, and on which they may be prohibited from installing a CAC reader. Thus, the username/password approach must be kept as a backup to CAC employment for these personnel.

- **Scalability:** The US Army has enjoyed password or single point access to many SSL-secured websites through its “Army Knowledge Online” program for several years. However, authorities believe that password-based logins are obsolete and vulnerable to compromise, especially as systems expand.

- **Non-Windows support:** The Common Access Card is based on X.509 certificates with software middleware enabling an operating system to interface with the card via a hardware card reader. Although card manufacturers such as Schlumberger provided a suite of smartcard readers and middleware for both Linux and Windows, not all other CAC systems integrators did likewise. In an attempt to correct this situation, Apple has done work for adding support for Common Access Cards to their operating system right out of the box using the MUSCLE (Movement for the Use of SmartCards in a Linux Environment) project. 62

- **Common problems:** The microchip is fragile and regular wear can make the card unusable. On a technical level, the cards have certificate issues where users cannot log on even though their computers are set up correctly. In addition, different CAC vendors have posed issues with different card reader systems.

62 [http://cisr.nps.edu/pub_techrep.html](http://cisr.nps.edu/pub_techrep.html)
3.3.2.5 Future enhancements

DoD recently upgraded the CAC to double data storage and memory capacity from 32 kilobytes to 64 kilobytes, improve compatibility with PKI-compliant systems, enable easy encryption of emails, and improve the electronic authentications processes used for physical and logical access control systems. DoD has announced no plans to make additional major changes to the CAC architecture and platform as of this writing.
3.4 Combat Zone Applications of Biometrics

In a previous, more classic model of warfare where battle lines were more clearly understood and respected, identification of the enemy was a simple matter of uniform recognition. If the other person wore the ‘wrong’ uniform, shoot. True, even in the most remote pages of the history of warfare, there were spies and infiltrators, but not so many that they comprised a serious threat mandating extraordinary protective measures. Current terrorist or insurgent-based combat, on the other hand, has changed the rules and it has become essential to be able to identify friend from foe quickly and reliably. The enemy today wears no distinctive uniform, but blends into the local native population with no obvious means of identification. Fortunately, the evolution of the modern terrorist is coincidental with the development of ruggedized, biometric field equipment useful for capturing and exploiting several conventional and some not-so-conventional biometric modalities.63

Conventional biometric modalities used in combat operations include fingerprints, iris images, and facial images. Unconventional biometric modalities or markers include gait analysis, scars, marks, and tattoos. While the latter may not meet the definition of a true biometric in terms of longevity, permanence, or ease of modification, the modern war fighter applies whatever tools he or she can against an unforgiving and dangerous opponent.

Solutions for the application of modern biometrics in today’s combat zones evolved (and are evolving) ‘on-the-run’ as US armed forces entered the Middle Eastern combat zones. Those approaches that seemed to work received a green light for further development. Since 2005, the DoD reports at least 83 biometric programs existing at some stage of development and application. Of these, 27 are considered “large” (i.e., 200 enrollees and/or involving $1 million or more). Many of these are classified and the details of which are, naturally, unavailable—as are the successes and failures. The really successful ones become even more classified and those that fail are quietly disposed of. At least two programs have been widely discussed and promoted by the DoD for combat applications: the “Biometrics Automated Toolset (BAT)” and the “Biometric Identification System for Access (BISA).” The BAT has been effectively applied in many applications to identify individuals from native populations who have been captured or interdicted during operations. The BISA program, on the other hand, is a program used to control access to US DoD facilities in Iraq by local nationals and other non-DoD personnel. This section provides information concerning these two programs. Most other DoD projects have similar goals and use similar resources.

3.5 Biometrics Automated Toolset (BAT) 64

Biometrics Automated Toolset (BAT) is a laptop-based application that is designed to collect biometric data in the field and store the information on a central server. Since its initial deployment it has evolved into a useful, tactical, multi-modal biometric suite of

---


64 http://www.eis.army.mil/DoDBiometrics.htm
devices that collects and fuses biometric (fingerprints, iris images, and facial photographs) and biographical information on people of interest to DoD.

### 3.5.1 Background and History

The BAT program was undertaken to support a pressing demand to identify potential threats to U.S. forces during field operations in civilian areas. Both the Army and Marine Corps knew that infiltrators were concealing themselves in the local population, but had no means to accurately ascertain who was a “person of interest” and who represented no apparent threat.

To address this need U.S. forces needed a rugged solution that depended on a remote hand held reader to capture the information from suspects and relay it by wireless link to laptops that could communicate with a central repository. The resulting solution was deployed in 2003, well before DoD introduced ABIS in 2004. BAT continues to be used in both the Afghanistan and Iraq theaters, and has since been fully integrated with ABIS.

### 3.5.2 Program Description

#### 3.5.2.1 Development

Initial development focused on the reader. This first BAT reader\(^{65}\) enabled the capture of iris and fingerprint information along with a small data set of biographic information. This equipment suite evolved in function and utility from the original set to the PIER series\(^{66}\), all of which have been incorporated into the BAT system.

The portable device is now known as the Handheld Interagency Identity Detection Equipment (HIIDE), which is the size of a large camera. While unit prices for the reader are fairly high (often quoted in the $2,000-$10,000+ range), by 2008 nearly 7000 units had been distributed to military forces in Iraq and Afghanistan. The device is reputed to be the world’s first hand-held tri-biometric system that allows users to enroll and match via any of the three primary biometrics: iris, finger and face. The user interface simplifies the process of entering biographic data to create a comprehensive database on the enrolled subject. The HIIDE can function while connected to a host PC or when operating in the field untethered. HIIDE can store up to 22,000 full biometric portfolios (2 iris templates, 10 fingerprints, a facial image and biographic data) to create comprehensive records on enrolled subjects.

#### 3.5.2.2 Configuration

The BAT configuration consists of the HIIDE unit, the BAT client, and the BAT server. The BAT client stores the iris, fingerprint and facial image and houses the algorithms needed to perform a match of live information against stored records. The HIIDE handheld device captures information for download to the client, and is also capable of performing matching operations against the biometric portfolios temporarily stored in the unit. The BAT server is networked with the BAT client. The server updates other servers on the BAT network and provides information to other systems for intelligence

---

\(^{65}\) Developed by Securimetrics, now a part of L-1 Identity Solutions

\(^{66}\) [www.l1id.com/pages/47-hiide-series-4](http://www.l1id.com/pages/47-hiide-series-4)
analysis. A typical procurement for a deployed unit may consist of six BAT servers, nearly 500 BAT clients, and 250 HIIDE units. The system life cycle is estimated to be 5-7 years.

**3.5.2.3 Operations**
The primary purpose of BAT is to identify a person of interest, meaning a potential terrorist or insurgent who may be concealed within a civilian population within or near a combat zone. As used by soldiers trained in its operation, BAT can link such individuals to past activities solely through the use of 1:n ("one to many") checks of iris, fingerprint, and face recognition biometrics; no validation of biographic data is needed to perform the searches.

In addition to uncovering threats, the system can be adapted to assist with detainee operations, border control, base access, humanitarian assistance and displaced persons management.

**3.5.2.4 Success Stories**
BAT has been credited with identifying “hundreds of high-value individuals” in 2008 alone, according to DoD officials at the Arlington, Virginia based Biometrics Task Force (BTF). One example given by BTF describes how BAT was used to decrease violence in a village near Baghdad International Airport by using HIIDE to verify credentials. As a result, residents benefited from increased security and Iraqi police gained influence and authority with village occupants.

BAT has been used in Afghanistan to screen local job applicants, and in Iraq to weed out police recruits whose biometrics matched those of previously identified terrorists and insurgents. By 2008 HIIDE units had collected over 240,000 records for inclusion in ABIS and enabled the match of more than 40,000 of the records.

**3.5.2.5 Problems encountered**
Public sources contain no documentation of problems that have been encountered in the development, deployment and use of BAT.

**3.5.2.6 Future enhancements**
In October 2008 software upgrades were made to the HIIDE units, and capacity was increased to 42,000 records. Further changes in early 2009 made available an expansion module that raises capacity to 240,000 records, and adds a GPS receiver, USB connectivity and a wireless ready port.

---

67 FY 2003 deployment by the Marine Corps; see http://www.marcorsyscom.usmc.mil/sites/cins/Fact%20Books/All_Source/BAT-HIIDE.pdf
3.6 Biometric Identification System for Access (BISA)\textsuperscript{70,71}

BISA is a $75 million DoD force protection initiative\textsuperscript{72} currently in use in Iraq to facilitate the access of local nationals into U.S. military facilities. At the heart of the project is a biometrically-authenticated credential using fingerprint, iris, and facial images, as well as selected biographic information to tie the credential to the bearer. Cards are issued to local or third-country nationals, coalition forces and certain non-DoD U.S. citizens.

The need to improve security at overseas installations originates from a memo sent by then-Deputy Secretary of Defense Paul Wolfowitz in May 2005,\textsuperscript{73} prompted by a 2004 bombing in Mosul, Iraq. General sources describe BISA as follows:\textsuperscript{74}

“\textit{The Biometric Identification System for Access (BISA)...collects multi-modal (fingerprint, facial and iris) biometric information and biographical information to produce a smartcard or PIN badge to control local and third-country nationals, coalition forces and a limited number of U.S. citizens accessing U.S.-controlled facilities in Iraq. BISA is self-contained – it includes all biometric enrollment, conversion and storage, transmission, badge production and verification devices. When a BISA badge holder requests entrance to a controlled facility, the individual is verified through a match between a live scan of the person’s fingerprint with the fingerprint stored on the smartcard.}”

While three modalities collected, only the fingerprints are used in routine access control applications. The other modalities are invoked in the event there is any question regarding the true identity of the card bearer. The operational BISA implementation involves over 120 Army personnel.

3.6.1 System Description

BISA is a smart card based biometric system that exists in three configurations. Tier I is the original base access configuration fielded at eight installations throughout Iraq, while Tier II is a modified system architecture that significantly reduces hardware and maintenance costs of each BISA site. A BISA “Dayworker” configuration is under development for the needs of the Iraqi day worker population not enrolled with BISA credentials.

3.6.2 BISA Capabilities

Public information on how BISA works in an operational environment is limited. According to official sources the system offers the following capabilities:

- Collects biometric data on all local- and third-country nationals in Iraq
- Screens applications against ABIS/IAFIS

\textsuperscript{70} \url{http://www.eis.army.mil/DoDBiometrics.htm}
\textsuperscript{71} \url{http://biometrics.org/bc2008/presentations/173.pdf}
\textsuperscript{72} \url{http://www.biometrics.dod.mil/Newsletter/issues/2005/July/v1Issue5_a1.htm}
\textsuperscript{73} \url{http://wv.ewa.com/BISA.htm}
\textsuperscript{74} \url{http://gen.com/microsites/reports/peo-eis-guide/pm-dod-biometrics.aspx}
• Produces and issues access credentials based on application’s fingerprint and photo
• Digitally verifies live biometrics at each entry to assure identity via electronic comparison to stored biometric templates on a smart card
• Tier II has capabilities of Tier I system with a smaller footprint, easily packaged/moved in pelican cases, and uses available secure networks
• Issues an International Civilian Aviation Organization (ICAO) compliant card at some Iraqi airports

3.6.3 Progress to Date\textsuperscript{75}
The BISA update was performed with remarkable speed, going from concept to prototype in 59 days and from prototype to field deployment in 71 days. Over 220,000 enrollments were completed by November 2008\textsuperscript{76}, and over 90,000 BISA badges had been issued. About 1,000 matches had been forwarded to Military Intelligence for review.

3.6.4 Schedule (FY09 Planned Activities and Deliverables)
During Fiscal Year 2009 the Army planned to complete several important enhancements to BISA that would better support field operations and integrate the system with other applications. These actions include:
• Support interoperability with other systems
• Begin use of Iris on Card
• Complete Tier II Deployment
• Complete Dayworker Deployment
• Complete Adjudication Website enhancements
• Complete NGIC Watchlist with Biometrics Deployment
• Complete Tier I Technical Refreshment Deployment
• Complete Patch and Remote Management Deployment
• Complete Agent of Certification Authority to extend ATO
• Continue sustainment and operations of Tier I and Tier II sites

4 The National Institute of Standards and Technology (NIST)\textsuperscript{77}
NIST performs research in measurement, evaluation and standards for fingerprint matching and interchange, criminal justice information systems, face recognition and multi-modal biometrics. NIST’s focus is on assisting with and supporting the needs of the following programs and initiatives:

\textsuperscript{75} http://assets1.csc.com/government/downloads/12683_3.ppt
\textsuperscript{76} http://www.securitymagazine.com/Articles/Feature_Article/BNP_GUID_9-5-2006_A_10000000000000464914
\textsuperscript{77} http://biometrics.org/bc2008/presentations/110.pdf
- R&D needs of industry, government, and academia
- Border Security
  - USA Patriot Act and Enhanced Border Security and Visa Entry Reform Act
  - US-VISIT (entry/exit system for foreign visitors)
- Law Enforcement
  - FBI - Integrated Automated Fingerprint Identification System (IAFIS)
  - Next Generation Identification (NGI)
- National Institute of Justice
  - DNA analysis
- Defense and Intelligence
  - The R&D components of Defense and Intelligence Communities
  - Identity Management
  - Personal Identity Verification (PIV) ID card for federal employees and contractors
- US Government Coordination
  - White House National Science & Technology Council (NSTC) Subcommittee on Biometrics and Identity Management
  - Coordination and involvement in the “National Biometrics Challenge”
  - Registry of Government recommended biometrics standards
  - Publication of the Identity Management Task Force Report

NIST’s biometrics work generally falls into three main categories: standards development, product testing and evaluations, and other research related to biometrics. NIST's primary technology concerns include Fingerprints (including latent images), face, iris, voice, DNA and multimodal combinations of biometrics.

4.1 Standards Development

NIST’s standards development work includes not only its own NIST Standards for biometrics work, but direct involvement in both national (ANSI) and international standards (ISO/IEC) panels as well, often leading the development of new and innovative standards. Notable among these standards are:

- NIST Special Publication 800-76-1 -- Biometric Specification for Personal Identity Verification

NIST is also active on the International Committee for Information Technology Standards
(INCITS M1), and on the International Organization for Standardization International
Electro-technical Commission (ISO/IEC SC37) committee. These standing committees
meet several times a year and will, no doubt, continue to generate new or modified
standards to recognize emerging technologies and capabilities.

4.2 Biometric Modal Research and Testing
NIST conducts on-going research into existing and new biometric technologies to
evaluate and advance the art and science of biometric identification in each of the
primary modalities.

4.2.1 Fingerprint Projects
NIST manages and oversees several on-going testing projects for fingerprints. These
include:

- Evaluation of Latent Fingerprint Technologies (ELFT), a project designed to help
  improve and advance latent fingerprint matching technologies.

- Proprietary Fingerprint Template Testing (PFT). Since June of 2003, NIST has
  been conducting tests of fingerprint-based biometric matching systems using
  vendor supplied SDKs and comparing these systems to an internal fingerprint
  matching system. Fingerprint matching systems from vendors are being evaluated
to insure that the accuracy of the matchers used in various existing and planned
government systems (including US-VISIT) are comparable to the most accurate
available COTS products. The main result obtained from these evaluations is an
estimate of how well commercial products performed one-to-one matching for
verification over a wide range of fingerprint image qualities. The relative
accuracy of thumbs and index fingers is also investigated.78

- Minutia Exchange Tests (MINEX), a program of NIST-coordinated development
efforts that are aimed at improving the performance and interoperability of core
implementations of the INCITS 378 and ISO/IEC 19794-2 fingerprint minutia
standards.79

- Slap Fingerprint Segmentation Evaluations (SlapSeg). The Slap Fingerprint
Segmentation Evaluations are assessments of the accuracy of algorithms used to
segment “slap” fingerprint images (i.e., those acquired by having the individual
place all ten fingers on the capture device at the same time) into individual
fingerprint images.

SlapSeg evaluations are conducted by NIST on behalf of the Department of Justice (DOJ)
Justice Management Division (JMD), which is overseeing the IDENT/IAFIS Integration
Project.

78 http://fingerprint.nist.gov/SDK/
79 http://fingerprint.nist.gov/minex/
The use of slap fingerprints for background checks is being considered in a variety of U.S. Government fingerprint systems, including US-VISIT and IAFIS. The segmentation of slap fingerprints is known to have an associated error rate, but no rigorous evaluation of current slap segmentation algorithms has ever been conducted. Knowing whether existing segmentation software is feasible for operational use will be of practical interest and value to policymakers.

The sponsors of this study want to determine the practicality of these operational scenarios:

- Batch segmentation of large databases of live scan, paper, or mixed slap fingerprints
- Real-time segmentation of live scan slap fingerprints at the time of capture

This evaluation will determine the accuracy (and error rate) of existing slap segmentation algorithms on a variety of operational-quality slap fingerprints, as well as the ability of segmentation algorithms to detect when segmentation was successful.80

4.2.2 Face Projects

NIST has sponsored several events to evaluate the performance of facial recognition systems. Principal among these have been:

- Face Recognition Grand Challenge (FRGC). The primary goal of the FRGC was to promote and advance the use of face recognition technology to support research efforts in the U.S. Government. FRGC developed new face recognition techniques and prototype systems and increased performance by an order of magnitude. The FRGC was open to face recognition researchers and developers in companies, academia, and research institutions. FRGC ran from May 2004 to March 2006.

- Face Recognition Vendor Tests (FRVT). FRVTs provide independent government evaluations of commercially available and prototype face recognition technologies. These evaluations are designed to give U.S. Government and law enforcement agencies information that could assist them in determining where and how facial recognition technology can best be deployed. In addition, FRVT results help identify future research directions for the face recognition community.

FRVT 2006 followed five previous face recognition technology evaluations - three Face Recognition Test (FERET) evaluations (1994, 1995 and 1996) and FRVT 2000 and 2002. The FERET program introduced evaluations to the face recognition community and helped advance face recognition from its infancy to the prototype system stage. By 2000 face recognition technology had matured from prototype systems to commercial systems. The Face Recognition Vendor

80 http://fingerprint.nist.gov/slapseg04/TestPlan.html
Test 2000 (FRVT 2000) measured the capabilities of these systems and their technical progress since the last FERET evaluation. Given the significant rise in public interest in face recognition technology by 2002, FRVT 2002 was designed to measure technical progress since 2000, to evaluate performance on real-life large-scale databases, and to introduce new experiments to help understand face recognition performance better. Since FRVT 2002 a number of new face recognition technologies have been developed that have the promise of improving performance by an order of magnitude. The Face Recognition Grand Challenge (FRGC) was organized to develop new face recognition technologies. The technologies being developed under FRGC include high resolution still image, three dimensional face scans, and multiple sample still imagery. FRVT 2006 will determine if the goals of FRGC are met; progress in face recognition since FRVT 2002; and effectiveness of new face recognition technologies being developed.\textsuperscript{81} Both FRVG and FRVT programs would be expected to be replicated in the forthcoming years as technologies and algorithms advance.

4.2.3 Iris Projects

Although a much newer technology than fingerprinting, iris recognition technology holds great promise for personal identification purposes. The error rates achievable from iris images and templates are much lower than fingerprints and the failure to enroll rate is much lower, both significant determinants in the utility of a biometric technology. Since 2005, NIST has been evaluating the performance of iris products and algorithms.\textsuperscript{82}

- Iris Challenge Evaluation (ICE). In 2005 and 2006, NIST conducted and managed the Iris Challenge Evaluation (ICE) projects. The ICE 2005 was a technology development project for iris recognition. The ICE 2006 was the first large-scale, open, independent technology evaluation for iris recognition. The primary goals of the ICE projects were to promote the development and advancement of iris recognition technology and assess its state-of-the-art capability. The ICE projects were open to academia, industry and research institutes.
  
  - ICE 2005 consisted of an iris recognition challenge problem that was distributed to potential participants.
  
  - ICE 2006 consisted of a large-scale, open, independent technology evaluation of iris recognition technology. To guarantee an accurate assessment, the ICE measured performance with sequestered data (data not previously seen by the researchers or developers). A standard dataset and test methodology was employed so that all participants were evenly evaluated.

While no official announcement has been made of subsequent ICE evaluations, they will undoubtedly occur from time to time as iris technology advances.

\textsuperscript{81} http://face.nist.gov/frvt/
\textsuperscript{82} http://iris.nist.gov/ICE/
4.2.4 Voice Projects

Voice recognition has two aspects that often get confused. The first or older meaning of the term is actually speech recognition, which refers to the ability of an automated device to recognize words, terms or phrases regardless of the identity of the speaker. Speaker identification, in this context, is based upon the speaker uttering a particular password or PIN, or responding to multiple queries for passwords or phrases; for example “This is my voice and it is my password.” Access is granted simply if the speaker uses the correct word(s) or phrase(s). This approach to “voice recognition” has been in use for number of years (at least 20-30 years in our experience). This use does not involve establishing the unique identity of the user, just the fact that the user is in possession of the correct word sequence.

The second and much newer aspect of voice recognition is the automated identity recognition based upon the waveform characteristics of the speaker’s voice. Like images of the face, the human voice is a desirable type of biometric in that capture of the trait can be done non-invasively, unobtrusively, and, in theory, at some distance, giving rise to the utility of voice recognition for intelligence and investigative purposes as well as access control.

Two problems have emerged, however, with the use of this type of voice recognition. The first is that it is difficult to match the waveform of a voice recorded for archive purposes in one audio environment with the waveform of the same voice captured in a different environment. The second problem is one of spoofing. Entertainers have long demonstrated an outstanding ability to mimic the sound of a more familiar personality. Testing, however, has often revealed that they may achieve this by producing a different waveform that combines in the listener’s ear to resemble the target, thus confounding the voice recognition problem.

NIST has been conducting “Speaker Recognition Evaluations” since 1996, focusing on the waveform analysis approach to speaker identification with varying degrees of success.83

4.2.5 Trends

NIST recognizes the importance of adapting multiple biometrics into government identity solutions, and is committed to several research project to support the migration to such “multi-modal” (using more than one biometric to confirm identity; also referred to as biometric fusion) applications of the technology. The FBI Next Generation Identification effort is a prime example of efforts to progress beyond dependency on fingerprints alone and instead incorporate voice, iris, facial and other biometrics to refine and improve the identification process. According to the FBI:

83 http://www.itl.nist.gov/iad/mig/tests/sre/
“The NGI Program will advance the integration strategies and indexing of additional biometric data that will provide the framework for a future multimodal system that will facilitate biometric fusion identification techniques. The framework will be expandable, scalable, and flexible to accommodate new technologies and biometric standards, and will be interoperable with existing systems. Once developed and implemented, the NGI initiatives and multimodal functionality will promote a high level of information sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification.”

With programs such as NGI gaining momentum, NIST will be engaged in a number of activities that will support the evolution from a “uni-modal” to multi-modal environment. These include:

- Conducting benchmarking and performance evaluations
- Developing and evaluating next generation biometric capabilities
- Integrating standards for new biometrics with the existing standards process
- Evaluating system interoperability, such as FBI IAFIS/NGI and DHS US-VISIT
- Researching ways to improve the quality of biometric images and templates
- Expanding the NIST “Grand Challenge” concept to include face-offs of multimodal solutions
- Conducting a specific evaluation of a multimodal application of face and iris technology

5 In Conclusion
The U.S. Government has led the development of large scale biometric identification systems with the establishment of the AFIS program in the late 1970s. Additional applications were slow to evolve, with the INSPASS and IDENT programs being two of the few examples of systems that were deployed prior to September 11. The only other major program to be in deployment mode by late 2001 was the DoD CAC, which led the way for the integration of smart card and biometric technologies on a massive scale.

The events of September 11 accelerated the development of systems to address unique operational problems. The Department of Defense has implemented ABIS, BATS and BISA to solve challenges in the Middle East theaters, and disparate agencies have recognized the need to make biometric identification platforms communicate with one another. Meanwhile the White House took note of the lack of standards – and security – inherent in identity systems used by the Executive Branch and mandated that all departments comply with the HSPD-12 order.

---

84 [http://www.fbi.gov/hq/cjisd/ngi.htm](http://www.fbi.gov/hq/cjisd/ngi.htm)
85 INSPASS was introduced by the Immigration & Naturalization Service in 1992 as an automated border clearance system. The program enrolled over 100,000 travelers in what became the largest voluntary system in existence at its peak in the mid-1990s. The program was terminated in 2002 and is being replaced by the DHS Global Entry and Nexus systems.
Not long ago, critics were saying that biometric technology was in its infancy and not ready to be used to meet critical identification needs in the fight against terrorism and the criminal justice arena. The robust performance of IAFIS and the DoD field applications has proven otherwise. Where government uses of biometrics have fallen short of initial expectations it is usually due to two main reasons: departments have been slow to fully implement HSPD-12 requirements, especially as they relate to interoperability between agencies and other departments; and the U.S. has been less successful than other countries in finding an efficient formula for using biometrics to handle routine identity chores in border control, airport access control, and other public-oriented applications.

Biometrics have moved into the mainstream to combat enemy infiltration, weed out terrorists, streamline the identification of government personnel, and quickly verify the identity of criminals in custody. As the new decade approaches, the lessons learned in these highly successful programs are certain to be drawn on to solve other pressing identity management challenges.