

# Improved Border Security Now!

## The Identity Document Inspection System (IDIS)

**Rev. 3 – 8/12/03**  
**AssureTec Systems, Inc.**

**Summary:** An estimated two million aliens enter the U.S. each year using forged or altered documents. Current plans to detect these documents will ultimately provide some solution, but not for many months or years.

An automated Identity Document Inspection System (IDIS) can be put into a pilot program within 30 days. This system would require little or no operator training and no more than 3 seconds to operate. Fully implemented the cost would be less than \$35 per current forged/altered document now entering the U.S. to set up and \$12 per false document to operate. Assuming less time needed for inspectors to pursue false positives, it's possible that it may actually pay for itself. In addition, the system would provide authentication of all travel documents and timely information vital to U.S. control authorities from documents issued by both VISA-Required and VISA-Waiver countries.

The problem is estimated by U.S. Immigration and State Department authorities to be "thousands of illegal entries" per month using forged or altered U.S. Visas and Visa-Waiver country passports (more than 2,000,000 every year!). Current planning for the US VISIT (formerly Exit-Entry) Program does not seem to be focused on the 50-60 million U.S. VISAs currently in circulation. These documents are valid for up to ten years. Also, VISIT will not have full impact until many infrastructure, technology, and global privacy/political issues are resolved many months (years?) from now. The first phase, which will be operational in January 2004, only begins the process with the capture of data and biometrics on visitors from Non-VISA Waiver countries.

Automation of the inspection of travel documents, more specifically the U.S. VISA, will provide the Inspections division of the Department of Homeland Security (DHS) Bureau of Customs and Border Protection a tool to dramatically reduce the risk of someone being able to enter the country using a fake document. Closely-held, hidden security features can be automatically verified and all relevant information extracted from the VISA in about the same time as currently required to just extract the machine-readable data. The need for such technology is further increased by the reorganization associated with the formation of DHS. This consolidation resulted in the merging of the inspections process under new management with many new front-line inspectors having limited experience in recognition of real/fake travel documents.

If used as a front-end screening process linked to the State Department's Open Source Information System, the on-line database of VISA issuance information, the system would take advantage of rapid response data retrieval. Also, photo images are available on-line for the last few years of issuance (approximately 20 million of the estimated 50-60 million issued). Hence, automated data verification and photo comparison (automated 1:1 graphic comparison, no facial recognition technology required!) can be used, either to resolve questionable ALERT situations and, thereby, avoid false alarms, or as an additional screening tool for all transactions.

It is anticipated that the technology will dovetail well with the requirements for the entry side of the US VISIT program and offer immediate improvement in border security. It is proposed that

a “pilot” project commence very quickly to validate these recommendations with the intent that deployment follows quickly upon successful completion. This project will require close cooperation between the State Department document security staff, Homeland Security Border Protection, and AssureTec Systems (a very limited number of vendors even have potential technology to reliably detect the unique Visa properties and time is of the essence).

Due to the sensitive nature of how this technology would function in its full embodiment, only an overview is presented herein. Costs are scalable according to the scope of the project approved, but they can be characterized in terms of \$7,000 to \$9,000 per station inclusive of server support, or about \$0.1 to \$0.2 per visitor per year entering the United States.

### **Background: The U.S. VISIT Program:**

There is a great deal of effort going into improvement of Border Security via the legislated “Exit-Entry” program now called U.S. VISIT. This project has become an “umbrella” for all efforts associated with improvement in security as it relates to people entering and leaving the country. Initially the focus is on data/biometric collection from “VISA-Required” countries and improvements in the process of issuing and authenticating VISAs.

A strong emphasis has been on collection of biometric information to provide a means to verify that the person leaving the country is the same person as the one who entered and that the bearer of a VISA is the person to whom the VISA was issued. Much discussion is on going relative to which biometric or combination is best suited to provide this verification.

It is legislated that all visitors entering the U.S. must have an approved biometric as a part of their countries passport process for “VISA-Waiver” countries and included as a part of the United States’ VISA issuance process. These provisions are to be implemented in two parts by the end of 2003 and the end of 2004. In this same time frame, the systems for the collection, management, and verification of this information are to be in place at all exit-entry points into the U.S.

The objectives are very clear. First and foremost is to be able to check the identities of people seeking entry into the U.S. against lists of people that we do not want to grant entry to! Second, is to be sure that we are able to reconcile the identity of people departing the country against those we have granted permission to enter the country. That is, to prevent someone from exiting the country on another person’s identity so as to convey the impression that the person who entered has left or to allow someone whom we do not wish to leave the country to do so under someone else’s identity. Lastly, information collected under the program can be evaluated and correlated for patterns of activity which would indicate intent to commit illegal acts.

In terms of combating terrorism, smuggling, illegal flight and supporting many other legitimate law enforcement objectives; the benefits of such a program are readily understood.

**Program Challenges:** In order to implement this program many obstacles need to be overcome. Some of the challenges involve the cooperation of other countries. Several of these challenges require substantial changes/upgrades to core infrastructure and processes/procedures. Many of the processes will require close scrutiny to pass current “privacy” guidelines or legislative changes to accommodate a new paradigm which balances security against legitimate individual rights.

Changes to the issuance process for new travel documents include both a new document features to adapt to new requirements and, equally important, changes to ensure that new “high security” documents are not issued to “high risk” individuals. High security documents issued to high risk individuals is worse than issuing them low security documents because it leads to a natural human tendency for great reliance on what the document represents and less attention to the behavior of the individual! This is a classic parallel to the ready acceptance of a U.S. passport as a “lower risk” when traveling worldwide than when the traveler is using a passport from most other countries.

**Long Timeline:** Given the challenges of such a mammoth project, years of effort and billions of dollars will be spent both in the U.S. and overseas to meet the objectives of the VISIT Program. There are more than 1500 issues/types of passports from the 237 countries of the world. The majority of these are not yet machine-readable! Virtually none are biometrically supported beyond the photo contained therein. There are 100s of millions of these documents in circulation! The U.S. has approximately 63 million passports and 50-60 million VISAs in circulation!

Many of these documents will still be valid ten years from now! Even if laws were changed, funds appropriated, and technical teams in place to move forward, this legacy would take many years to “flush!” The process will have to adapt to accommodate this reality. Pragmatically this leads to the conclusion that there will be no substantial impact on security for several years as the VISIT Program is implemented.

The overwhelming challenges of modeling, specifying, and budgeting for such a program have understandably taken the attention of critical resources away from specific actions that would impact current border security and led to a generally adopted view that “we will include that in Exit-Entry.”

### **Overview: The Identity Document Inspection System**

**Introduction:** There has been great progress in bringing together many government agencies and their resources in the fight against terrorism. However, there is a step which can be taken that will provide potentially dramatic returns on an investment and likely dovetail very well into the VISIT Program.

There are many peripheral benefits to the proposed system which are consistent with the objectives of VISIT; however, accelerated implementation is fully justified by considering only the benefits returned from being able to reliably determine the risk associated with the authenticity of U.S. VISAs presented at ports of entry much sooner. There are “hundreds to thousands” of bogus VISAs detected monthly and sources estimate that for every one detected at least ten fakes/alterations are missed!

There would be many side benefits by way of detection of fraudulent documents from VISA – Waiver countries; virtually immediate reconciliation against Open Source; checks against “watch” lists in addition to Interagency Border Inspection System (IBIS); and immediate notification of law enforcement and intelligence agencies of border crossing activity.

**Constraints:** There are four major constraints on the current system which inhibit improvement in the inspection process. One constraint is time available for document inspection. Another factor is the human limitations; such as, training/turnover, boredom, distraction, job dissatisfaction, et al. A third concern is increased security risk. Dissemination of the many

levels of security built in to these documents to a large number of people (10,000-15,000 inspectors), combined with the creation of a large body of training documents and reference materials, presents a substantial risk that the information necessary to create very exact duplicates would be sold or stolen. Also, people (even excellent inspectors!) are subject to intimidation, bribery, and blackmail. The fourth is an antiquated IT infrastructure with limited network bandwidth and resulting poor performance that makes comprehensive real-time primary (frontline) inspection station with access to State Department VISA data and photo for validation prohibitive.

Today, fraudulent documents are most often detected at secondary inspection stations after the frontline inspector has detected suspicious behavior of some kind. The primary intent of the proposed Identity Document Inspection System (IDIS) is to provide frontline inspectors with a tool that will greatly heighten their awareness of potentially fraudulent VISAs and other documents and provide immediate validation against VISA records if available. This objective can only be achieved through use of a secure, automated, audited process. Obviously, a link to IBIS would be maintained and the database checked and updated as it is today, except that stolen document records and other "watch" lists would be queried with full name, document number, et al as appropriate.

Each of the constraints on the current system is overcome by IDIS. Much better document examinations are conducted in less time, without human limitations while maintaining absolute protection of the document security characteristics being validated! Independent secure network communications with a gateway to IBIS would preserve compatibility, yet provide real-time Open Source validation and reporting to interested control authorities.

**System Elements:** The elements of the IDIS are a secure document reader/authenticator workstation (with support for current applications), an independent local site (port of entry) network, a site server, and a secure WAN link to a central server and to the State Department. The reader/authenticator automatically identifies the travel document and analyses it according to parameters in its encrypted database. The network/servers provide the mechanisms for audited, data dissemination, and IBIS connection, database/software updates and the State Department Open Source database link if/when available.

**The Process:** The process is very similar to that currently used for reading ICAO standard documents without the constraint of ICAO compliance. Greet the traveler, accept the document and place it on the reader/authenticator for 1-2 seconds while interacting with them, glance at a screen to view the risk assessment results and any prompts appropriate to the risk level. Total time for the entire process is 2-5 seconds. Two to three seconds would be all that is needed for just a US VISA analysis.

The key to robustness is the degree of cooperation between the issuer of the document under test and the reader/authenticator vendor. The vendor can read or measure characteristics observable under a variety of light sources. If these characteristics conform to international or other published standards then they can be validated with a very high degree of accuracy. However, these characteristics are also available to would be forgers! Other characteristics are "obvious" under particular frequencies or angles of light. A little experimentation on a sample document will reveal the overall "look and feel" of these characteristics. Known characteristics of forgery or alteration attempts are readily detected as well.

The challenge to the forger is to attempt to simulate a document or to alter a stolen document well enough to pass any anticipated inspection. Since it is very unlikely that the document will

be looked at using anything other than normal available room light and even then with only a cursory look due to time constraints, many forgery/alteration attempts ignore features that are not revealed in normal lighting. As the forgery attempts become more sophisticated, given the funding of a country, criminal syndicate, or terrorist organization, then more attention is paid to sophisticated features in order to pass even a secondary examination. This is often just a matter of expense and not a technology challenge.

Even if data and a photo image were consistently available and retrieved for human comparison from Open Source, the human foibles and time constraints would still exist and “look-alike” document thefts remain an open issue.

**The Solution:** The value of a U.S. VISA is so great that the investment in forging them can provide a substantial return (not always in money!). The best answer to maximize security and limit false rejects is to enable very close, very secure cooperation between the issuer, inspector, and solution provider to enable validation of security features that are not publicly documented nor readily detectable.

Detection of “hidden” security features, as with the breaking of a security code, requires multiple samples of a variety of documents containing variations that can be correlated. These samples in sufficient quantity and variety are not available even if the would be forger knew where to look! Many of these features are “keyed” and/or data, time, issuance location dependent. Often they are a combination of all of the above.

It is not appropriate in this document to speculate on what the U.S. VISA might have for hidden security features, in addition to its many observable security characteristics. However, it is certain that such features exist and equally certain that, if examined, they would reveal even the most sophisticated forgery! Since, the U.S. VISA was designed by the State Department, the document experts there, such as Arthur Lindberg and John Mercer, can corroborate their presence. The applicability of State Department’s Open Source Information System can be confirmed with Ted Holstead at State Department. Certainly the viability of detection of physical security features and observable remnants of alteration/forgery attempts can be responded to by Chief Intelligence Officer Jim Hesse and his people, such as Pete Riley at the Department of Homeland Security (DHS) Forensic Development Laboratory. Some examples of readily detectable VISA alterations are illustrated in the Appendix. These examples are not very sophisticated and do not reflect the depth of examination possible.

It is not clear to this author who within Commissioner Robert Bonner’s DHS Bureau of Customs and Border Protection would be the person having operational responsibility. Of course Robert Mocny, Director of the VISIT Project Office or Shonnie Lyon from his group can provide details regarding U.S. VISIT as it might relate.

**Phase One “Pilot:”** Obviously, the above assertions need to be confirmed. If confirmed then a major gap in the entry process can be closed very quickly. A “pilot” test, which evaluates the effectiveness of the technology, could be commenced within 30 days of the initiation of such a project. This could be extended to include a test of a link to Open Source (or a surrogate system) for real-time cross validation. If successful, deployment could commence very quickly at major ports. The same system would also capture data from all travel documents and authenticate them according to all observable security features. The extent to which other countries cooperate in providing similar “hidden” information would determine the level of confidence that VISA-Waver countries passports can be authenticated.

This phased test could also provide a cost-effective accelerator for evaluation of an approach to add another biometric beyond the photo to the VISA/bearer validation process. If the Open Source (or surrogate) system were extended to add a fingerprint, facial or other template(s) then there would be yet another level of cross-check available to link the traveler to the VISA. This check would not be necessary except in cases where the "risk factor" is determined to warrant it.

This would be an intermediate step in the implementation of the full VISIT Program, but it could link to a process that would accelerate inclusion of a new biometric without the need to implement a full VISA (very, very expensive) recall. The authentication of a VISA as a part of the first-time embarkation (air/sea) or border crossing (landport) for a traveler could be used as the database link to post to the Open Source system the needed information. This subjects frequent travelers to the process just once and provides a "de facto" enhancement to existing VISA information without a full re-enrollment. It is of great concern that a very reliable authentication of the VISA presented and verification of the identity of the bearer (photo comparison) are made to avoid registering an imposter.

A biometric-enabled VISA process which does not require storage of biometric parameters on/in the document would be much less expensive and more secure. No matter what data storage mechanism is used it will be subject to "hacking" or data transfer. This risk is not present with central data/image storage.

The issue of improvement in the enrollment process for new/old travel documents remains, but, even there, IDIS technology is of use in the authentication of "breeder" documents used to verify the identity of applicants.

**COST PROJECTIONS:** There are a great many variables to consider when estimating costs. This document is not intended to be a proposal, but it is important to understand on a relative basis the magnitude of what is being recommended. A "pilot" development program supporting two sites for 30-45 days to provide a "proof of concept" is estimated to require 2-3 full-time equivalent government employees and \$250,000 in vendor cost for labor and material.

Assuming a full rollout at the approximately 4500 entry stations nationwide and up to 500 embarkation points and embassies worldwide, including the required project management and server/network support, the installed cost would be about \$65,000,000 and require approximately \$25,000,000 in annual support, maintenance, update, and program/operational costs. Inclusion of support for one or more biometrics (beyond a photo) is not included, but does not represent a substantial cost impact beyond the direct costs associated with equipment and licenses for the specific biometric selected.

Virtually all of this cost would represent re-usable equipment/effort under U.S. VISIT. Even if the cost is not totally recovered, it is very inexpensive compared to the potential harm done by allowing 2,000,000 illegal entrants to the U.S. each year! It is also just a small fraction of the project cost estimates being floated for the total U.S. VISIT program.

# **APPENDIX**

## **Typical “Observable” Issues with VISA Authenticity**



Passport Numbers do not match.

Issue Dates do not agree. MRZ Issue Date is wrong format

Blue wave line lacks distinct USA letters in photo area indicates photo alteration.



Passport Numbers do not match.

Issue Dates do not agree. MRZ Issue Date is wrong format

Issuance date cross check and foil serial number rane are inconsistent.

Blue wave line lacks distinct USA letters in photo area indicates photo alteration.



Passport Numbers do not match.

Issue Dates do not agree. MRZ Issue Date is wrong format

Blue wave line lacks distinct USA letters in photo area indicates photo alteration.



**Example of Good VISA UV**

Note UV Seal over photo area and dark/dull area behind UV Seals

NOTE: General increased level of background brightness indicates solvent exposure.

Missing UV Seal over photo area indicates photo alteration.

Bluish areas indicate tampering caused by "washing" with solvent to remove original information.