

RELEASED IN FULL

P 578

INFORMATION MEMORANDUM  
S/ES

UNCLASSIFIED

TO: Under Secretary Green

FROM: CA - George Lannon, Acting

SUBJECT: The U.S. Passport and Biometrics

- Section 303 of the Border Security Act of 2002 requires the U.S.G. to issue aliens visas with biometric identifiers by October 26, 2004; it also requires Visa Waiver Program countries to certify that they issue passports that incorporate biometric and document authentication identifiers.
- Although the border security laws do not address the issue of biometrics in the United States passport, the Department may be compelled to include biometric identifiers in the U.S. passport to satisfy demands by Visa Waiver Program governments that might impose reciprocal requirements on U.S. citizens.
- Passport Services fully supports the goals of the border security laws. However, the biometric selected for use in the visa process is not necessarily the appropriate biometric for use in the United States or other nations' passport processes.
- The use of ten print fingerprint enrollment is unnecessary to ensure document integrity. Moreover, the national and international infrastructure is not ready to accommodate the introduction of full-image fingerprints. The massive amount of data needed to store full-image fingerprints would overwhelm the finite amount of storage space on travel documents, requiring expensive solutions for on-board data storage solutions.
- United States passports and passports of other nations must be machine-readable by all countries to which passport bearers may travel. In short, passports must be globally interoperable while visas do not. Because passports require a globally interoperable solution, it is important to

# UNCLASSIFIED

UNCLASSIFIED

consider a biometrics and document authentication solution that can work for all passports.

- Passport Services proposes that the U.S. passport carry a facial template and favors facial recognition as the primary biometrics concept for global interoperability.

Attachment:

Tab 1 - The U.S. Passport and Biometrics

Tab 2 - NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability

Tab 3 - An Introduction to Evaluating Biometric Systems

UNCLASSIFIED  
UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

-1-

## The U.S. Passport and Biometrics

### Summary

Passport Services fully supports the goals of the border security laws. However, the biometric selected for use in the visa process is not necessarily the appropriate biometric for use in the United States or other nations' passport processes.

The use of ten print fingerprint enrollment is unnecessary to ensure document integrity. Moreover, the national and international infrastructure is not ready to accommodate the introduction of full-image fingerprints. The massive amount of data needed to store full-image fingerprints would overwhelm the finite amount of storage space on travel documents, requiring expensive solutions for on-board data storage solutions.

Full image fingerprints rather than facial images or fingerprint minutiae templates are also vulnerable to misuse. Instead, we seek a workable solution in the form of facial recognition that both operationally and politically, ensures document integrity and global interoperability of passports, as well as the protection of the privacy of U.S. citizens.

### The passport and visa processes have different requirements.

Visas issued by the United States need only be machine readable by border control authorities at United States ports of entry. This basic requirement allows a multitude of possible biometrics and document authentication solutions that can be exclusive to the United States.

However, United States passports and passports of other nations must be machine-readable by all countries to which passport bearers may travel. In short, passports must be globally interoperable while visas do not. Because passports require a globally interoperable solution, it is important to consider a biometrics and document authentication solution that can work for all passports, particularly the United States passport, but also those of U.S. Visa Waiver Program countries.

The International Civil Aviation Organization (ICAO) establishes standards for passports and visas. The standards are intended to promote document security and global interoperability. ICAO is currently engaged in a process of scenario testing to identify the biometric that it considers globally interoperable. ICAO has already indicated that facial recognition technology best meets the travel document business processes of most passport and visa

UNCLASSIFIED  
UNCLASSIFIED

# UNCLASSIFIED

UNCLASSIFIED

-2-

issuing authorities since those nations already capture the face as part of their normal business process.

## Fingerprint technology should not be used in the U.S. passport.

The unilateral imposition of fingerprint requirements would be problematic for both the United States and other passport issuing authorities.

- Some nations' laws will not permit the storage of fingerprints in databases and will not use fingerprints in their passports. In some countries, the association of fingerprints with criminal connotations still remains.
- Some nations have indicated informally that, if fingerprints are unilaterally imposed upon them, their citizens may wish to find a destination other than the United States in which to spend their travel dollars. The impact upon the economy must be calculated in the decision on a choice of biometrics.
- The use of full images of fingerprints on travel documents opens up a privacy vulnerability that predictably will be resisted by privacy advocates in the United States and other nations. Even the International Biometrics Industry Association warns against the use of full fingerprint images and instead endorses the use of minutiae templates that cannot be reverse engineered to obtain persons' fingerprints.
- Data files for full fingerprint images are enormous in size, requiring 8 - 10 thousand bytes of storage per image. The imposition of full fingerprint images will automatically make passports and insert visas of the United States and other nations unacceptable for storage of such large file sizes. More expensive data storage solutions such as integrated circuit chip technology would be required.
- Full fingerprint images would also create inefficiencies, add delays in the enrollment process, and would create delays at ports of entry where their slow download and comparison speeds (due to large file sizes) could create gridlock situations at already overcrowded airports.
- Fingerprint technology is an intrusive technology that may be resisted by American citizens.
- For all of the aforementioned reasons, Congress itself may find fingerprinting of American citizen travelers repulsive to the notion of what we stand for as free Americans. Any form

UNCLASSIFIED

UNCLASSIFIED

# UNCLASSIFIED

UNCLASSIFIED

-3-

- of biometrics solutions employed in the U.S. passport must be acceptable to Congress and the American public. The Department must be prepared to establish a highly transparent process of working with our oversight committees on the selection of a biometric and the prescribed use of the biometric as it concerns U.S. citizens. We anticipate much more concern and resistance to fingerprint technology than any other form of biometrics. Full fingerprint images stored in databases and on-board passports that would be read by other nations will be nearly impossible to justify.
- If any form of fingerprint technology is mandated for the passport, it should be in the form of a minutiae template that will at least prohibit the skimming of full fingerprint images from travel documents and would be small enough to store practically on travel documents.

## Facial images are the best biometrics solution for U.S. passports.

Passport Services and passport issuance authorities of other nations already capture the face of its citizens. Facial recognition technology can be more easily integrated into our business process. Of all the biometrics concepts, it has the greatest chance of being accepted by the traveling public and other nations since it requires no additional information to be captured and stored.

We recognize that facial recognition technology currently is not the most accurate biometric. However, it is making advances through government test programs sponsored by DOD and other entities. Recent scenario testing of facial recognition by other nations indicates that one-one facial verification of persons can be successful when tested and employed in a specific business process and environment (i.e. passport issuance and control). The use of facial recognition technology itself serves as a major deterrent to those who might attempt to perpetrate document fraud. Deterrence would be accomplished if a potential fraud perpetrator recognized that in nine attempts out of ten, the fraud perpetrator would be caught.

Facial recognition is non-intrusive. The simple capture of one's face by a camera system causes no contact with the capture device as does fingerprint technology.

Watch list data is more likely to include facial images rather than fingerprints of terrorists and others that would attempt harm to the U.S. The potential for accumulating face data to match against in watch lists is greater than the potential of gathering fingerprint data on terrorists. The draft report from the National

UNCLASSIFIED  
UNCLASSIFIED

# UNCLASSIFIED

UNCLASSIFIED

-4-

Institute of Standards and Technology (NIST) infact states the Face Recognition Vendor Test 2002 (FRVT2002) will show that "facial recognition is a viable technology for verification and "watch lists" identification." Based on FRVT 2002 - "facial recognition provides an 90% probability of true verification with a 1% probability of false verification."

## National Institute of Standards and Technology.

The National Institute of Standards and Technology (NIST) is eminently qualified to assist in the selection of biometrics solutions for visas. NIST's technical credentials cannot be challenged. The biometrics testing that is currently being performed by NIST and its initial reporting that it preliminarily views full fingerprint images as the optimum biometric solution is exactly what one would expect in a laboratory test. In the confines of a laboratory and in a purely technical sense, NIST's initial assessment may be accurate. However, the biometrics solution selected by the United States, for the visa process and for inclusion in passports of Visa Waiver Program countries, must work successfully in the real world.

The biometrics solution for passports must:

- be globally interoperable.
- protect the privacy of the bearer.
- be capable of being stored in travel documents without the need for large and expensive on-board storage media.
- Ensure that the biometrics solution is acceptable to the American public and Visa Waiver Program countries such as UK, Canada, Australia, New Zealand, Japan and Germany etc., who are our global partners and upon whom this unilateral action by the United States is being imposed.

Full fingerprint images cannot meet these practical, real-world, non-laboratory requirements. NIST's final technical assessment will not consider these practical issues. We must choose an operationally deployable and workable solution.

## Recommendation:

The biometrics solution selected for the visa issuance process should not be necessarily used in the U.S. passport. While fingerprints may be determined to be acceptable for use in the visa process, facial recognition technology should be the primary

UNCLASSIFIED  
UNCLASSIFIED

UNCLASSIFIED

Drafted: CA/PPT/IML:RMCClevey  
CA/PPT/FO/FC:RMHolly  
CA/PPT/PAS:JMercer  
(x32472) 09-27-02

Clearances: CA/VO:JCook (ok)  
CA/PPT/FO:FGFultz (ok)  
CA/PPT/PAS:JHotchner (ok)  
CA/EX/CSD/PS:RMartin (ok)  
CA/PPT:Abarrett (ok)

UNCLASSIFIED