Executive Memorandum

Published by The Heritage Foundation

No. 921
April 13, 2004

E-Passports: A Strategy for Long-Term Success

Ha Nguyen, Paul Rosenzweig, and James Jay Carafano, Ph.D.

As part of the Bush Administration's ongoing efforts to secure America's borders, the Department of Homeland Security (DHS) recently initiated a series of security measures, including an automated entry-exit system called the US-VISIT program. In conjunction with US-VISIT, the Enhanced Border Security and Visa Entry Reform Act of 2002 set a deadline of October 26, 2004, for visa waiver countries (countries such as the United Kingdom and Japan, whose citizens do not need a visa to enter the United States) to issue machine-readable travel documents with biometric information. After the October 26 deadline, visitors from visa waiver countries will be required to present e-passports that contain biometric information (i.e., a digital photograph or digital fingerprints). Many nations are scrambling to implement e-passport programs and are turning to the International Civil Aviation Organization (ICAO) for guidance on standards. However, the ICAO has not established clear criteria for e-passport implementation.

- Congress should consolidate all visa activities within the DHS and extend the deadline for e-passport implementation.
- The Bush Administration should push the ICAO for guidance on e-passport standards.

In order to ensure that America's security needs are met, the Bush Administration should push the ICAO to promulgate clear and cohesive guidelines. Meanwhile, Congress should provide stronger oversight of visa programs by consolidating all visa activities within the DHS and by extending the deadline for e-passport implementation. Proper execution of the e-passport program is important: We should not rush to failure.

Privacy Concerns. The anticipated inclusion of biometrics into e-passports has raised legitimate privacy concerns regarding the security of stored information. The ICAO has not yet issued clear guidelines about whether personal biometric data should be stored in its raw form or in an encrypted form. Using raw biometric data facilitates the interoperability of different countries' passports and their individual data readers. However, its use in passports raises serious privacy concerns because the raw data could easily be stolen and misused.

The success of the e-passport program depends on resolving concerns about interoperability without sacrificing travelers' privacy. The Administration should insist that the ICAO provide guidelines for biometric technology and establish clear international standards to help with system interoperability. Furthermore, it is imperative that the ICAO ensures the privacy of travelers by requiring encryption of all e-passport biometric data.

The United States can help to ensure data privacy by establishing screening systems that conduct one-to-one matches rather than one-to-many matches. In other words, biometric data contained in passports should be used to match the passport to the individ-

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/em921.cfm

Produced by the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation,
214 Massachusetts Ave., NE, Washington, D.C. 20002–4999
(202) 546-4400 heritage.org

ual traveler, rather than identifying the person by matching the passport data to some central database.

One-to-one matching will benefit travelers in many ways. First, it will protect a traveler's privacy by limiting the need to use a large central database to identify individuals because the goal of the e-passport would be only to authenticate the traveler's identity. Second, a one-to-one matching method would be more efficient, reduce check time, and enhance the continuity of operations because it would not require access to a central database. Moreover, since passport readers have a higher rate of success with one-to-one matches, this method will decrease the error rate.

How to Implement an Efficient Process. Implementing an e-passport system that performs one-to-one matches places great reliance on the e-passport as a dependable and authentic document. This poses concerns about how to create tamper-resistant and tamper-evident travel documents. Documents would require some kind of digital watermarking and a smart chip. Security measures placed in e-passports should be able to expose tampering of either the passport or the smart chip.

Greater reliance on travel documents issued by visa waiver countries requires a tighter process for determining whether or not to waive the visa requirements for a particular country. This determination process must include frequent and stringent reviews of a country's e-passport procedures, with oversight to ensure that appropriate measures are carried out.

Under the terms of the Enhanced Border Security and Visa Entry Reform Act of 2002, the authority to waive a foreign country's visa requirement rests with the Attorney General (in consultation with the Secretary of State). However, the Homeland Security Act of 2002 gave the Secretary of DHS exclusive authority to regulate and administer the visa program. To further complicate matters, under the Homeland Security Act, consular officers remained part of the Department of State. Given the national security-aspect of all visa-related affairs and the DHS responsibility to secure America's borders, all visa operations should be consolidated under the DHS—including the authority to award visa waiver status to a country. This would enable the DHS to focus on tightening, improving, and more broadly utilizing the visa function to meet the exigencies of homeland security.

The visa waiver legislation establishes clear and detailed criteria that visa waiver countries must meet. It also requires that the Attorney General—in consultation with the Secretary of State—report to the appropriate congressional committees about these countries' visa waiver applications and status. In order to consolidate all visa functions under the DHS, Congress should give the Secretary of DHS responsibility for overseeing the visa waiver program.

Finally, Congress should provide the DHS with authority to extend the deadline for the implementation of e-passports by visa waiver countries. This would allow time for the implementation of new technologies in a manner that enhances both security and individual privacy.

Conclusion. Effective implementation of the e-passport program is essential to homeland security. To this end, the Bush Administration should push the ICAO to promulgate clear and cohesive international e-passport guidelines, and Congress should consolidate all visa operations within the Department of Homeland Security.

—Ha Nguyen is Research Assistant for Homeland Security and James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University.