January 2010

BORDER SECURITY

Better Usage of Electronic Passport Security Features Could Improve Fraud Detection

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-96, a report to congressional requesters

Why GAO Did This Study

In 2005, the Department of State (State) began issuing electronic passports (e-passports) with embedded computer chips that store information identical to that printed in the passport. By agreement with State, the U.S. Government Printing Office (GPO) produces blank e-passport books. Two foreign companies are used by GPO to produce e-passport covers, including the computer chips embedded in them. At U.S. ports of entry, the Department of Homeland Security (DHS) inspects passports. GAO was asked to examine potential risks to national security posed by using foreign suppliers for U.S. e-passport computer chips. This report specifically examines the following two risks: (1) Can the computer chips used in U.S. e-passports be altered or forged to fraudulently enter the United States? (2) What risk could malicious code on the U.S. e-passport computer chip pose to national security? To conduct this work, GAO reviewed documents and interviewed officials at State, GPO, and DHS relating to the U.S. e-passport design and manufacturing and e-passport inspection systems and procedures.

What GAO Recommends

GAO recommends that DHS implement the systems needed to fully verify e-passport digital signatures at U.S. ports of entry, and in coordination with State, implement an approach to obtain the necessary data to validate the digital signatures on U.S. and other nations' e-passports. DHS agreed with our recommendations.

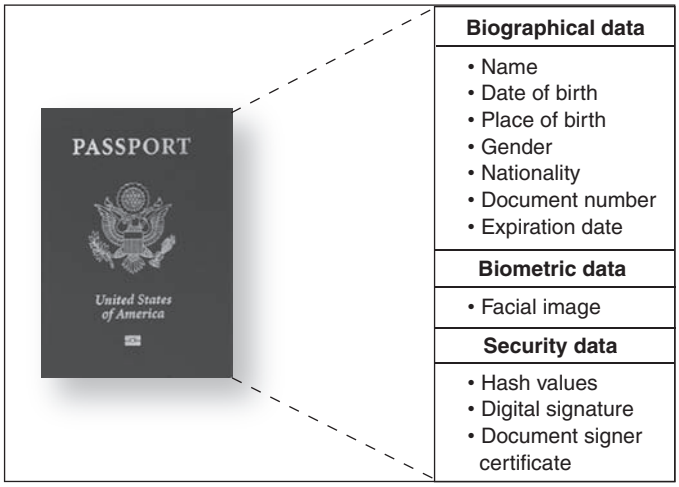
View GAO-10-96 or key components.
For more information, contact Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

State has developed a comprehensive set of controls to govern the operation and management of a system to generate and write a security feature called a digital signature on the chip of each e-passport it issues. When verified, digital signatures can help provide reasonable assurance that data placed on the chip by State have not been altered or forged. However, DHS does not have the capability to fully verify the digital signatures because it has not deployed e-passport readers to all of its ports of entry and it has not implemented the system functionality necessary to perform the verification. Because the value of security features depends not only on their solid design, but also on an inspection process that uses them, the additional security against forgery and counterfeiting that could be provided by the inclusion of computer chips on e-passports issued by the United States and foreign countries, including those participating in the visa waiver program, is not fully realized.

Protections designed into the U.S. e-passport computer chip limit the risks of malicious code being resident on the chip, a necessary precondition for a malicious code attack to occur from the chip against computer systems that read them. GPO and State have taken additional actions to decrease the likelihood that malicious code could be introduced onto the chip. While these steps do not provide complete assurance that the chips are free from malicious code, the limited communications between the e-passport chip and agency computers significantly lowers the risk that malicious code—if resident on an e-passport chip—could pose to agency computers. Finally, given that no protection can be considered foolproof, DHS still needs to address deficiencies noted in our previous work on its computer systems to mitigate the impact of any malicious code that may be read from e-passport computer chips and infect those systems.

Contents of the U.S. E-passport Computer Chip



Source: GAO analysis based on State Department information.