

Final Assessment Report 07-02, November 27, 2006, “WebTrust Assessment of GPO’s Certification Authority – Attestation Report”

GPO implemented a Public Key Infrastructure (PKI) to support its “born digital and published to the web” methodology to meet GPO customer expectations that documents are official and authentic. The GPO PKI also directly supports GPO’s mission related to electronic information dissemination and e-government. The GPO PKI recently became cross-certified with the Federal Bridge Certificate Authority (FBCA) whose certification provisions require that the GPO PKI undergo a compliance review. To satisfy this compliance requirement, the GPO Office of Inspector General (OIG) tasked an independent public accounting (IPA) firm to conduct a WebTrust assessment of its Certification Authority (CA). The assessment was conducted in accordance with the American Institute of Certified Public Accountants (AICPA) “WebTrust Principles and Criteria for Certificate Authorities.” The assessment represents an evaluation of whether GPO management’s assertions related to the adequacy and effectiveness of controls over its CA operations is fairly stated based on underlying principles and evaluation criteria.

A pre-assessment was performed to identify gaps and deficiencies between the current GPO PKI environment and the required criteria of the WebTrust Program for CA. During the final WebTrust phase, controls were tested to gather support for an opinion regarding compliance with applicable WebTrust principles and criteria for certification. As a result of work performed in the final WebTrust phase, the IPA issued an Attestation Report which expresses their opinion that GPO management’s assertions regarding its CA operations is fairly stated in all material respects. This opinion is contained in the final report, which is considered sensitive.