AUDITOR LETTER OF COMPLIANCE

Compliance Audit Requirements
October 29, 2007

In order to evaluate a compliance audit, the following background information is required.

- Identity of the Auditor and the individuals performing the audit;
- Competence of the Auditor to perform audits;
- Experience of the individuals performing the audit in auditing PKI systems;
- Relationship of the Auditor to the entity that owns the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.

The following information regarding the audit itself is required.

- The date the audit was performed.
- Whether a particular methodology was used, and if so, what methodology.
- Which documents were reviewed as a part of the audit, including document dates and version numbers.

In addition to this background, the entity should ensure that, as part of the audit, an audit summary is prepared, signed by the auditor, reporting on the following elements after conducting the compliance audit:

- State that the operations of the entity PKI's Principal CA were evaluated for conformance to the requirements of its CPS.
- Report the findings of the evaluation of operational conformance to the Principal CA CPS.
- State that the entity PKI's Principal CA CPS was evaluated for conformance to the entity PKI's CP.
- Report the findings of the evaluation of the Principal CA CPS conformance to the entity PKI CP.
- For PKIs with multiple CAs, state whether audit reports showing compliance were on file for any additional CA components of the entity PKI

Since the FBCA CP is neutral as to audit methodology, and does not prefer one methodology over another, any audit approach is acceptable to it provided that these points are addressed. For entities choosing a Webtrust audit, so long as the proper

questions are posed at the beginning of the audit, and care is made to tailor the assertions / representations to the FPKI context (see above), Webtrust audits will satisfy the Government's requirements. If one of the entity's assertions (representations) was that the CPS conformed to the CP, then examination of the CPS would be within the scope of the Webtrust audit.

Note: *The FBCA does not require and will not consider any statements with respect to the entity PKI's suitability for cross certification with the FBCA or conformance to the FBCA certificate policies. Such a determination is exclusively the purview of the FPKIPA and its working groups.*