U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT
12-22

Webtrust for Certification Authority
September 18, 2012

U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

September 18, 2012

To

Chief Information Officer

From

Inspector General

Subject

Assessment Report - Webtrust for Certification Authority

Report Number 12-22

Enclosed please find the subject final report. The Office of the Inspector General administered a contract with Ernst & Young LLP (E&Y) to provide an opinion on the Government Printing Office's (GPO) assertions regarding their certification authority process for July 1, 2011 through June 30, 2012. E&Y conducted their work in accordance with attestation standards established by the American Institute of Certified Public Accountants.

E&Y concluded that GPO's assertion is fairly stated in all material respects. E&Y is responsible for the attached report and the opinion expressed therein.

We appreciate the courtesies extended to E&Y and to our audit staff. If you have any questions or comments about this report, please do not hesitate to contact me at (202) 512-0039.

Michael A. Raponi
Inspector General

Enclosure

cc:
Acting Public Printer
Assistant Public Printer, Operations
General Counsel

US Government Printing Office

Report of Independent Accountants

Webtrust for CA

For the Period July 1, 2011 to June 30, 2012

Ernst & Young

Quality In Everything We Do

Table of Contents

Ernst & Young LLP
Westpark Corporate Center
8484 Westpark Drive
McLean, VA 22102
Tel: + 1 703 747 1000
Fax: +1 703 747 0100
www.ey.com

Report of Independent Accountants

To the Inspector General of the United States Government Printing Office and the Management of the United States Government Printing Office Certification Authority:

We have examined the assertion by the management of the U.S. Government Printing Office (GPO) that in providing its Certification Authority (CA) services known as GPO Public Key Infrastructure Certification Authority (GPO-CA) in Washington, D.C. for the Root CA: GPO-CA during the period July 1, 2011 through June 30, 2012, management of GPO has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
  - Certification Practice Statements and
  - Certificate Policy
- maintained effective controls to provide reasonable assurance that
  - GPO's Certification Practice Statements are consistent with its Certificate Policy
  - GPO provides its services in accordance with its Certificate Policy and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - the Subscriber information is properly authenticated; and
  - subordinate CA certificate requests are accurate, authenticated and approved
- maintained effective controls to provide reasonable assurance that
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

for the CA services known as GPO-CA, based on the AICPA/CICA *Trust Services Criteria for Certification Authorities*.

GPO's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of GPO's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at GPO and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, GPO's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, for the period July 1, 2011 through June 30, 2012, GPO management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA *Trust Services Criteria for Certification Authorities*.

The WebTrust seal of assurance for Certification Authorities on GPO's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of GPO's services beyond those covered by the *Trust Services Criteria for Certification Authorities*, or the suitability of any of GPO's services for any customer's intended purpose.

Ernst & Young LLP

August 20, 2012

U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

Assertion by Management of the U.S. Government Printing Office Regarding Its Disclosure of Its Business Practices and Its Controls Over Its Certification Authority Operations During the period July 1, 2011 through June 30, 2012

August 20, 2012

The U.S. Government Printing Office (GPO) operates as a Certification Authority (CA) known as the GPO Public Key Infrastructure Certification Authority (GPO-CA) in Washington, D.C. GPO-CA, as a Root CA, provides the following certification authority services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing
- Integrated circuit card life cycle management

Management of GPO is responsible for establishing and maintaining effective controls over its Certification Authority operations, including CA business practices disclosure in GPO's Certificate Practices Statement, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal control can provide only reasonable assurance with respect to GPO's Certification Authority operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in GPO Management's opinion, in providing its Certification Authority (CA) services known as GPO-CA in Washington D.C., GPO during the period July 1, 2011 through June 30, 2012 —

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its
  - Certification Practice Statements and
  - Certificate Policy

- maintained effective controls to provide reasonable assurance that
  - GPO's Certification Practice Statements are consistent with its Certificate Policy
  - GPO provides its services in accordance with its Certificate Policy and Certification Practice Statements

- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - the Subscriber information is properly authenticated; and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

for the CA services known as GPO-CA, in accordance with the AICPA/CICA *Trust Services Criteria for Certification Authorities* [http://www.webtrust.org/homepage-documents/item54279.pdf] including the following:

CA Business Practices Disclosure

CA Business Practices Management
Certification Practice Statement Management
Certificate Policy Management
CP and CPS Consistency

Service Integrity

CA Key Life Cycle Management Controls
CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Compromise
CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls
CA- Provided Subscriber Key Generation Services
CA- Provided Subscriber Key Storage and Recovery Services
Integrated Circuit Card Life Cycle Management
Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls
Subscriber Registration

Certificate Renewal
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Validation
Subordinate CA Certificate Life Cycle Management Controls
Subordinate CA Certificate Life Cycle Management

CA Environmental Controls

Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Audit Logging

Charles Riddle
Chief Information Officer

John Hannan
Chief Information Security Officer