



U.S. GOVERNMENT PRINTING OFFICE  
OFFICE OF INSPECTOR GENERAL

**ASSESSMENT REPORT**  
**12-23**

---

**Federal PKI Compliance Report**  
**September 18, 2012**

---

**Date**

September 18, 2012

**To**

Chief Information Officer

**From**

Inspector General

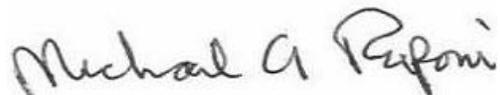
**Subject**

Assessment Report - Federal PKI Compliance Report  
Report Number 12-23

Enclosed please find the subject final report. The Office of the Inspector General administered a contract with Ernst & Young LLP (E&Y) to provide a compliance report of GPO's Public Key Infrastructure (PKI) 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 also issued a Letter of Supplementary Information, concluding that the GPO Principal Certification Authority Certificate Practices Statement conformed in all material respects to the GPO-Certificate Authority and Federal PKI common policies. 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

A decorative graphic on the left side of the page consists of a series of vertical bars of varying heights that taper to the right, meeting a solid yellow arrow that points diagonally upwards and to the right.

# US Government Printing Office

Report of Independent Accountants

Federal PKI Compliance Report

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

## Table of Contents

Report of Independent Accountants .....	1
Management Assertion .....	2
Letter of Supplementary Information .....	5
Summary of Matters Relating to Project Personnel.....	7

## Report of Independent Accountants

We have examined the assertion, dated August 20, 2012, by the management of the United States Government Printing Office ("GPO"), that GPO's Certification Authority (GPO-CA) complied with certain requirements of its Certificate Policy (CP), Version 1.3.1 dated August 17, 2009 and its Certificate Practices Statement (CPS) Version 1.7.1 dated June 3, 2011, for the period July 1, 2011 to June 30, 2012, as well as the requirements of the Federal PKI Authority and all current cross-certification Memorandum of Agreements (MOAs) executed by the GPO-CA with other entities.

Management of the GPO is responsible for its compliance with those requirements. Our responsibility is to express an opinion on management's assertion about the GPO's compliance 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 examining, on a test basis, evidence about GPO-CA's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on GPO-CA's compliance with specific requirements.

In our opinion, for the period from 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.

This report is intended solely for the information and use of the GPO and the U.S. Federal PKI Policy Authority and is not intended to be and should not be used by anyone other than those specified parties.

*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 (CPS), 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.

We confirm, to the best of our knowledge and belief, the following assertions made to you during your examination. With respect to our compliance with certain requirements in the GPO Certificate Policy (CP), Version 1.3.1 dated August 17, 2009, the GPO Certificate Practices Statement (CPS), Version 1.7.1 dated June 3, 2011, as well as the requirements of the Federal PKI Authority and all current cross-certification Memorandum of Agreements (MOAs) executed by the GPO-CA with other entities, for the period of July 1, 2011 through June 30, 2012 GPO has –

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

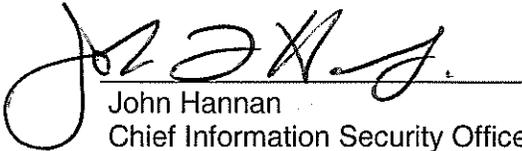
- Certification Practice Statements and
- Certificate Policy
- maintained effective controls to provide reasonable assurance that
  - GPO-CA's Certification Practice Statements are consistent with its Certificate Policy
  - GPO-CA provides its services in accordance with its Certificate Policy and Certification 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;
    - Procedures defined in Section 2 (Publication and Repository Responsibilities) of the GPO CPS are in place and operational.
    - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO CPS are in place and operational.
    - Procedures defined in Section 6 (Technical Security Controls) of the GPO CPS are in place and operational.
    - Procedures defined in Section 7 (Certificate, CARL/CRL and OCSP Profiles Format) of the GPO CPS are in place and operational.
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
    - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO CPS are in place and operational.
    - Procedures defined in Section 6 (Technical Security Controls) of the GPO CPS are in place and operational.
  - the Subscriber information is properly authenticated; and
    - Procedures defined in Section 1 (Introduction) of the GPO CPS are in place and operational.
    - Procedures defined in Section 3 (Identification and Authentication) of the GPO CPS are in place and operational
  - Subordinate CA certificate requests are accurate, authenticated, and approved
    - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO CPS are in place and operational.
- maintained effective controls to provide reasonable assurance that
  - logical and physical access to CA systems and data is restricted to authorized individuals;

- Procedures defined in Section 5 (Facility Management and Operations Controls) of the GPO CPS are in place and operational.
- Procedures defined in Section 8 (Compliance Audit and other Assessments) of the GPO CPS are in place and operational.
- Procedures defined in Section 9 subsections 9.4.4 (Privacy of Personal Information – Responsibility to Protect Private Information) and 9.6.3 (Representations and Warranties – Subscriber Representations and Warranties) are in place and operational.
- the continuity of key and certificate management operations is maintained; and
  - Procedures defined in Section 5 (Facility Management and Operations Controls) of the GPO CPS are in place and operational.
- CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity
  - Procedures defined in Section 6 (Technical Security Controls) of the GPO CPS are in place and operational.



---

Charles Riddle  
Chief Information Officer



---

John Hannan  
Chief Information Security Officer

August 20, 2012

## Letter of Supplementary Information

To the Inspector General of the United States Government Printing Office and the Management of the United States Government Printing Office Certification Authority (GPO CA):

This letter provides supplementary information to the examination performed by Ernst & Young LLP of the assertion by the management of the GPO-CA regarding the certification authority services it provides at <http://www.gpo.gov/projects/pki.htm>.

Management's assertions were based on the American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants WebTrust for Certification Authorities criteria. GPO-CA's management was responsible for its assertion. Our responsibility was to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included examining, on a test basis, evidence about GPO's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on GPO-CA's compliance with specified requirements.

The audit period for this examination was from July 1, 2011 through June 30, 2012. Our examination was performed between March 26, 2012 and July 6, 2012.

We examined the Certificate Policy (CP) for the GPO-CA version 1.3.1, dated August 17, 2009, and the Certification Practices Statements (CPS) for the GPO Principal Certification Authority (GPO-PCA) version 1.7.1, dated June 3, 2011. Multiple Root CAs were not in operation at GPO-CA.

Our examination included, through our testing of management's assertion, the evaluation of GPO-CA's operations for conformance to the requirements of its CPS and the evaluation of GPO-CA's operations for conformance to the requirements of all current cross-certification Memorandum of Agreements (MOAs) executed by the GPO-CA with other entities. In our Report of Independent Accountants dated August 20, 2012, we reported that management's assertion was fairly stated in all material respects.

We have compared the CPS for the GPO-PCA version 1.7.1, dated June 3, 2011, for conformance to the CP for the GPO-CA version 1.3.1, dated August 17, 2009. We found, in all material respects, that the GPO-PCA CPS is in conformance with GPO-CA CP.

We have compared the CPS for the GPO-PCA version 1.7.1, dated June 3, 2011 for conformance to the FPKI Common Policy. For this analysis we utilized the Framework Certification Practice Statement Evaluation Mapping Matrix, Version 2.8 (September 22, 2010). We found, in all material respects, that the GPO-PCA CPS is in conformance with the requirements of the FPKI Common Policy.

We are independent of the GPO for the professional engagement period as required by the AICPA Professional Standards.

*Ernst + Young LLP*

August 20, 2012

## Summary of matters related to project personnel provided by Ernst & Young LLP

To the Inspector General of the United States Government Printing Office and the Management of the United States Government Printing Office Certification Authority (GPO-CA):

The GPO Office of Inspector General (OIG) has asked Ernst & Young LLP (EY or we) to provide certain information to assist in its efforts to provide the Federal Public Key Infrastructure Policy Authority (FPKIPA) with information about the individuals who performed work as part of the WebTrust for Certification Authority (WTCA) examination services; these services are performed in accordance with relevant American Institute of Certified Public Accountants (AICPA) standards. The FPKIPA sets policy governing operation of the U.S. Federal PKI Infrastructure, composed of: the Federal Bridge Certification Authority (FBCA); the Federal Common Policy Framework Certification Authority (CPFCA); the Citizen and Commerce Class Common Certification Authority (C4CA) and the E-Governance Certification Authority. EY makes no representation regarding the sufficiency of this information for the purposes for which this information was requested. That responsibility rests solely with the FPKIPA.

### **Educational level and professional experience**

Client serving personnel (Professionals) EY has provided to the Agency have received a degree from an accredited college or university (or its equivalent if the individual was educated outside of the United States). Certain individuals may also have advanced degrees. The majority of Professionals provided to the Agency are part of EY's Advisory Services (AS) service line. Recruiting efforts for the AS practice focuses on candidates with information technology, accounting, finance and other business-related degrees. Hiring activities and types of Professionals hired into each EY service line, including Assurance and Tax, are generally the same as similar service lines and personnel of Deloitte & Touche, PricewaterhouseCoopers and KPMG (who along with EY, are the Big Four).

The experience levels of Professionals provided will vary based upon various factors including age and length of time the individual has worked since receiving their degree. The amount of professional experience of Professionals may not solely be related to a person's employment period with EY, as EY normally hires a combination of experienced Professionals and Professionals who recently graduated from a college or university. In most cases, the experience level within a rank classification of EY Professionals is generally the same as the other Big Four.

## **Methodologies, policies and procedures**

EY Professionals carrying out WTCA examinations are required to comply with policies and procedures within the EY Advisory Global Practice Manual and related methodologies. In those cases where we do not perform work directly under the supervision and responsibility of Agency personnel as part of an engagement to provide loan staff, and we provide management with our findings and recommendations in those areas where we observe internal controls that, in our view, could be improved, the Advisory Global Practice Manual requires the work and any reports or deliverables to be in accordance with the Statement on Standards for Consulting Services (CS100) of the AICPA. The initial adoption of, and any subsequent changes in, policies and procedures have been reviewed and approved by EY's Professional Practice group.

## **Professional certification and continuing education**

EY encourages its Professionals to obtain a professional certification. In certain service lines, obtaining a professional certification is a requirement for promotion. Individuals in AS are encouraged to obtain a professional certification, but it is not a requirement of employment or advancement. AS' more experienced Professionals (which we refer to as managers, senior managers, executive directors, principals or partners) usually have a professional certification and some may have more than one certification. In the AS service line, the most common certifications are Certified Public Accountant (CPA) (or its equivalent in other countries), Certified Internal Auditor (CIA) as recognized by the Institute of Internal Auditors, Certified Information Systems Auditor (CISA) as recognized by the Information Systems Audit and Control Association, or Certified Management Accountant (CMA) as recognized by the Institute of Management Accountants.

The continuing professional education requirements of the SEC (Securities and Exchange Commission) Practice Section of the AICPA Division for CPA firms are the foundation of EY's professional development policy. The policy applies to all professionals and Government Accountability Office (GAO) Guidance, as confirmed in consultation with GAO personnel, suggests that staff and those individuals not managing an engagement subject to Government Auditing Standards (GAS) may generally satisfy the Government Auditing Standards (Yellow Book) 24 hour CPE requirement through completion of the firm's core training because significant portions of core training content involve auditing under AICPA standards and AICPA standards are incorporated into GAS. As a subset of the 24 hour GAS requirement, our firm has a governmental audit continuing education policy that applies to individuals acting as partner in charge, the independent reviewer, and each individual managing a governmental audit or attestation engagement. An individual's professional development principally occurs through formal learning and on-the-job training. Participation in formal education programs (including self-study programs and meetings organized at least in part for educational purposes) is intended to supplement on-the-job training and other learning activities.

Participation in professional development programs is measured in units of continuing professional education (CPE) credit hours earned in our educational year. EY's educational year is July 1 through June 30. The EY policy for compliance is as follows:

- Commencing with the first full educational year of employment, each professional must obtain at least 20 CPE credit hours each year and at least 120 CPE credit hours during the most recent three-year period.
- Professionals who were not employed during the entire most recent educational year are not required to earn continuing professional education credits in that year.
- Professionals who were employed during the entire most recent educational year, but not during the entire most recent two educational years, are required to have participated in at least 20 hours of qualifying continuing professional education during the most recent educational year.
- Professionals who were employed during the entire most recent two educational years, but not during the entire most recent three educational years, are required to have participated in at least 20 hours of qualifying continuing professional education during each of the two most recent educational years.

Professionals who hold a professional designation or certification other than the CPA certification (e.g., CIA, attorney at law, CISA, CMA) may be subject to continuing education requirements as part of that designation or certification. Completion of courses to meet these requirements may be used to meet the firm's CPE requirements as long as the courses also meet the requirements of the AICPA's SEC Practice Section.

### **Experience Auditing PKI Systems**

The EY executive team assigned to the GPO project has experience in performing audits and implementation of PKI systems and IT security. In addition, certain team members also have participated in a number of other commercial PKI and WebTrust for CA examinations both as a team member and as a quality reviewer. We have incorporated consultations with other EY staff who represent the firm on the AICPA WebTrust Task Force. EY's client roster for PKI projects for governmental agencies other than the GPO includes other US federal agencies as well as foreign governmental monetary organizations.

We are available if you need any additional information or would like to further discuss this memorandum.

*Ernst + Young LLP*

**Summary information for EY executives assigned to the engagement**

<b>Name</b>	<b>Rank</b>	<b>Certifications</b>	<b>Years of experience</b>	<b>In compliance with EY CPE policy (Yes/No)</b>
Werner Lippuner	Principal	CA (Switzerland), CISA, CISM	23	Yes
James Merrill	Executive Director	CPA, CISA	30	Yes
Bruce Hamilton	Senior Manager	CISSP, CISA, CISM, CPA	31	Yes
Timothy Iijima, Ph.D.	Senior Manager	PMP	15	Yes
Staci Angel	Manager	CISA	8	Yes