U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT
REPORT NUMBER 17-27

Federal PKI Compliance Report
September 15, 2017

GPO

U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

Date

September 15, 2017

To

Acting Chief Information Officer

From

Inspector General

Subject:

Assessment Report — Federal PKI Compliance Report
Report Number 17-27

Enclosed please find the subject final report. The Office of Inspector General contracted with Ernst & Young LLP (E&Y) to provide a compliance report of the Government Publishing Office's (GPO) Public Key Infrastructure (PKI) for July 1, 2016 through June 30, 2017. 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 concluded 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

MICHAEL A. RAPONI
Inspector General

Attachment
cc:
Director, GPO
Deputy Director, GPO
Acting General Counsel
Chief of Staff
Chief Administrative Officer

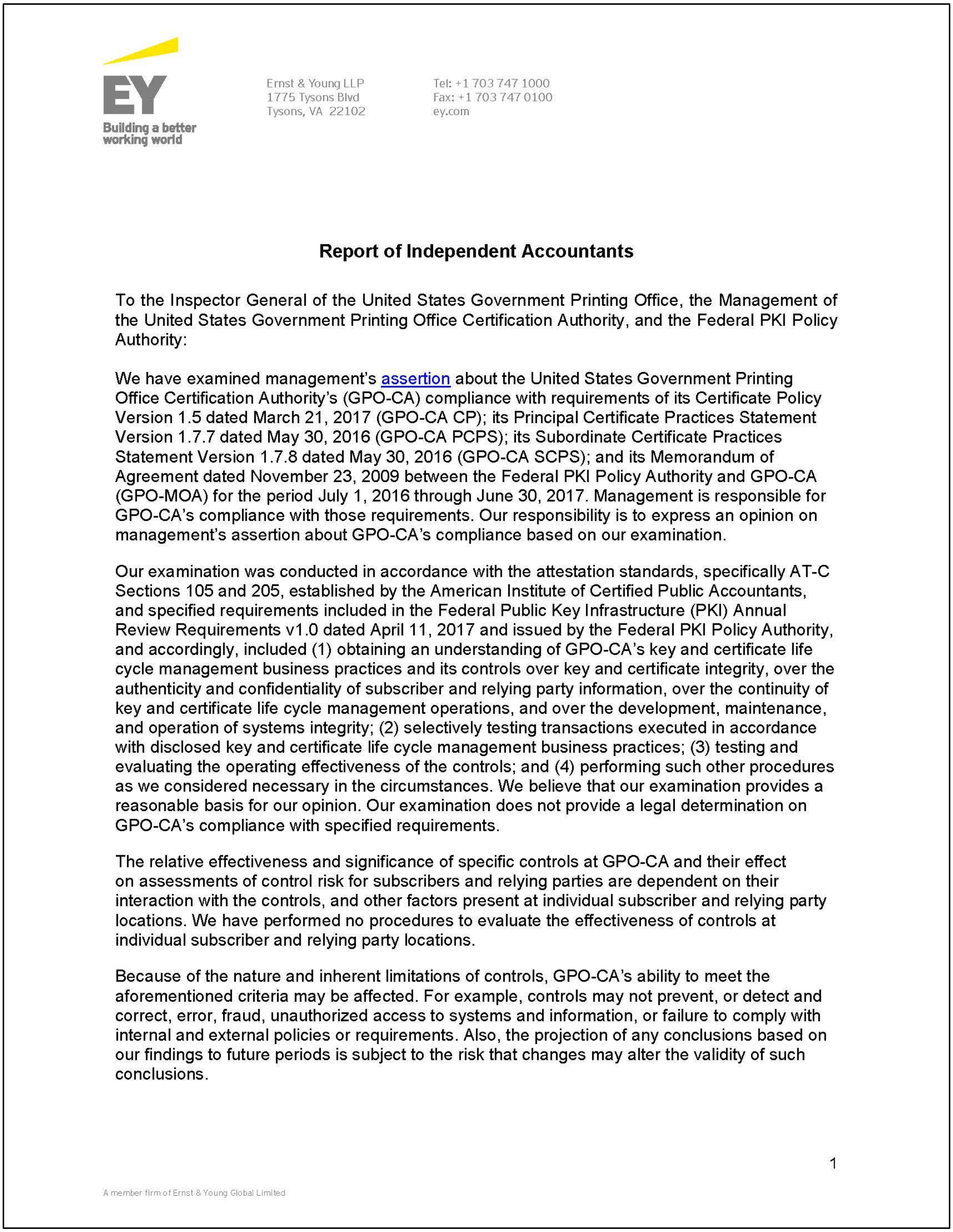
Contents

U.S. Government Printing Office

Report of Independent Accountants
Federal PKI Compliance Report
For the Period July 1, 2016 to June 30, 2017

EY
Building a better
working world

Table of Contents



EY
Building a better working world

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

Tel: +1 703 747 1000
Fax: +1 703 747 0100
ey.com

Report of Independent Accountants

To the Inspector General of the United States Government Printing Office, the Management of the United States Government Printing Office Certification Authority, and the Federal PKI Policy Authority:

We have examined management's assertion about the United States Government Printing Office Certification Authority's (GPO-CA) compliance with requirements of its Certificate Policy Version 1.5 dated March 21, 2017 (GPO-CA CP); its Principal Certificate Practices Statement Version 1.7.7 dated May 30, 2016 (GPO-CA PCPS); its Subordinate Certificate Practices Statement Version 1.7.8 dated May 30, 2016 (GPO-CA SCPS); and its Memorandum of Agreement dated November 23, 2009 between the Federal PKI Policy Authority and GPO-CA (GPO-MOA) for the period July 1, 2016 through June 30, 2017. Management is responsible for GPO-CA's compliance with those requirements. Our responsibility is to express an opinion on management's assertion about GPO-CA's compliance based on our examination.

Our examination was conducted in accordance with the attestation standards, specifically AT-C Sections 105 and 205, established by the American Institute of Certified Public Accountants, and specified requirements included in the Federal Public Key Infrastructure (PKI) Annual Review Requirements v1.0 dated April 11, 2017 and issued by the Federal PKI Policy Authority, and accordingly, included (1) obtaining an understanding of GPO-CA's key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality 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. Our examination does not provide a legal determination on GPO-CA's compliance with specified requirements.

The relative effectiveness and significance of specific controls at GPO-CA 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-CA'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.

The GPO-CA operates a Principal Root CA (GPO-PCA) and its Subordinate CA (GPO-SCA). Multiple Root CAs were not in operation at GPO-CA. We examined the GPO-CA PCPS for conformance to the GPO-CA CP. We have also compared the GPO-CA SCPS for conformance to the GPO-CA CP. We found, in all material respects, that the GPO-CA PCPS and the GPO-CA SCPS are in conformance with GPO-CA CP.

We examined the GPO-CA PCPS and the GPO-CA SCPS for conformance to the Federal Bridge Certification Authority (FBCA) Certificate Policy Version 2.30 dated October 5, 2016 (FBCA-CP). For this analysis we utilized the FBCA Mapping Table dated October 5, 2016. We found, in all material respects, that the GPO-CA PCPS and the GPO-CA SCPS are in conformance with the requirements of the FBCA-CP.

We evaluated GPO-CA's operations, including activity performed by Registrant Authorities (RAs) on behalf of GPO-CA, for conformance to the requirements of the GPO-CA PCPS and the GPO-CA SCPS and we evaluated GPO-CA's operations for conformance to the requirements of the current cross-certification Memorandum of Agreement dated November 23, 2009 between the Federal PKI Policy Authority and the GPO-CA (GPO-MOA).

In our opinion, GPO-CA management's assertion referred to above is fairly stated, in all material respects for the period July 1, 2016 through June 30, 2017.

The examination was conducted by Ernst & Young professionals. The qualifications of the professionals are further described in Exhibit I - Summary of matters related to project personnel. Our fieldwork examination procedures were primarily performed between April 15, 2017 and August 15, 2017.

We are independent with respect to the United States Government Printing Office within Rule 1.200 of the Code of Professional Conduct of the American Institute of Certified Public Accountants.

This report does not include any representation as to the quality of GPO-CA's services beyond those covered by the *Trust Services Principles and Criteria for Certification Authorities, Version 2.0*, those covered by the Federal Public Key Infrastructure (PKI) Annual Review Requirements v1.0 dated April 11, 2017, nor the suitability of any of GPO-CA's services for any customer's intended purpose.

This report is intended solely for the information and use of GPO-CA and the Federal PKI Policy Authority and is not intended to be, and should not be, used by anyone other than GPO-CA and the Federal PKI Policy Authority.

Ernst & Young LLP

September 13, 2017

Exhibit I – Summary of matters related to project personnel

As part of the WebTrust for Certification Authority (WTCA) examination services provided to GPO-CA, in accordance with relevant American Institute of Certified Public Accountants (AICPA) standards, 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 examination. 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 service line. Recruiting for the Advisory practice focuses on candidates with information technology, accounting, finance and other business-related degrees.

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.

Methodologies, policies and procedures

EY Professionals carrying out WTCA examinations are required to comply with EY's policies for performing examinations in accordance with the attestation standards established by the American Institute of Certified Public Accountants.

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 Advisory are required to obtain a professional certification to be promoted to Manager. In the Advisory 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.

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. 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.

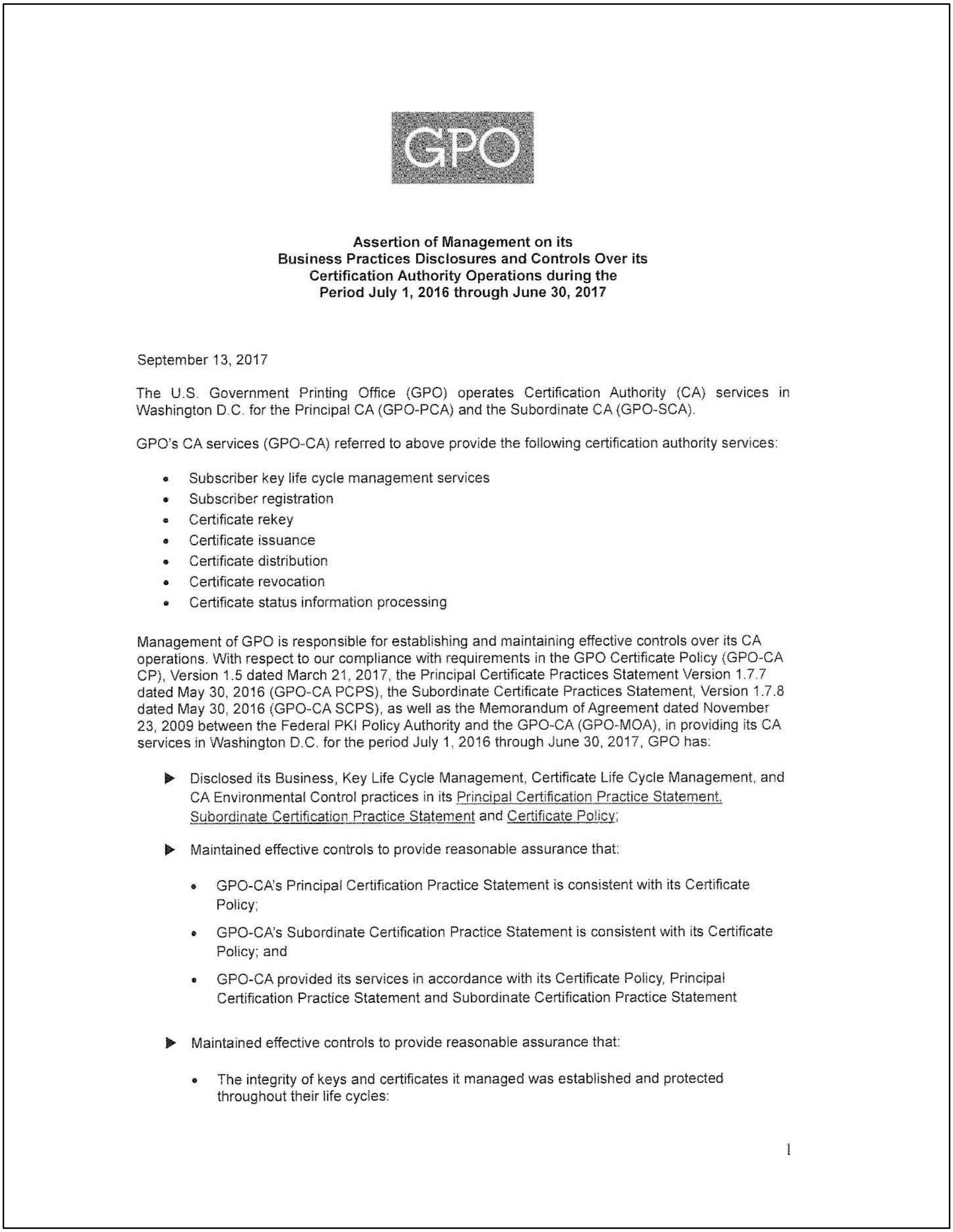
Professionals who hold a professional designation or certification other than the CPA certification (e.g., CIA, CISA) may be subject to continuing education requirements as part of that designation or certification.

Experience Auditing PKI Systems

The EY executive team assigned to the GPO project has experience in performing audits and/or examinations 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 personnel who represent the firm on the AICPA WebTrust for CA Task Force.

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

Summary information for EY executives assigned to the engagement				
Name	Rank	Certifications	Years of experience	In compliance with EY CPE policy (Yes/No)
Werner Lippuner	Principal	CA (Switzerland), CISA, CISM	28	Yes
James Merrill	Executive Director	CPA, CISA	35	Yes
Bruce Hamilton	Senior Manager	CISSP, CPA, CISA, CISM	36	Yes
Staci Angel	Senior Manager	CISA	13	Yes



GPO

Assertion of Management on its
Business Practices Disclosures and Controls Over its
Certification Authority Operations during the
Period July 1, 2016 through June 30, 2017

September 13, 2017

The U.S. Government Printing Office (GPO) operates Certification Authority (CA) services in Washington D.C. for the Principal CA (GPO-PCA) and the Subordinate CA (GPO-SCA).

GPO's CA services (GPO-CA) referred to above provide the following certification authority services:

- Subscriber key life cycle management services
- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

Management of GPO is responsible for establishing and maintaining effective controls over its CA operations. With respect to our compliance with requirements in the GPO Certificate Policy (GPO-CA CP), Version 1.5 dated March 21, 2017, the Principal Certificate Practices Statement Version 1.7.7 dated May 30, 2016 (GPO-CA PCPS), the Subordinate Certificate Practices Statement, Version 1.7.8 dated May 30, 2016 (GPO-CA SCPS), as well as the Memorandum of Agreement dated November 23, 2009 between the Federal PKI Policy Authority and the GPO-CA (GPO-MOA), in providing its CA services in Washington D.C. for the period July 1, 2016 through June 30, 2017, GPO has:

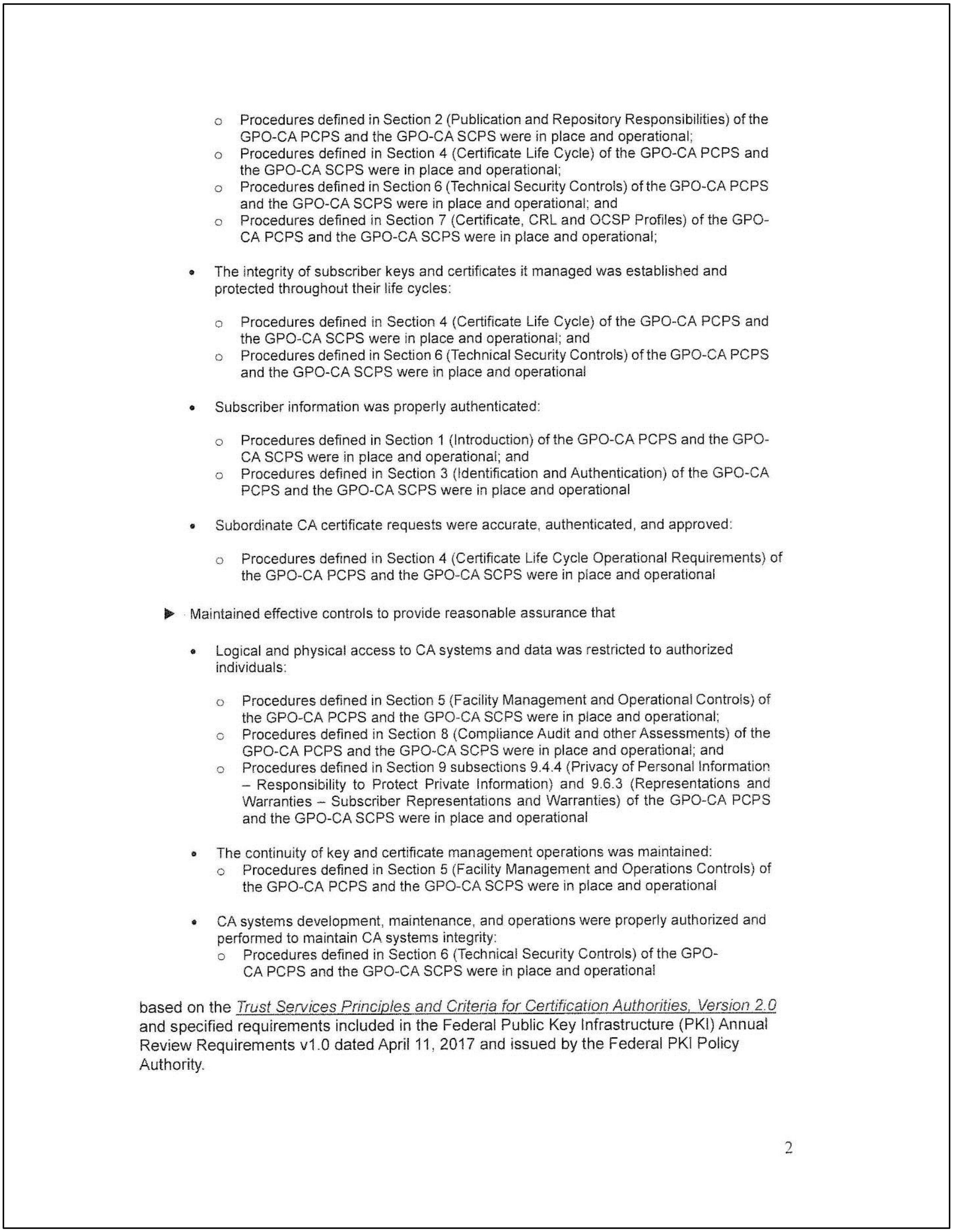
▶ Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Principal Certification Practice Statement, Subordinate Certification Practice Statement and Certificate Policy;

▶ Maintained effective controls to provide reasonable assurance that:

- GPO-CA's Principal Certification Practice Statement is consistent with its Certificate Policy;
- GPO-CA's Subordinate Certification Practice Statement is consistent with its Certificate Policy; and
- GPO-CA provided its services in accordance with its Certificate Policy, Principal Certification Practice Statement and Subordinate Certification Practice Statement

▶ Maintained effective controls to provide reasonable assurance that:

- The integrity of keys and certificates it managed was established and protected throughout their life cycles:



    - Procedures defined in Section 2 (Publication and Repository Responsibilities) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational;
    - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational;
    - Procedures defined in Section 6 (Technical Security Controls) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational; and
    - Procedures defined in Section 7 (Certificate, CRL and OCSP Profiles) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational;

  - The integrity of subscriber keys and certificates it managed was established and protected throughout their life cycles:
    - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational; and
    - Procedures defined in Section 6 (Technical Security Controls) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational

  - Subscriber information was properly authenticated:
    - Procedures defined in Section 1 (Introduction) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational; and
    - Procedures defined in Section 3 (Identification and Authentication) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational

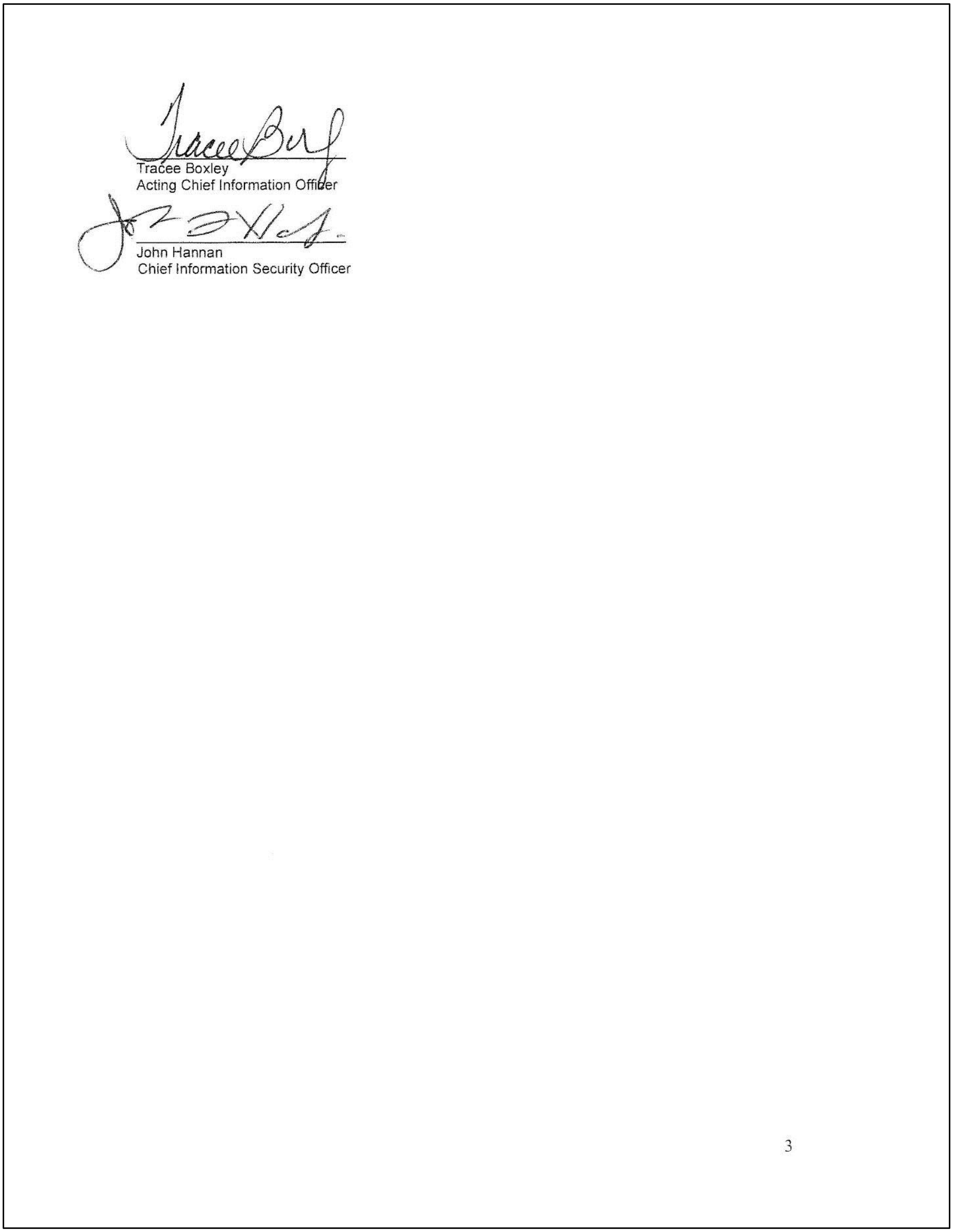
  - Subordinate CA certificate requests were accurate, authenticated, and approved:
    - Procedures defined in Section 4 (Certificate Life Cycle Operational Requirements) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational

- Maintained effective controls to provide reasonable assurance that
  - Logical and physical access to CA systems and data was restricted to authorized individuals:
    - Procedures defined in Section 5 (Facility Management and Operational Controls) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational;
    - Procedures defined in Section 8 (Compliance Audit and other Assessments) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational; and
    - 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) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational

  - The continuity of key and certificate management operations was maintained:
    - Procedures defined in Section 5 (Facility Management and Operations Controls) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational

  - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity:
    - Procedures defined in Section 6 (Technical Security Controls) of the GPO-CA PCPS and the GPO-CA SCPS were in place and operational

based on the *Trust Services Principles and Criteria for Certification Authorities, Version 2.0* and specified requirements included in the Federal Public Key Infrastructure (PKI) Annual Review Requirements v1.0 dated April 11, 2017 and issued by the Federal PKI Policy Authority.



Tracee Boxley
Acting Chief Information Officer

John Hannan
Chief Information Security Officer

Appendix A – Report Distribution

Director, GPO
Deputy Director, GPO
Acting General Counsel
Chief of Staff
Chief Administrative Officer

Major Contributor to the Report

Tony Temsupasiri – Lead Information Technology Specialist