U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT
REPORT NUMBER 17-28

Webtrust for Certification Authority
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 — Webtrust for Certification Authority
Report Number 17-28

Enclosed please find the subject final report. The Office of Inspector General contracted with Ernst & Young LLP (E&Y) to provide an opinion on the Government Publishing Office's (GPO) assertions regarding their certification authority process 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 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

Webtrust for Certification Authority
Ernst & Young LLP
September 13, 2017

U.S. Government Printing Office

Report of Independent Accountants
WebTrust for Certification Authorities
For the Period July 1, 2016 to June 30, 2017

EY
Building a better
working world

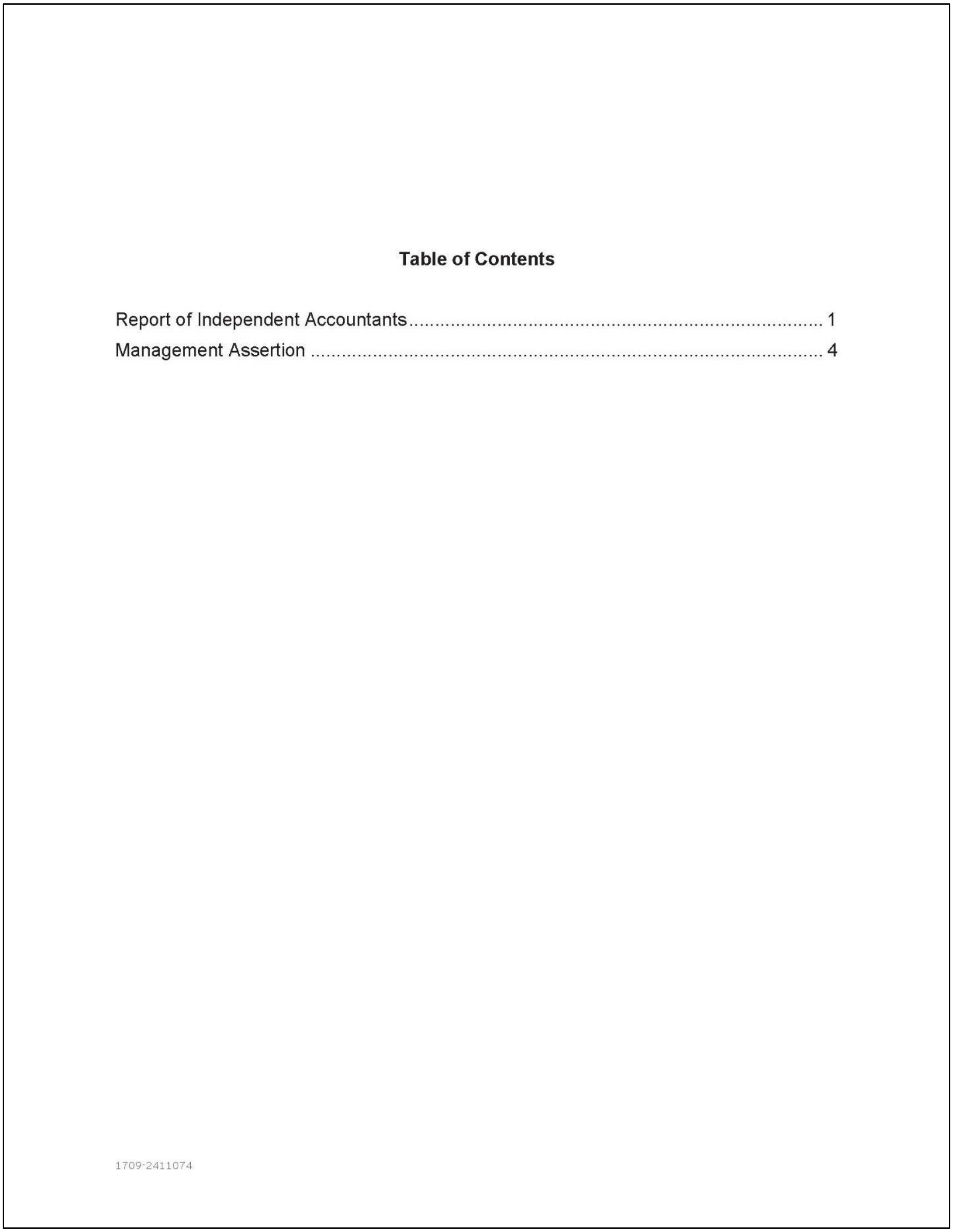


Table of Contents

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

Approach

We have examined management's assertion that the U.S. Government Printing Office Certification Authority (GPO-CA), in providing its Certification Authority (CA) services in Washington, D.C. for the Principal CA (GPO-PCA) and the Subordinate CA (GPO-SCA) during the period July 1, 2016 through June 30, 2017, GPO-CA has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Principal Certification Practice Statement Version 1.7.7 dated May 30, 2016, Subordinate Certification Practice Statement Version 1.7.8 dated May 30, 2016 and Certificate Policy Version 1.5 dated March 21, 2017.

- 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

  - 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;

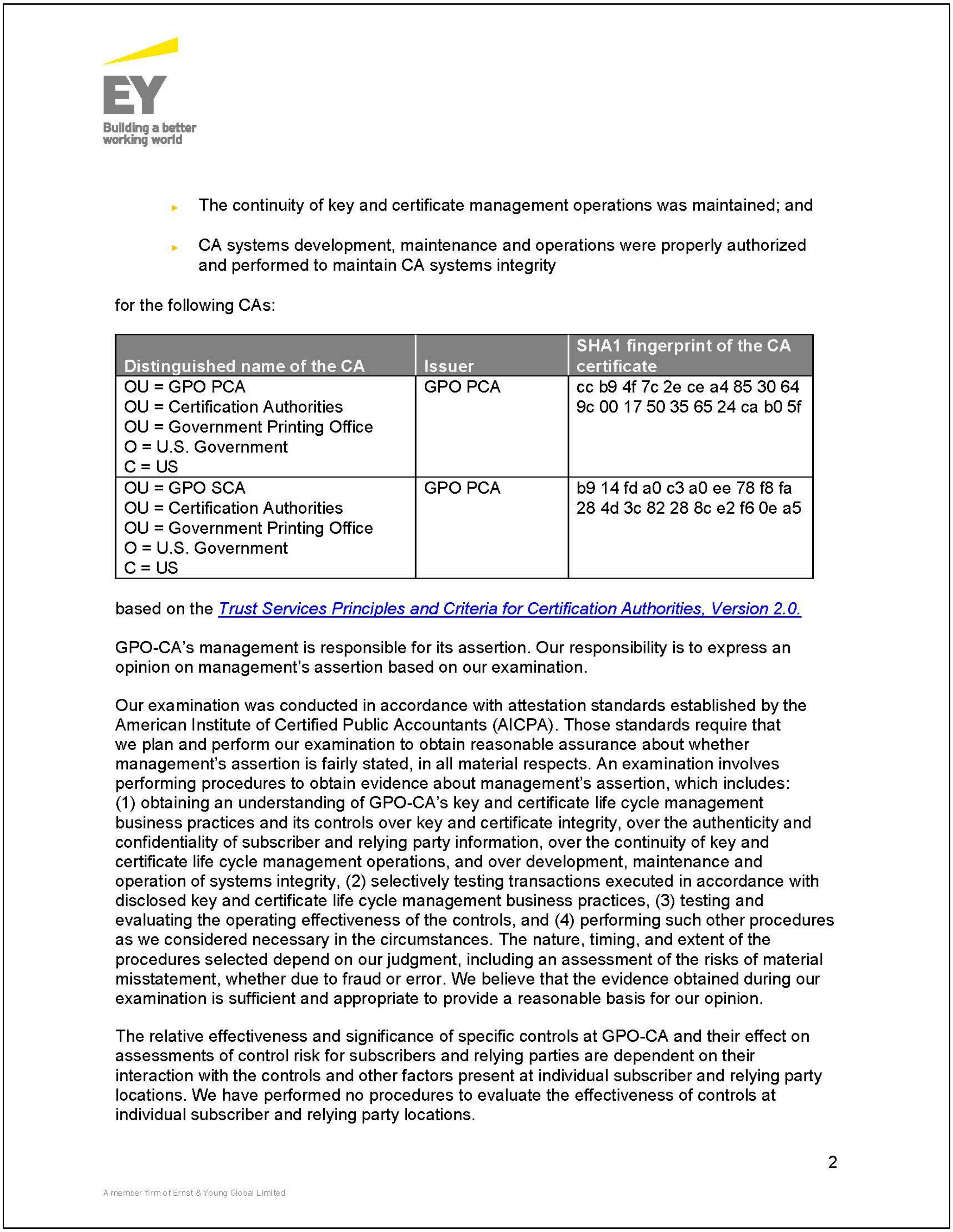
  - The integrity of subscriber keys and certificates it managed was established and protected throughout their life cycles;

  - Subscriber information was properly authenticated; and

  - Subordinate CA certificate requests were accurate, authenticated and approved.

- Maintained effective controls to provide reasonable assurance that:

  - Logical and physical access to CA systems and data was restricted to authorized individuals;



- The continuity of key and certificate management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the following CAs:

Distinguished name of the CA	Issuer	SHA1 fingerprint of the CA certificate

OU = GPO PCA
OU = Certification Authorities
OU = Government Printing Office
O = U.S. Government
C = US
	GPO PCA	cc b9 4f 7c 2e ce a4 85 30 64 9c 00 17 50 35 65 24 ca b0 5f

OU = GPO SCA
OU = Certification Authorities
OU = Government Printing Office
O = U.S. Government
C = US
	GPO PCA	b9 14 fd a0 c3 a0 ee 78 f8 fa 28 4d 3c 82 28 8c e2 f6 0e a5

based on the *Trust Services Principles and Criteria for Certification Authorities, Version 2.0.*

GPO-CA'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 (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (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 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. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

Our examination was not conducted for the purpose of evaluating the GPO-CA's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of control, including the possibility of human error and the circumvention of controls. Because of the nature and inherent limitations of controls, the GPO-CA may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are achieved. 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. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

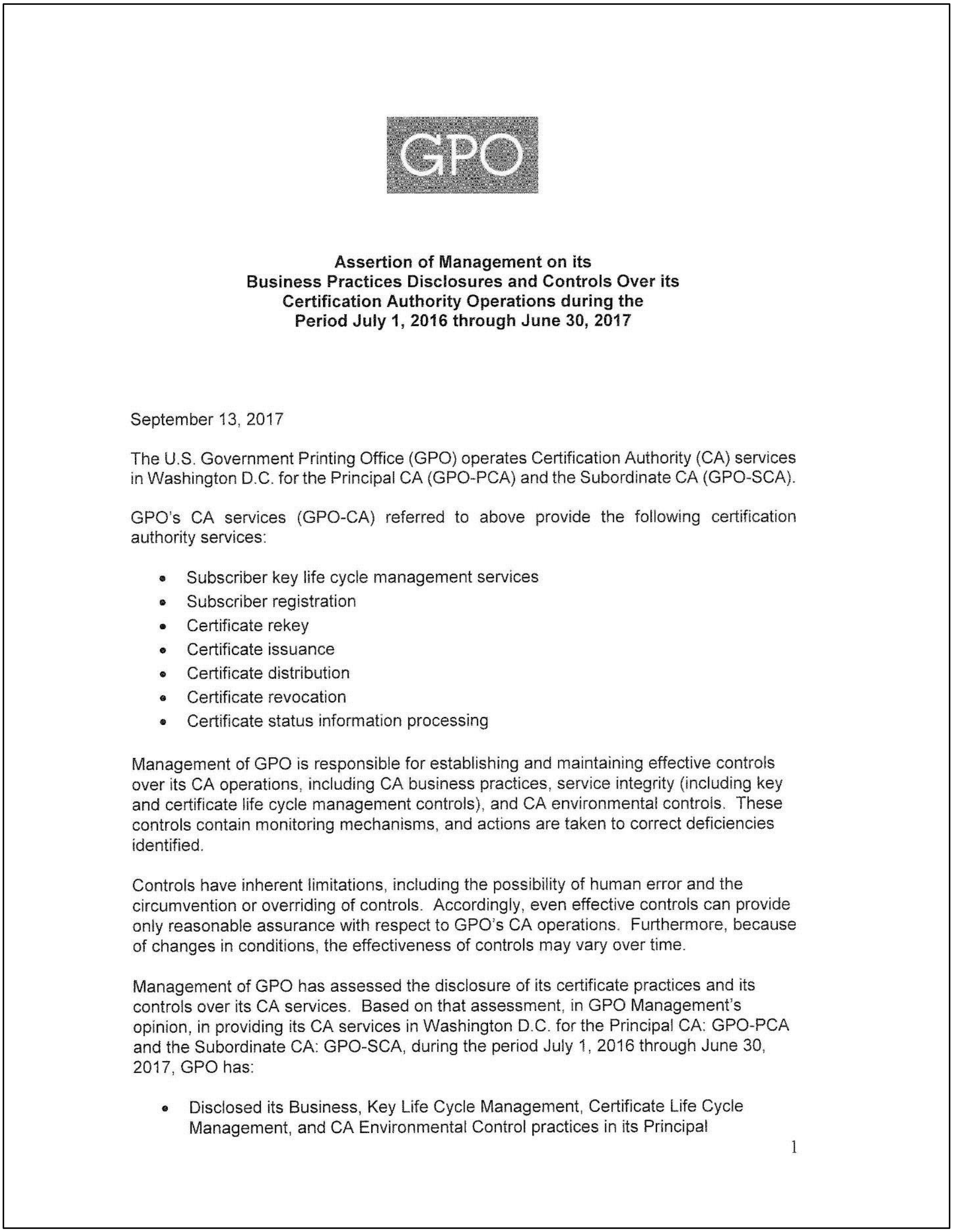
Opinion

In our opinion, for the period July 1, 2016 through June 30, 2017, GPO-CA's management's assertion referred to above is fairly stated, in all material respects, based on the *Trust Services Principles and Criteria for Certification Authorities Criteria, Version 2.0.*

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* criteria, or the suitability of any of GPO-CA's services for any customer's intended purpose.

Ernst + Young LLP

September 13, 2017



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:

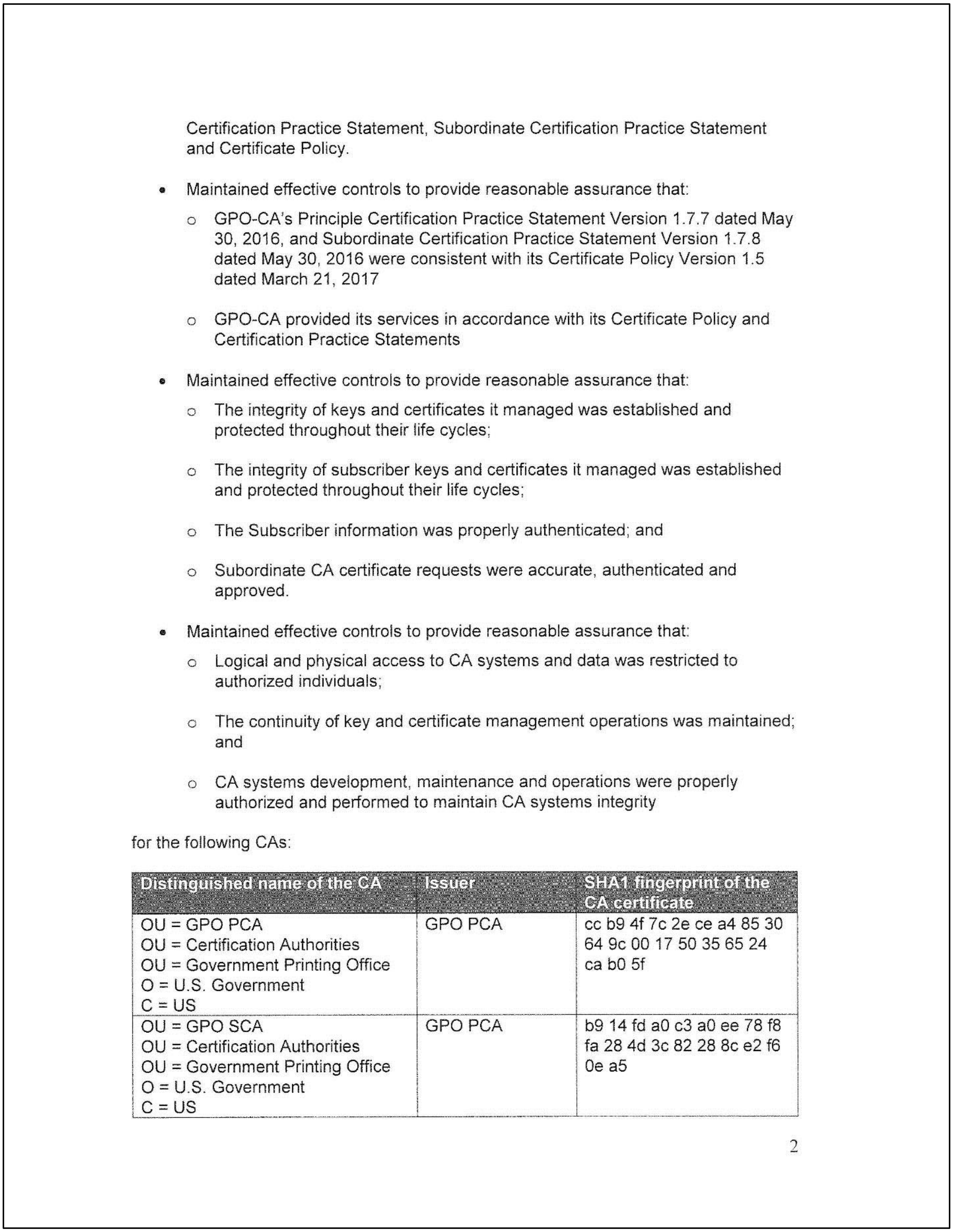
- Subscriber key life cycle management services
- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

Management of GPO is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices, 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 controls can provide only reasonable assurance with respect to GPO's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of GPO has assessed the disclosure of its certificate practices and its controls over its CA services. Based on that assessment, in GPO Management's opinion, in providing its CA services in Washington D.C. for the Principal CA: GPO-PCA and the Subordinate CA: GPO-SCA, during 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.

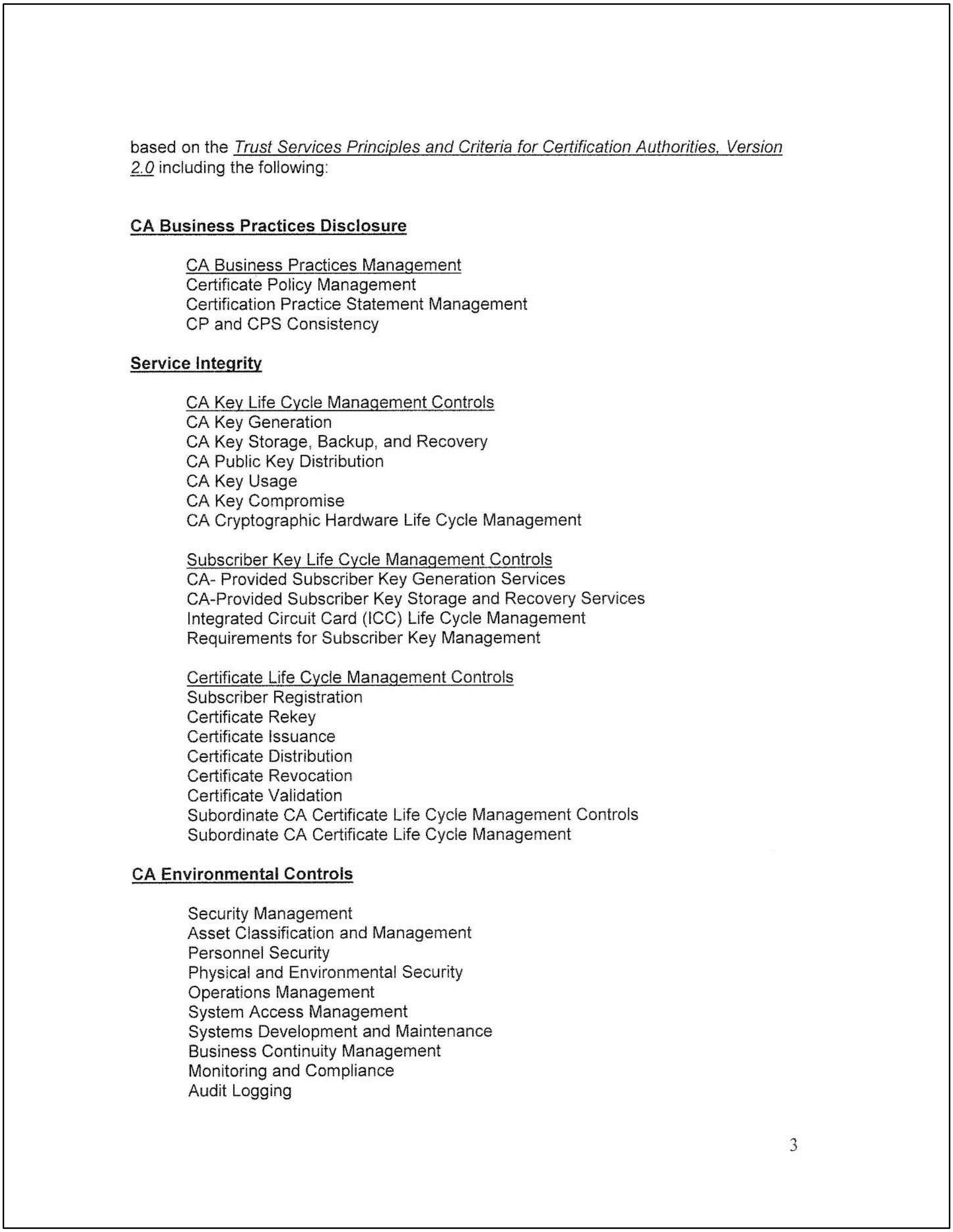
- Maintained effective controls to provide reasonable assurance that:
  - GPO-CA's Principle Certification Practice Statement Version 1.7.7 dated May 30, 2016, and Subordinate Certification Practice Statement Version 1.7.8 dated May 30, 2016 were consistent with its Certificate Policy Version 1.5 dated March 21, 2017
  - GPO-CA provided 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 managed was established and protected throughout their life cycles;
  - The integrity of subscriber keys and certificates it managed was established and protected throughout their life cycles;
  - The Subscriber information was properly authenticated; and
  - Subordinate CA certificate requests were accurate, authenticated and approved.
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the following CAs:

Distinguished name of the CA	Issuer	SHA1 fingerprint of the CA certificate

OU = GPO PCA
OU = Certification Authorities
OU = Government Printing Office
O = U.S. Government
C = US
	GPO PCA	cc b9 4f 7c 2e ce a4 85 30 64 9c 00 17 50 35 65 24 ca b0 5f

OU = GPO SCA
OU = Certification Authorities
OU = Government Printing Office
O = U.S. Government
C = US
	GPO PCA	b9 14 fd a0 c3 a0 ee 78 f8 fa 28 4d 3c 82 28 8c e2 f6 0e a5



based on the *Trust Services Principles and Criteria for Certification Authorities, Version 2.0* including the following:

CA Business Practices Disclosure

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

Service Integrity

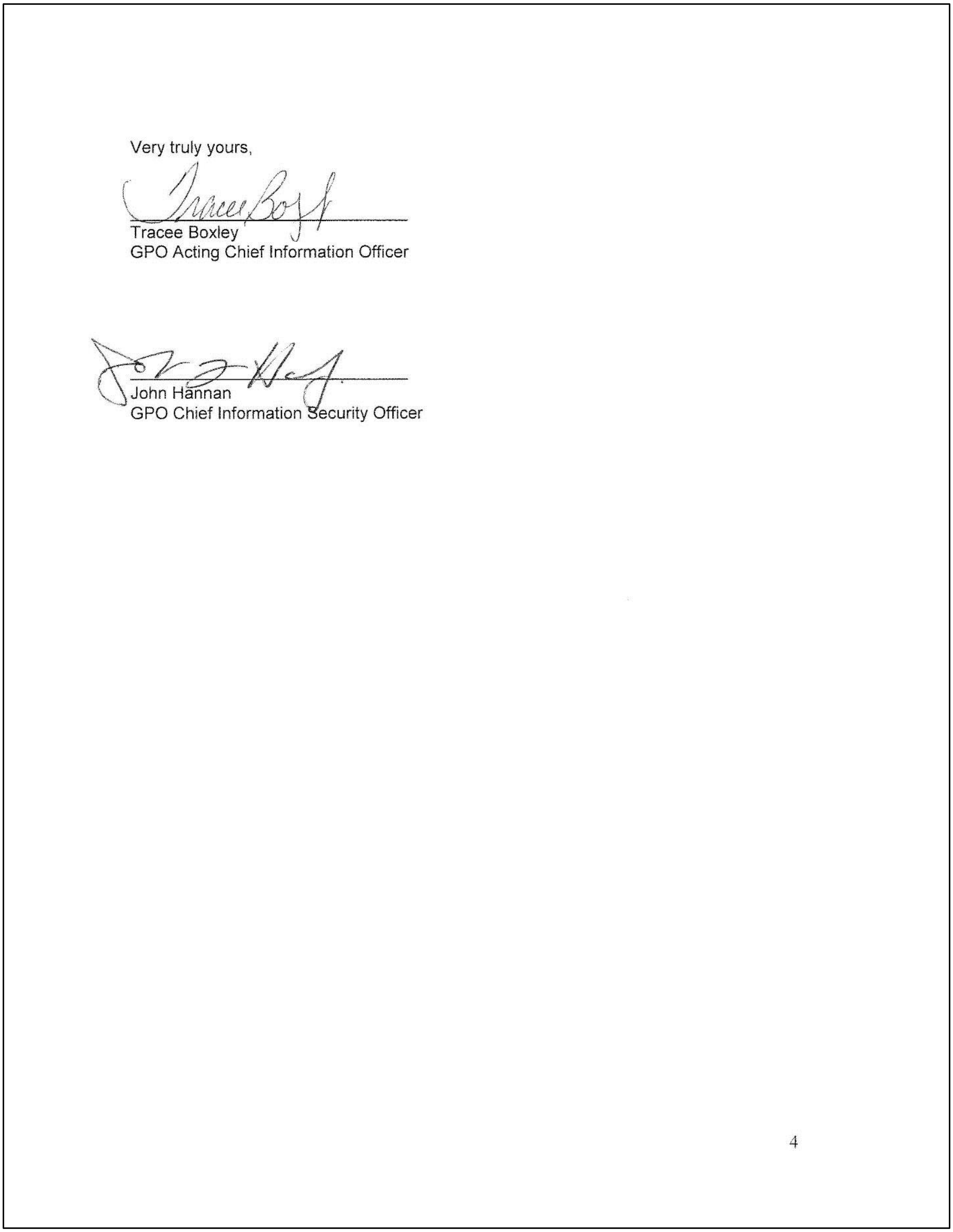
CA Key Life Cycle Management Controls
CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Compromise
CA Cryptographic Hardware Life Cycle Management

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

Certificate Life Cycle Management Controls
Subscriber Registration
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



Very truly yours,

Tracee Boxley
GPO Acting Chief Information Officer

John Hannan
GPO 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