U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT

REPORT NUMBER 18-20

Webtrust for Certification Authority

September 17, 2018

GPO **U.S. GOVERNMENT PUBLISHING OFFICE**

OFFICE OF INSPECTOR GENERAL

Date

September 17, 2018

To

Acting Deputy Director

From

Inspector General

Subject:

Assessment Report — Webtrust for Certification Authority
Report Number 18-20

Enclosed please find the subject final report. The Office of Inspector General (OIG) contracted with Ernst & Young, LLP (E&Y) to provide an opinion on the Government Publishing Office's (GPO) assertions regarding its certification authority process for July 1, 2017 through June 30, 2018. E&Y conducted its 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.

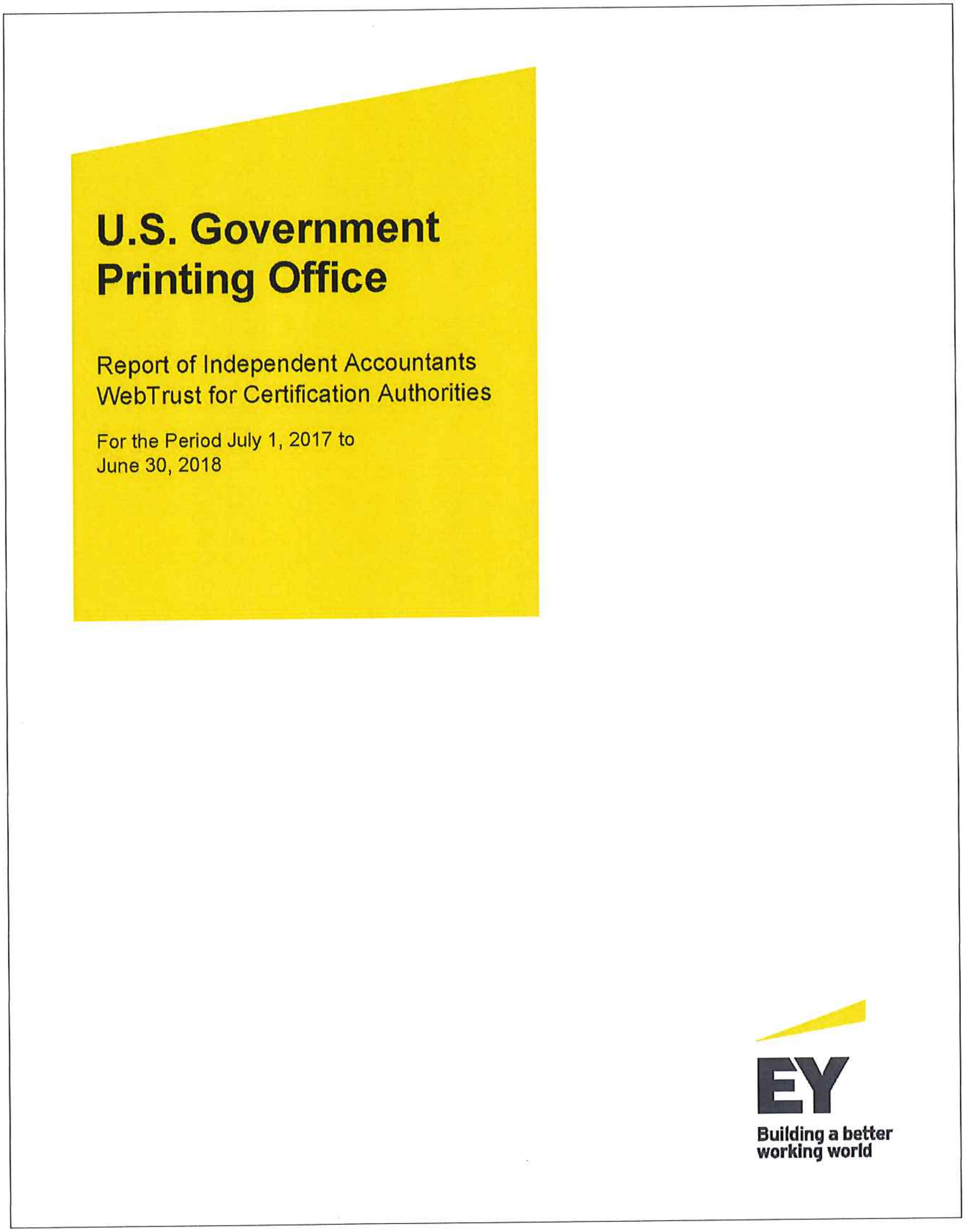
We appreciate the courtesies extended to E&Y and to our audit staff. If you have any questions or comments about this report, please do not hesitate to contact Mr. Freddie W. Hall, Assistant Inspector General for Audits and Inspections at (202) 512-1597 or me at (202) 512-1512.

Melinda M. Miguel

MELINDA M. MIGUEL
Inspector General

Attachment
cc:
Acting Chief of Staff, GPO
Acting General Counsel, GPO
Chief Information Officer, GPO

Contents



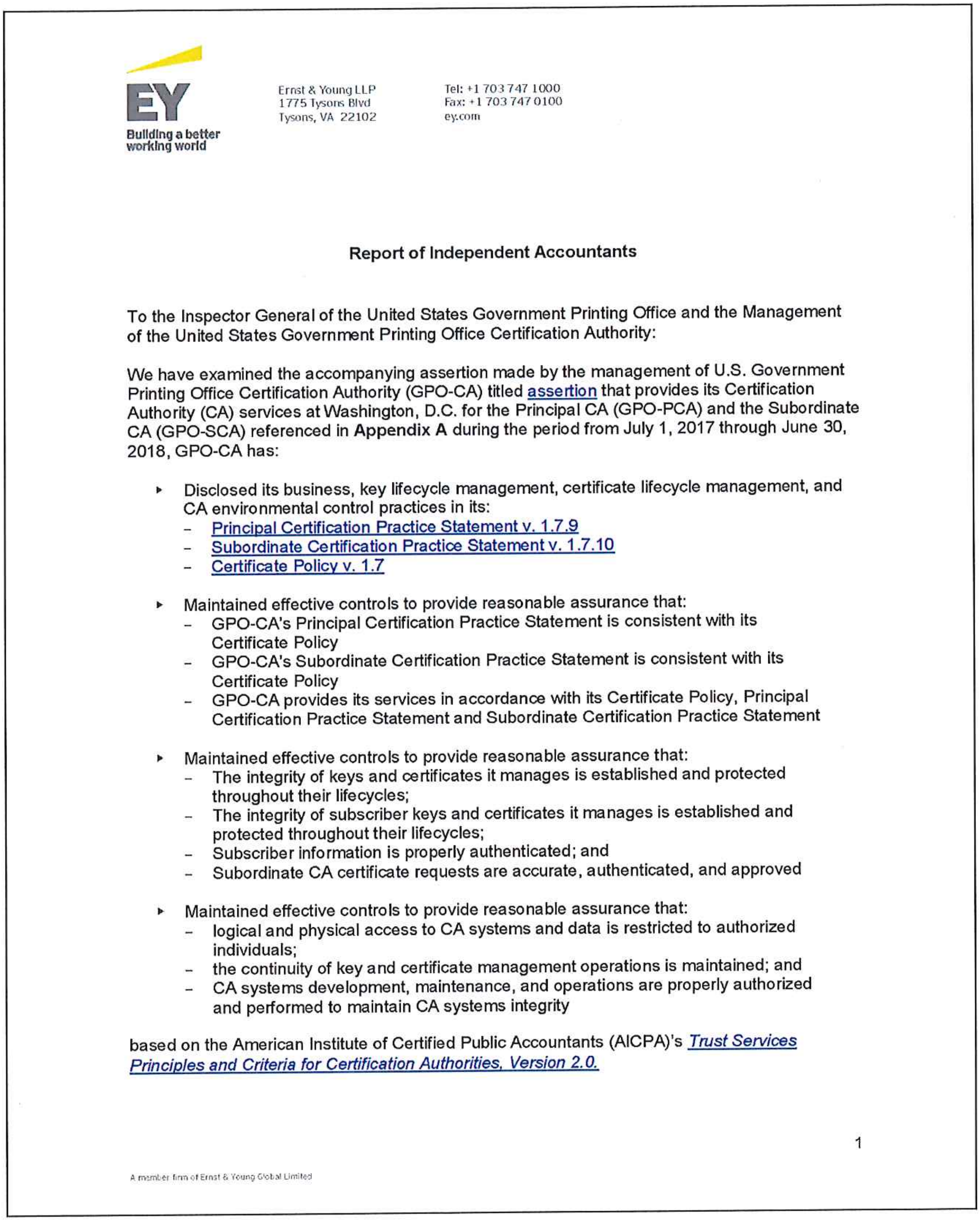
U.S. Government Printing Office

Report of Independent Accountants
WebTrust for Certification Authorities

For the Period July 1, 2017 to
June 30, 2018

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

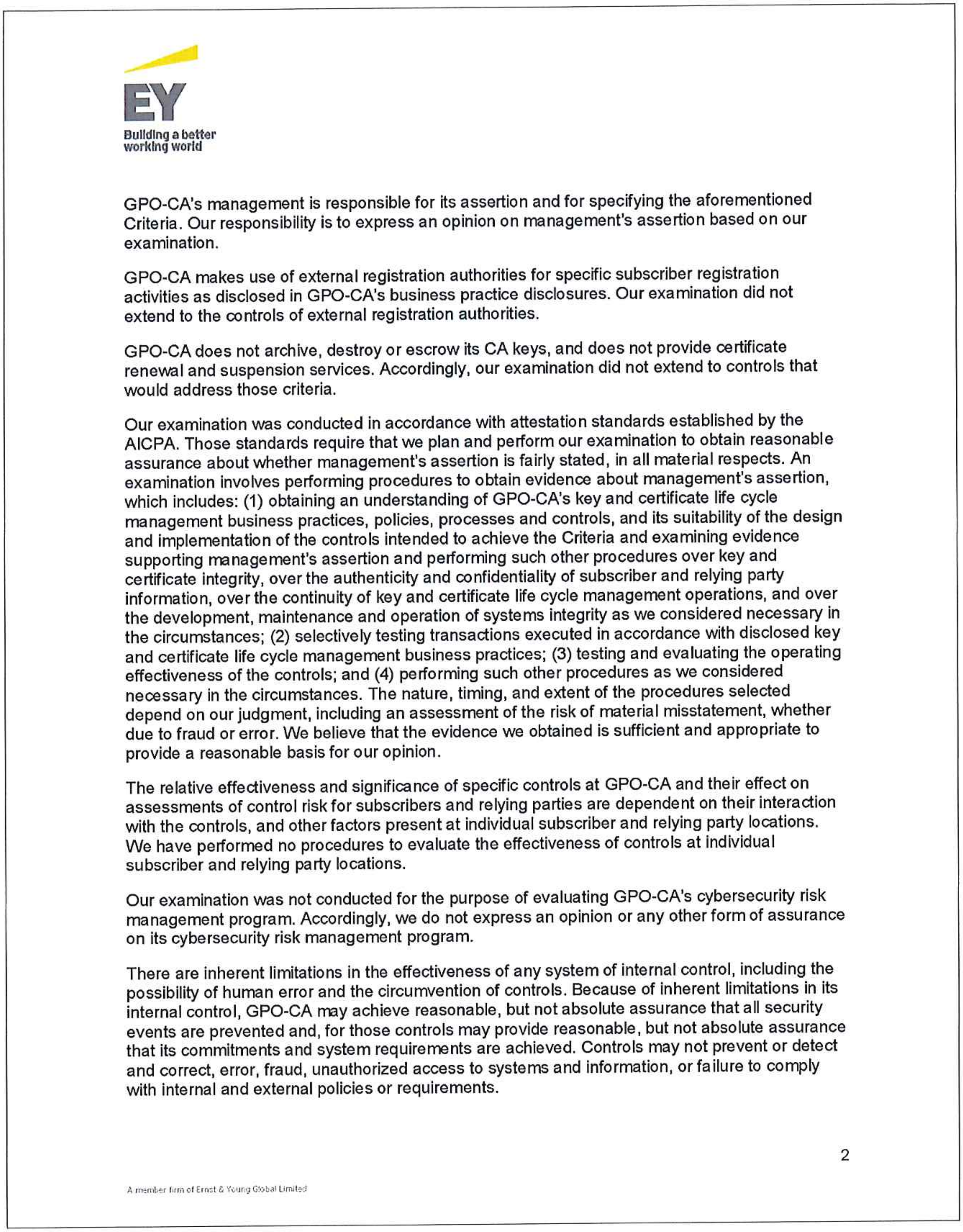
Report of Independent Accountants

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

We have examined the accompanying assertion made by the management of U.S. Government Printing Office Certification Authority (GPO-CA) titled assertion that provides its Certification Authority (CA) services at Washington, D.C. for the Principal CA (GPO-PCA) and the Subordinate CA (GPO-SCA) referenced in **Appendix A** during the period from July 1, 2017 through June 30, 2018, GPO-CA has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Principal Certification Practice Statement v. 1.7.9
  - Subordinate Certification Practice Statement v. 1.7.10
  - Certificate Policy v. 1.7
- 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 provides 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 manages is established and protected throughout their lifecycles;
  - The integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - 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

based on the American Institute of Certified Public Accountants (AICPA)'s *Trust Services Principles and Criteria for Certification Authorities, Version 2.0.*



Building a better working world

GPO-CA's management is responsible for its assertion and for specifying the aforementioned Criteria. Our responsibility is to express an opinion on management's assertion based on our examination.

GPO-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in GPO-CA's business practice disclosures. Our examination did not extend to the controls of external registration authorities.

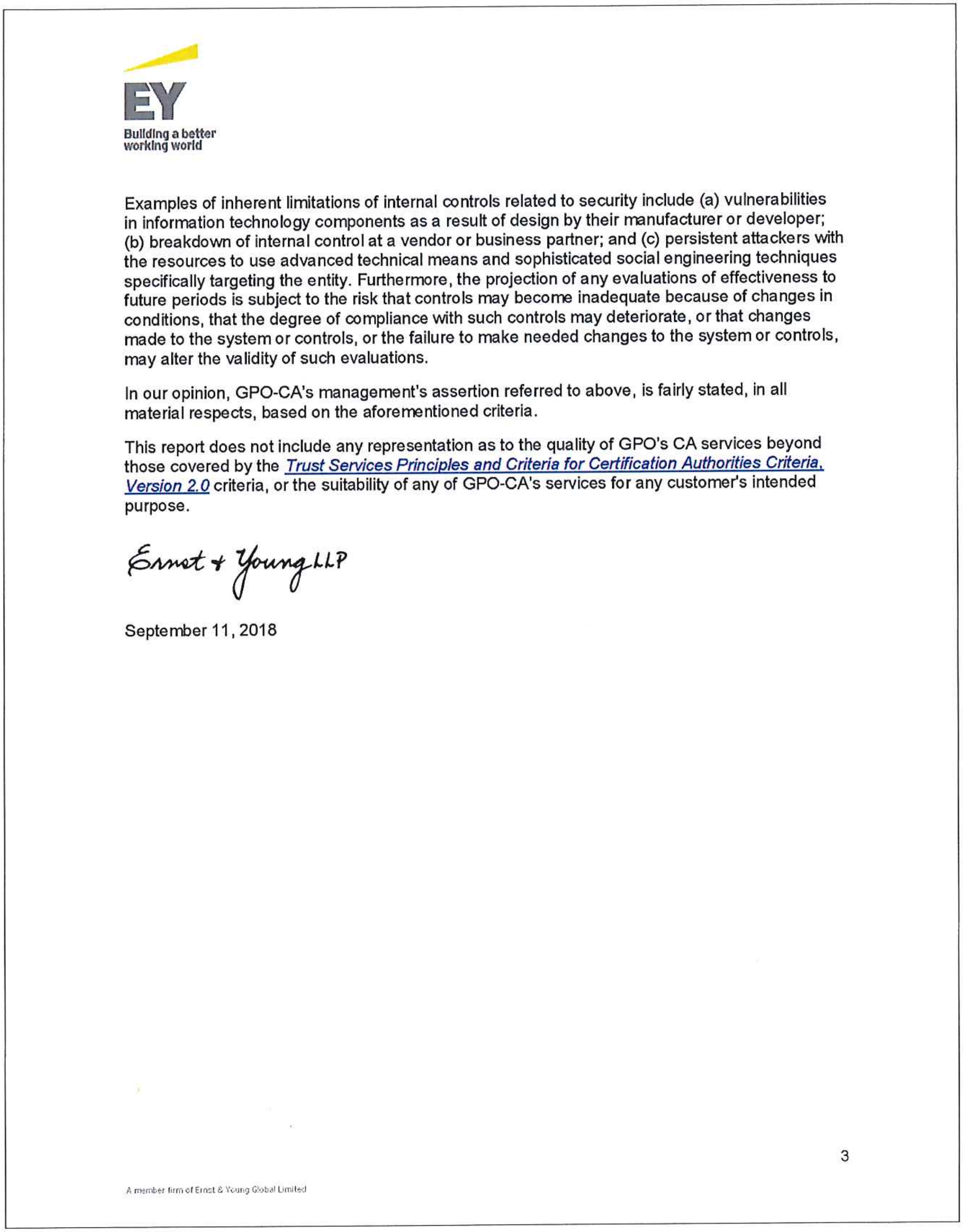
GPO-CA does not archive, destroy or escrow its CA keys, and does not provide certificate renewal and suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination was conducted in accordance with attestation standards established by the 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, policies, processes and controls, and its suitability of the design and implementation of the controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures 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 as we considered necessary in the circumstances; (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 risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained 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 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.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, 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.



Building a better working world

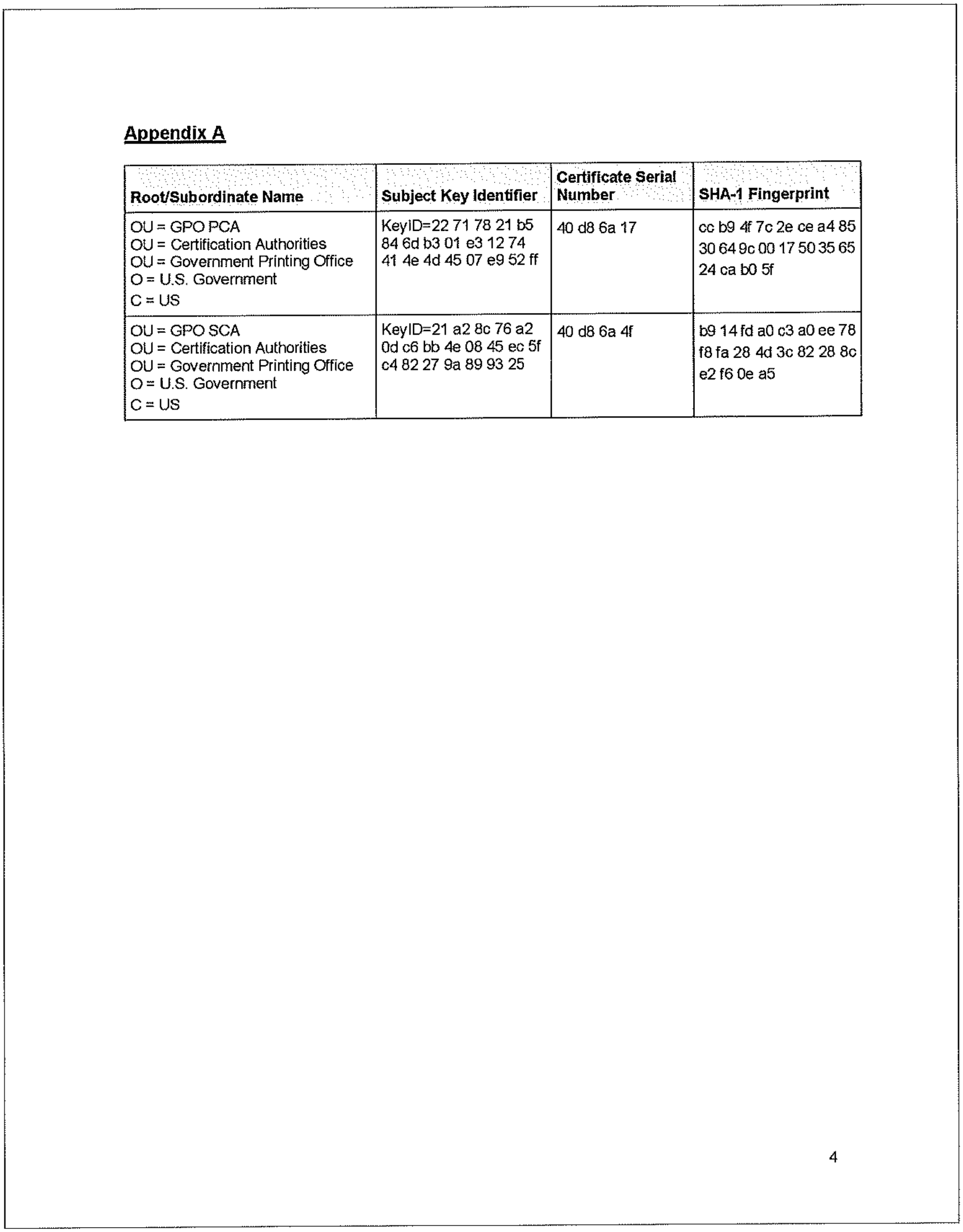
Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the 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.

In our opinion, GPO-CA's management's assertion referred to above, is fairly stated, in all material respects, based on the aforementioned criteria.

This report does not include any representation as to the quality of GPO's CA services beyond those covered by the *Trust Services Principles and Criteria for Certification Authorities Criteria, Version 2.0* criteria, or the suitability of any of GPO-CA's services for any customer's intended purpose.

Ernst & Young LLP

September 11, 2018

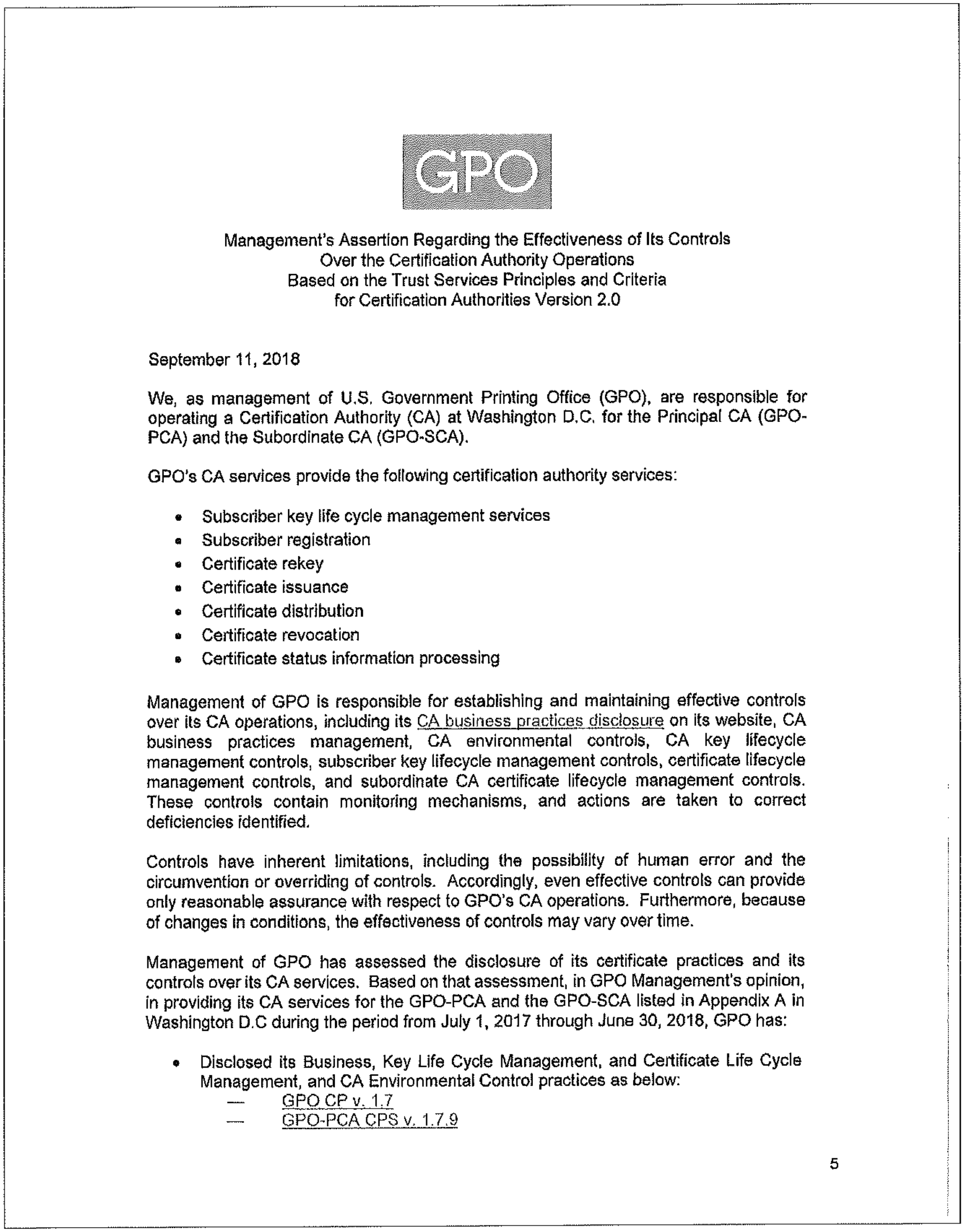


Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-1 Fingerprint

OU = GPO PCA
OU = Certification Authorities
OU = Government Printing Office
O = U.S. Government
C = US
	KeyID=22 71 78 21 b5 84 6d b3 01 e3 12 74 41 4e 4d 45 07 e9 52 ff	40 d8 6a 17	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
	KeyID=21 a2 8c 76 a2 0d c6 bb 4e 08 45 ec 5f c4 82 27 9a 89 93 25	40 d8 6a 4f	b9 14 fd a0 c3 a0 ee 78 f8 fa 28 4d 3c 82 28 8c e2 f6 0e a5



GPO

Management's Assertion Regarding the Effectiveness of Its Controls
Over the Certification Authority Operations
Based on the Trust Services Principles and Criteria
for Certification Authorities Version 2.0

September 11, 2018

We, as management of U.S. Government Printing Office (GPO), are responsible for operating a Certification Authority (CA) at Washington D.C. for the Principal CA (GPO-PCA) and the Subordinate CA (GPO-SCA).

GPO's CA services provide the following certification authority services:

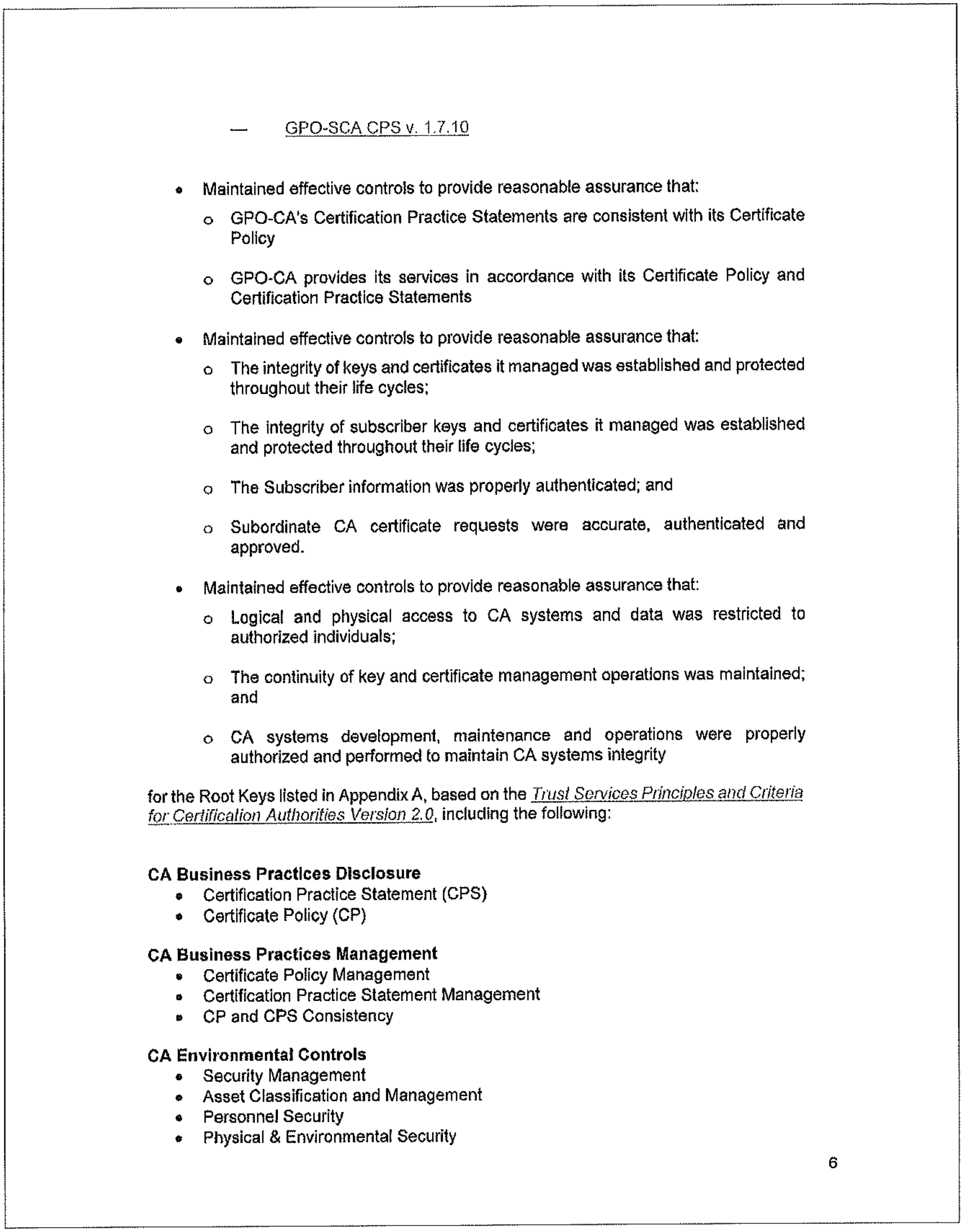
- Subscriber key life cycle management services
- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

Management of GPO is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management 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 for the GPO-PCA and the GPO-SCA listed in Appendix A in Washington D.C during the period from July 1, 2017 through June 30, 2018, GPO has:

- Disclosed its Business, Key Life Cycle Management, and Certificate Life Cycle Management, and CA Environmental Control practices as below:
  - — GPO CP v. 1.7
  - — GPO-PCA CPS v. 1.7.9



— GPO-SCA CPS v. 1.7.10

- 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 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 Root Keys listed in Appendix A, based on the *Trust Services Principles and Criteria for Certification Authorities Version 2.0*, including the following:

CA Business Practices Disclosure

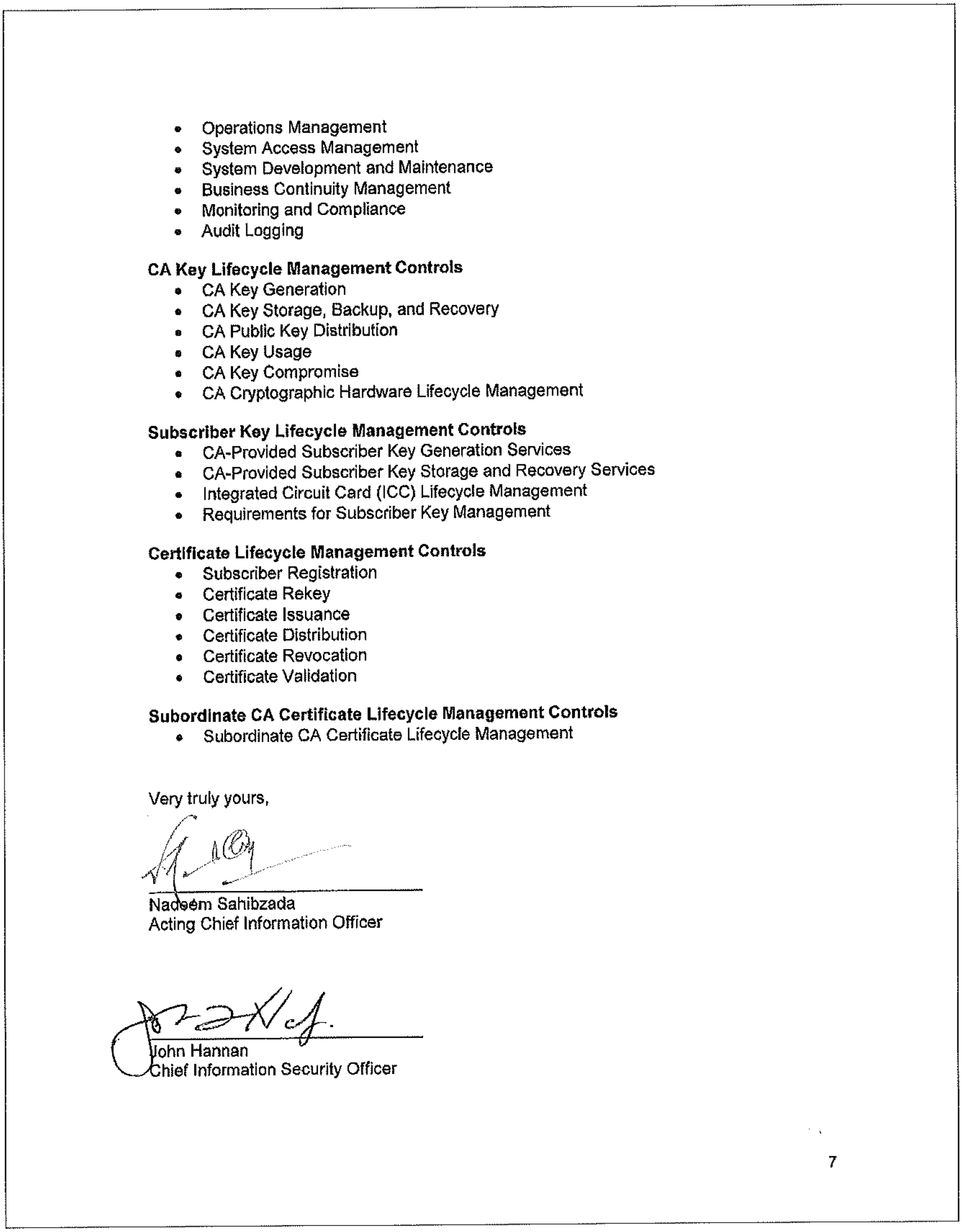
- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security



- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

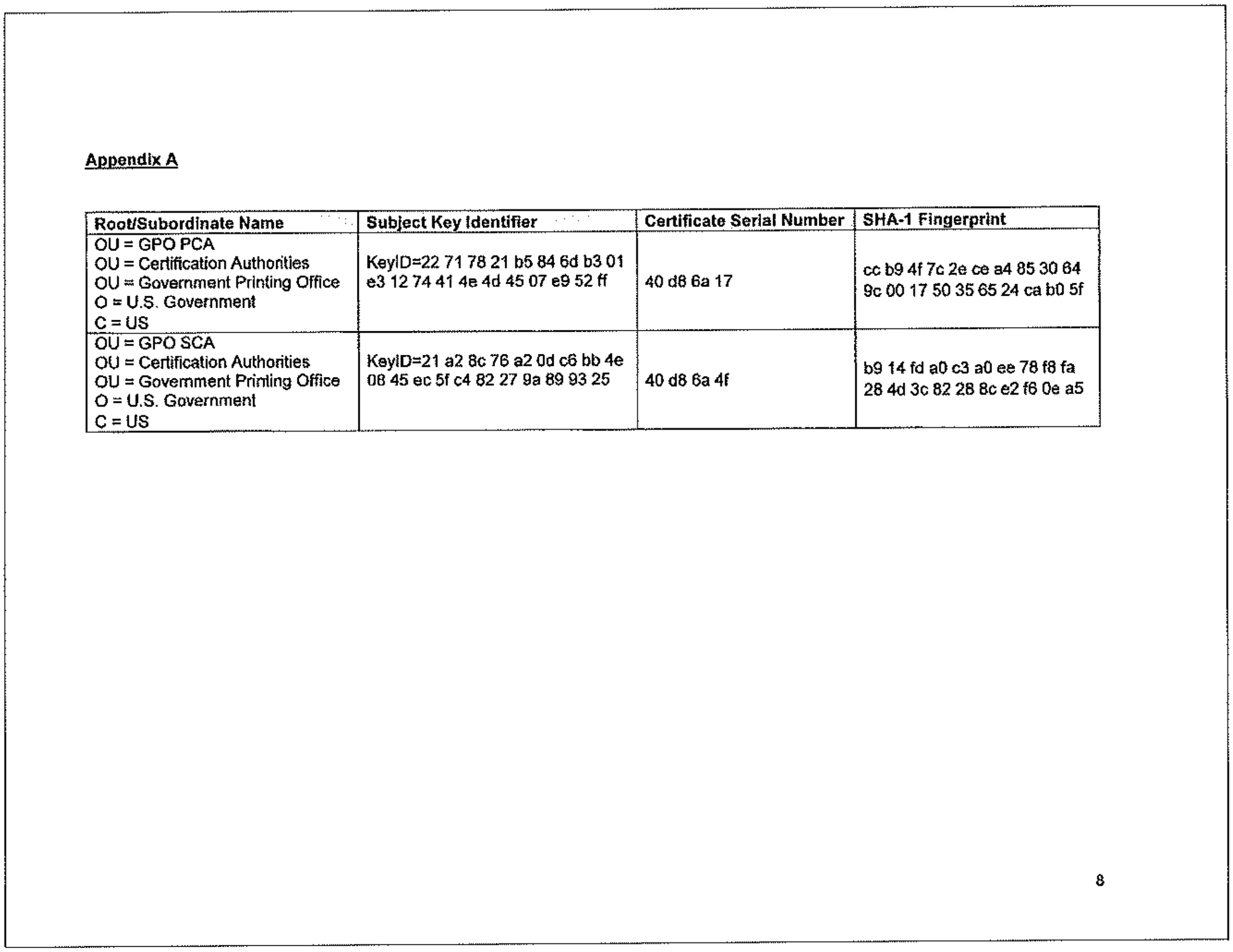
- Subordinate CA Certificate Lifecycle Management

Very truly yours,

Nadeem Sahibzada
Acting Chief Information Officer

John Hannan
Chief Information Security Officer

7



Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-1 Fingerprint

OU = GPO PCA
OU = Certification Authorities
OU = Government Printing Office
O = U.S. Government
C = US
	KeyID=22 71 78 21 b5 84 6d b3 01 e3 12 74 41 4e 4d 45 07 e9 52 ff	40 d8 6a 17	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
	KeyID=21 a2 8c 76 a2 0d c6 bb 4e 08 45 ec 5f c4 82 27 9a 89 93 25	40 d8 6a 4f	b9 14 fd a0 c3 a0 ee 78 f8 fa 28 4d 3c 82 28 8c e2 f6 0e a5

Appendix A – Report Distribution

Acting Chief of Staff, GPO
Acting General Counsel, GPO
Chief Information Officer, GPO

Major Contributor to the Report

Tony Temsupasiri – Lead Information Technology Specialist