Controlled Substance Ordering System
(CSOS)
Certification Practices Statement (CPS)

Prepared for

Drug Enforcement Administration
Office of Diversion Control
Technology Section (ODT)
Arlington, VA 22202

Version 4.0

January 6, 2010

Table of Contents

Page

Table of Contents

Page

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Section 1 – Introduction

1.1 Overview

A Certification Practices Statement (CPS) is a statement of the practices that a Certification Authority employs when issuing certificates. It is, in many ways, the implementation of the policies set forth in the Certificate Policy (CP). A certification authority is a collection of certificate authorities within a given domain. This CPS establishes the procedures that satisfy the DEA Diversion Control Technology Section Controlled Substance Ordering System (CSOS) System Certificate Policy (CP) for the management of certificates within the CSOS Certification Authority domain, stating the operating procedures for the Certificate Authorities operating within the Certification Authority and clarifying legal rights and obligations therein. For simplicity, the DEA Diversion Control Technology Section Controlled Substance Ordering System shall hereafter be referred to as simply CSOS.

This *CSOS Certification Practices Statement* (henceforth referred to as CPS) has been developed in accordance with recommendations contained in Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 and with recommendations set forth by the Federal Public Key Infrastructure Architecture (FPKIA).

The CSOS Certification Authority is an entity consisting of two Certificate Authorities (CAs) established to create, sign, and issue public key certificates to authorized CSOS Subscribers through subordination to the CSOS Root CA. For simplicity, the two subordinate CAs shall hereafter be referred to as SCAs.

This CPS describes the practices of the CSOS Certification Authority in issuing and otherwise managing CSOS certificates issued to DEA Registrants, CSOS Coordinators, and holders of Powers of Attorney (POAs). It provides the details for the certification process. This CPS also describes the process for suspending, revoking, and renewing certificates. The scope of this document is applicable to the CSOS Public Key Infrastructure (PKI). Due to the sensitive nature of the security controls described within this document, this document is not made publicly available in its entirety. Requests for the complete CPS must be made by authorized parties to the Policy Management Authority (PMA) at the address cited in Section 1.5.2.

This CPS describes:

- The mechanisms used to authenticate the identity of all individuals who need to interact with the CSOS PKI.
- The methods used to ensure the integrity of all information that is communicated.
- The format(s) of the input certification requests.
- The algorithms(s) used for signing the hashed content summary of the certificate request that are accepted by the CSOS Certification Authority and the algorithms used by the CSOS Certification Authority to sign the certificates that it generates.

- The validity period of the certificates issued by the CSOS Certification Authority.
- The procedures for renewing certificates.
- The technical procedures for revoking certificates generated by the CSOS Certification Authority.
- The backup procedures that ensure that all data is recoverable in case of failure.
- The methods of protecting sensitive information from unauthorized access.
- The methods of distributing and accessing the certificates generated by the CSOS Certification Authority.

1.2 Document Name and Identification

This document serves as the CSOS CPS. The practices stated herein conform to and support the CSOS System Certificate Policy, version 3.1, dated October 2009, that is registered with the National Institute of Standards and Technology (NIST) and identified by the assigned object identifier (OID) dea-csos-cp ::= { 2.16.840.1.101.3.2.1.9.1}. All certificates issued to CSOS Subscribers by the CSOS Certification Authority carry this OID. Administrative and component certificates used for device or service signing or encryption, issued by the CSOS Certification Authority, do not carry this OID.

Only the CSOS Certification Authority that is designated and managed by the DEA or its contractor, ASRC Primus, is authorized to issue CSOS Subscriber certificates. The CSOS Certification Authority will not fully cross-certify with other CAs. It is anticipated that cross-certification of the CSOS Root CA with the Federal Bridge CA in a one-way trust configuration enables Relying Parties to accept CSOS Subscriber certificates for purposes other than controlled substance orders.

1.3 PKI Participants

This CPS identifies the specific privileges and the specific restrictions assigned to CSOS Certification Authority participants and the mechanisms by which these attributes are granted and enforced. This includes individuals involved in both implementing the CP, CPS, and managing the CSOS PKI. This CPS contains information sensitive to the security of the CSOS PKI and therefore is not released in its entirety to the public without the express permission of the DEA Diversion Control Technology Section Chief or Policy Management Authority Chair.

1.3.1 Certification Authority Entities

1.3.1.1 Policy Management Authority (PMA)

The CSOS System Policy Management Authority (PMA) is the governing body responsible for the CSOS System initiatives. The mission of the PMA is to establish, interpret, and enforce policy for the CSOS Certification Authority in accordance with all applicable US laws and regulations. The PMA approves the CP and CPS for the CSOS System and approves all changes to the document as discussed in Section 9.12 of this CPS. Operational tasks for which the PMA has oversight responsibility are delegated to the Operations Management Authority (OMA).

The PMA is a formal committee. PMA membership consists of selected individuals working within DEA Office of Diversion Control, CSOS Section (ODC), Liaison and Policy Section (ODL), Registration and Program Support Section (ODR), the DEA Diversion Control PKI Operations Management Authority (OMA), the DEA CIO or his or her representative and the Contracting Officer's Technical Representative (COTR) supervising contractor activities relating to the CSOS System.

The official list of PMA members is maintained at the CSOS System web site at: http://www.deaecom.gov.

1.3.1.1.1 Policy Management Authority (PMA) Obligations

PMA obligations are as follows:

- The PMA is responsible for review and approval of this CPS, and provides approval authority for subsequent changes to this CPS, to ensure its consistency with the CP as specified in Section 2.1 of the *PMA Operations Guide*.

- The PMA is responsible for the approval of all Subscriber agreements as specified in Section 2.2 of the *PMA Operations Guide*.

- The PMA is ultimately responsible for resolution of any name claim disputes as specified in Section 2.5 of the *PMA Operations Guide*.

- The PMA approves any fees levied by the OMA as specified in Section 3.14 of the *PMA Operations Guide*.

- The PMA establishes the qualifications for the selection of entities seeking to perform a compliance audit as specified in Section 4.1.1.1 of the *PMA Operations Guide*.

- The PMA reviews compliance audits for the CSOS Certification Authority and any cross-certified or subordinate CAs and make appropriate determinations as specified in Section 4.1.2 of the *PMA Operations Guide*.

- The PMA ensures that the database information is readily available for verification as specified in Section 3.13 of the *PMA Operations Guide*.

The PMA evaluates (or direct the evaluation of) applicant CAs seeking cross-certification or subordination to the CSOS Root CA as specified in Section 2.3 of the *PMA Operations Guide*.

1.3.1.2 Operations Management Authority (OMA)

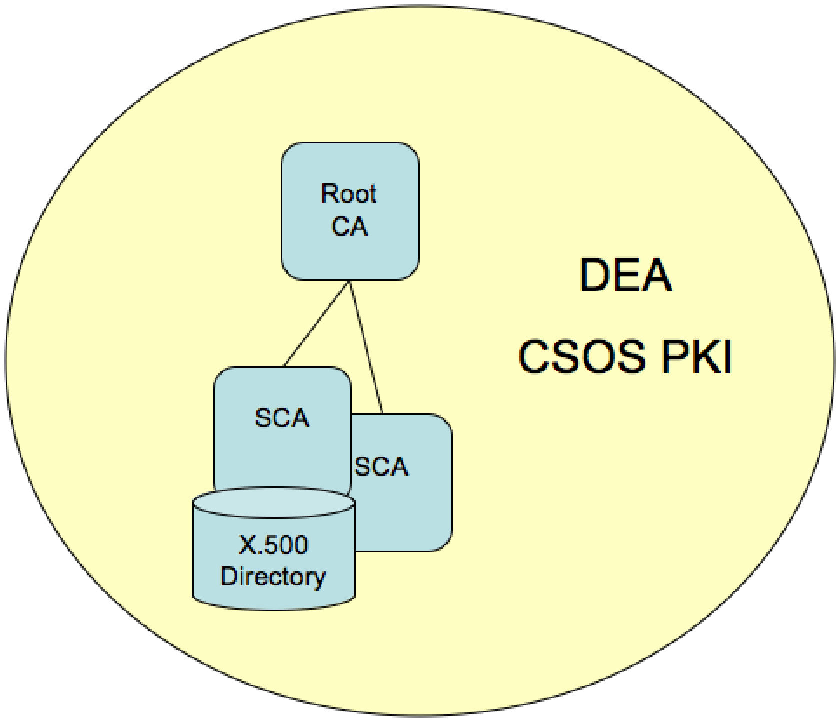
The OMA is responsible for the daily operation and maintenance of the CSOS PKI systems that issue Controlled Substance Ordering System (CSOS) digital certificates. The OMA consists of the DEA Diversion Control Technology Section Chief, the Program Manager and his/her staff, and the CSOS. Policy Lead and Systems Engineering Lead. The CSOS Section Chief provides planning guidance and direction to this team and, in turn, presents operational status and issues to the PMA for consideration.

1.3.1.2.1 Operations Management Authority (OMA) Obligations

The OMA is responsible for daily operations of the CSOS System and for the development and maintenance of operations and policy documents. Operational roles, responsibilities and procedures are maintained in the *Operations Management Guide*, available to staff in the DEA Office of Diversion Technology Section facilities.

1.3.1.3 CSOS Certification Authority Entities

The CSOS Certification Authority is depicted below at a very high level:



1.3.1.3.1 CSOS System Root CA

The CSOS Certification Authority is comprised of one Root CA .The CSOS Root CA is operated and maintained under the authority of the DEA. The CSOS Root CA serves as the Root CA to the CSOS Certification Authority, issuing and signing public key certificates for the CSOS Certification Authority.

The CSOS Root CA executes the following obligations in accordance with the CSOS CP:

- Provides a copy of its CPS to the PMA, as well as any subsequent changes, for approval and conformance assessment;
- Protects the private signing key of the CSOS Root CA in accordance with the CP and this CPS;
- Issues and manages certificates to the CSOS subordinate CAs (SCAs);
- Signs certificates only after verifying the identity of the certificate subject in accordance with the CP and this CPS, and that the subject holds the private key corresponding to the public key in the certificate;
- Uses the private signing key only when issuing certificates or signing Authority Revocation Lists (ARLs) which conform to the CP and this CPS;
- Operates a repository for maintaining CA certificate information and status, publishing information to the repository consistent with this CPS;
- Revokes the CSOS SCA certificate if the CSOS SCA is found to have acted in a manner counter to those obligations to which it agreed to conform.;
- Provides for CSOS SCA certificate updating or re-keying.

1.3.1.4 CSOS Subordinate Certification Authority (CSOS SCA)

The CSOS Certification Authority is comprised of one Root CA and two logical SCAs. The CSOS SCA is an entity established and authorized by the PMA to create, sign, and issue public key certificates to authorized CSOS Subscribers through subordination to the CSOS Root CA. The CSOS SCA is operated and maintained by under the authority of the DEA. A description of the implementation may be found in Section 5 of this document. The CSOS SCA issues and manages CSOS Subscriber certificates and Certificate Revocation Lists (CRLs) in accordance with the terms and conditions specified within the most recent version of the CP.

1.3.1.4.1 CSOS SCA Obligations

The CSOS SCA complies with the provisions defined in the CSOS System CP, by following the procedures outlined in this CPS. Obligations include the following:

- Provides this CSOS CPS to the PMA, as well as any subsequent changes to the CPS, for conformance assessment in accordance with Section 9.12 of this CPS.
- Protects the CA’s private signing key in accordance with Section 5.2 of this CPS;
- Signs certificates only after verifying the identity of the certificate subject in accordance with Section 3.2 of this CPS;

- Verifies that the subject holds the private key corresponding to the public key in the certificate in accordance with Section 3.2.5 of this CPS;
- Uses the private signing key only when issuing certificates or signing Certificate Revocation Lists (CRL), following the procedures documented in the *Operations Management Guide.*
- Accepts registration information only from enrolled CSOS Coordinators as described in Section 3.2 of this CPS,
- Includes only valid and appropriate information in the certificate in accordance with Section 7.1 of this CPS,
- Maintains evidence that due diligence was exercised in validating the information contained in the certificate in accordance with Sections 4.1 and 4.3 of this CPS;
- Ensures that Subscribers are informed of their obligations and informed of the consequences of not complying with those obligations in a Subscriber Agreement and by requiring acceptance of these obligations and terms as a condition of certificate retrieval as specified in Section 3.2 of this CPS.
- Revokes the certificates of Subscribers found to have acted in a manner counter to those obligations as specified in Sections 4.8 and 4.9 of this CPS;
- Provides for certificate updating or re-keying as specified in Sections 3.3.1, 4.6, and 4.7 of this CPS;
- Operates or provides for the service of a repository for maintaining Subscriber certificate information and status as specified in Section 2.1 of this CPS;
- Maintains records necessary to support requests concerning its operation, including audit files and archives as specified in Sections 2.1 and 5.5 of this CPS;
- Accurately publishes CRLs, processes certificate applications and responds to revocation requests in a timely and secure manner as specified in Section 4.4.3 of this CPS.

1.3.2 Registration Authorities (RAs)

The CSOS Certification Authority also encompasses both the role and the functions of a Registration Authority (RA). The RA processes applications of CSOS Coordinators and Subscribers according to the stipulations of the Certificate Policy. The RA function includes both automated and manual processes performed by the CSOS RA and its associated Help Desk. In this CPS, the term *Registrar* is used to refer to an individual performing RA functions, while RA is used to refer to the total RA entity, including the software and its operations. Functions performed by the RA include:

- The verification and authentication of individuals or entities who are designated CSOS Coordinators;

- The approval or rejection of certificate applications;
- The initiation and authentication of certificate revocations; and
- The authentication of individuals or entities submitting requests to renew certificates or seeking a new certificate following revocation.

The following documents detail the RA's responsibilities and tasks specific to CSOS enrollment, adjudication and revocation processes:

- *CSOS Subscriber Manual* located at http://www.deaecom.gov;
- *Operations Management Guide* (RA and Help Desk Sections);
- *DEA Diversion Control RA System Design*.

1.3.2.1 RA Obligations

The CSOS RA is responsible for controlling the registration process through the adjudication of applications received from CSOS Coordinators and Subscribers, collecting and verifying the information to be entered into the certificates issued by the CSOS Certification Authority. In the performance of these duties, the CSOS RA is obligated to:

- Verify the accuracy and authenticity of the Subscriber information at the time of application for a certificate.
- Validate and process Subscriber certificate revocation requests in accordance with the stipulations of the CP and this CPS.
- Provide the CSOS Certification Authority with the necessary information to complete the certificate issuance and revocation processes.

1.3.3 Subscribers (all who transmit electronic orders)

A Subscriber is the entity whose name appears as the subject in a certificate issued by the CSOS CAs, who attests that they use the key and certificate in accordance with the Certificate Policy asserted in the certificate. DEA registrants are those entities required under the Federal Controlled Substances Act (CSA) to register with DEA. According to the CSA, a separate registration is required for each principal place of business or professional practice at one general physical location where controlled substances are manufactured, distributed, imported, exported, or dispensed by a person (21 U.S.C. 822(e)). Distributors, manufacturers, importers, and exporters of controlled substances fall into this category of DEA registrant. Other registrants include individual practitioners such as doctors, dentists, nurses, veterinarians, and other medical personnel who are not "an agent or employee of any registered manufacturer, distributor, or dispenser of any controlled substance or list I chemical."

There are various classes of DEA registrants: manufacturers, distributors, dispensers/ practitioners (which include hospitals, clinics, retail pharmacies, and teaching institutions), researchers, narcotic treatment programs, importers, exporters, and chemists. When the designation "registrant" refers only to an approved company location, that company must designate legal Powers of Attorney (POAs) the responsibility for ordering controlled substances on that company's behalf. CSOS Subscriber certificates are issued only by the CSOS Certification Authority and are limited to approved DEA Registrants and the company's holders of Powers of Attorney (POAs).

The CSOS Certification Authority limits the issuance of special purpose or administrative certificates to CSOS Principal and Alternate Coordinators, DEA employees, authorized Department of Justice (DOJ) officials, and properly cleared and approved contractor personnel. The *Subscriber Agreement* and *CSOS Subscriber's Manual* documents located at www.deaecom.gov provide enrollment instructions.

1.3.3.1 Subscribers Obligations

CSOS Subscribers are obligated to adhere to the regulations specified in 21 U.S.C. 1300-end and the responsibilities specified in the Subscriber Agreement (available at http://www.deaecom.gov).

1.3.4 Relying Parties (all who accept electronic orders)

A Relying Party is the entity that, by using a Subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message and relies on the validity of the public key bound to the Subscriber's name. The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

Relying Party Obligations

Relying Parties that accept orders for controlled substances are obligated to adhere to the regulations specified in 21 U.S.C. 1300-end.

1.3.5 Other Participants (CSOS Coordinator)

Each participating organization must designate Principal and optional Alternate CSOS Coordinators for each of its DEA registered locations. These CSOS Coordinators serve as the Local Registration Authority (LRA) for the DEA Registrations identified on their applications and are responsible for verifying the identity and applicability of organization personnel applying for a CSOS Certificate. CSOS Coordinators not possessing ordering authority receive administrative certificates for identification purposes when communicating electronically with the RA. The *Registrant Agreement* and the *CSOS Subscriber Manual* documents located at http://www.deaecom.gov detail the CSOS Coordinator's responsibilities.

CSOS Coordinator Obligations

For individuals applying for a CSOS certificate associated with a DEA registered location for which the CSOS Coordinator is responsible, the CSOS Coordinators:

- Verify the applicant's identity and employment;
- Verify that the applicant's CSOS application packet has been properly completed and signed by the applicant;
- Submit the signed application packet to the CSOS RA;
- Maintain evidence that due diligence was exercised in validating the information contained in the Subscriber's application;
- Serve as a point of contact for CSOS notification for their registered location, supplying confirmation of certificate requests, certificate renewals, and revocation requests.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

CSOS Subscriber certificates are only issued to entities engaged in the transfer of controlled substances between manufacturers, distributors, retail pharmacies, authorizing institutions and other registrants and must be used for the signing of electronic transaction orders, however the use of CSOS certificates is not restricted to this single application.

1.4.2 Prohibited Certificate Uses

CSOS certificates may not be used for the signing of electronically transmitted controlled substance prescriptions. The practices described in this CPS apply to the issuance and use of those certificates, Authority Revocation Lists (ARL) and Certificate Revocation Lists (CRL) for users within the CSOS Certification Authority domain.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The DEA, Office of Diversion Control, Technology Section, is the administering organization for this CPS.

1.5.2 Contact Person

The contact details for the CSOS System Certificate Policy and CSOS Certification Practices Statement are located at http://www.deaecom.gov. Written communication should be sent to:

Drug Enforcement Administration
Office of Diversion Control
Technology Section (ODT)
Attn: Chair, Policy Management Authority
Arlington, VA 22202

1.5.3 Person Determining CPS Suitability for the Policy

The CSOS System PMA is responsible for determining the suitability of this CPS and of the CSOS System. The PMA is responsible for the approval of the CP, approval of all Subscriber agreements, and the review and approval of this CPS to ensure its consistency with the CP. The CSOS Certification Authority is required to periodically attest to the compliance of the CPS to the CP as set forth in the CP.

1.5.4 CPS Approval Procedures

This CPS and all subsequent changes to the CPS will be formally approved by the PMA. The PMA must vote on the approval as detailed in the *PMA Operations Guide*.

1.6 Definitions and Acronyms

Definitions

Access Control Process of granting access to information only to authorized users, programs, processes, or other systems.

Activation Data Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Applicant The Subscriber is sometimes also called an “applicant” after applying to a CA for a certificate, but before the certificate issuance procedure is completed.

Archive Long-term, physically separate storage.

Audit Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Data Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.

Authenticate To confirm the identity of an entity when that identity is presented.

Authority Revocation List (ARL) A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.

Backup Copy of files and programs made to facilitate recovery if necessary.

Binding Process of associating two related elements of information.

Biometric A physical or behavioral characteristic of a human being such as a fingerprint.

Certificate A digital representation of identity. Subscriber certificates identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating the Subscriber is operating under the authority of the CSOS System program.

Certificate Policy (CP) A "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [X.509]. The CSOS System Certificate Policy specifies (1) the Certification Authorities, the Subscribers, and the Relying Parties authorized to participate in the PKI program described by this Policy, (2) the obligations of the participants governed by this Certificate Policy, and (3) the minimum requirements for the issuance and management of digital certificates used within the CSOS program and other suitable applications.

Certificate Revocation List (CRL) A list maintained by a Certification Authority of the certificates that it has issued that are revoked prior to their stated expiration date.

Certification Authority (CA) A Certification Authority issues digital certificates which contain a public key and the identity of the owner.

Certification Authority (CA) A Certification Authority refers to one or more Certificate Authorities operating in concert with a Root Certification Authority all within the same domain. These Certification Authorities may be subordinate to or peers of the Root Certification Authority. The Certification Authority attests that the public key contained in the certificate issued by the Certification Authority belongs to the person, organization, server or other entity noted in the certificate. A Certification Authority's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the Certification Authority's certificates.

CA Facility The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate Re-key The act or process of extending the validity of the certificate by issuing a new certificate with a new key pair.

Certification Practices Statement (CPS) A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific CP requirements

Compromise Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality Assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certified CA A Certification Authority that has been issued a certificate by the DEA CA that establishes a trust relationship between the CA and DEA CA in order that it may issue Subscriber certificates.

Cryptographic Module Set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

CSOS Controlled Substance Ordering System. A secure electronic system for the transmission of controlled substances orders without the supporting paper DEA Form 222.

Drug Enforcement Administration (DEA) The DEA regulates the manufacture and distribution of controlled substances in the United States.

DEA CA A term assigned to DEA’s Certification Authority that is comprised of a Root CA and Subordinate CAs. The Root CA issues other CA certificates as needed.

End Entity Relying Parties and Subscribers.

Federal Information Processing Standards (FIPS) These are Federal standards that prescribe specified performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc.

Firewall Gateway that limits access between networks in accordance with local security policy.

Intellectual Property Useful artistic, technical, and/or industrial information, knowledge Property or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Internet Engineering Task Force (IETF) A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the architecture and the smooth operation of the Internet.

Key Changeover The procedure used to change CA keys.

Key Escrow A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.

Key Pair Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.

Non-Repudiation Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID) An alphanumeric number registered with an internationally recognized standards organization used within PKI to uniquely identify policies and supported cryptographic algorithms.

Operations Management Authority (OMA) Parties responsible for managing all personnel and activities involved in the day-to-day operations of the Certification Registration Authority and Help Desk.

Policy Management Authority (PMA) Body established to oversee the creation and update of Certificate Policies, review Certification Practices Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.

Private Key (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure (PKI) A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA) CAs that process the registration of Subscribers and operate according to the stipulations of a Certificate Policy.

Relying Party A Relying Party is the entity that, by using a Subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message, and relies on the validity of the public key bound to the Subscriber's name. The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party must use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

Repository A database containing information and data relating to certificates as specified in this CPS

Revoke a certificate To prematurely end the operational period of a certificate effective at a specific date and time.

Risk An expectation of loss expressed as the probability that a particular threat exploits a particular vulnerability with a particular harmful result.

Root CA A term assigned to a Certification Authority that issues other CA certificates. The CSOS System Root CA serves as a "Root CA" to the CSOS Certification Authority. The Root CA operates in accordance with the provisions of its Certification Practices Statement. The Root CA performs the following functions: (1) accept and process applications for operations from subordinate CAs; (2) issue certificates to subordinate CAs approved by the PMA; (3) publish subordinate CA certificate status information.

Server A system entity that provides a service in response to requests from clients.

Subordinate CA (SCA) An SCA is a CA authorized by the PMA to create, sign, and issue public key certificates to authorized CSOS Subscribers. Subordinate CAs operate in a hierarchical PKI, subordinate to the Root CA.

Subscriber A Subscriber is the entity whose name appears as the subject in a certificate issued by a DEA CSOS Subordinate CA, who attests that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate. CSOS Subscribers are limited to DEA registrants and agents of registrants as stipulated in the Code of Federal Regulations (CFR) §1301.22.

Threat Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Trusted Role A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

Vulnerability Assessments Vulnerability assessments are conducted to identify potential vulnerabilities or events that would affect the integrity and operation of the CA.

Acronyms

Acronym	Description
AES	Advanced Encryption Standard
AICPA	American Institute of Certified Public Accountants
ARL	Authority Revocation List
CA	Certification Authority
CFR	Code of Federal Regulations
CIMC	Certificate Issuing and Management
CISA	Certified Information System Auditor
CN	Common Name
COTR	Contracting Officer's Technical Representative
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
CSOS	Controlled Substance Ordering System
CSS	Certificate Status Servers

Acronym	Description
DEA	Drug Enforcement Administration
DN	Distinguished Names
DNS	Domain Name System
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
EPCS	Electronic Prescriptions for Controlled Substances
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FTCA	Federal Tort Claims Act
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MOA	Memorandum of Agreement
NARA	U.S. National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OD	Office of Diversion Control
ODC	Office of Diversion Control CSOS Program
ODL	Office of Diversion Control Liaison and Policy Section
ODR	Office of Diversion Control Registration and Program Support Section
OID	Object Identifier

Acronym	Description
OMA	Operations Management Authority
PINS	Personal Identification Numbers
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
POA	Power of Attorney
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SA	System Administrator
SCA	Subordinate Certification Authority
SIA	Strong Identification and Authorization
SHA	Secure Hash Algorithm
SO	Security Officer
SSL	Secure Socket Layer
TLS	Transport Layer Security

Section 2 – Publication and Repository Responsibilities

2.1 Repositories

An X.500 directory provides the public repository for this Certification Authority in the external network. Access to the directory is provided through an interoperable implementation of the Lightweight Directory Access Protocol version 3 (LDAPv3). A web site is also provided to publish CSOS documentation.

Repository Obligations

The OMA operates and utilizes a variety of mechanisms as required by the CP to ensure that there is a repository where the CSOS CA certificates and CRLs are published. The mechanisms supported and operated include:

- An X.500 compliant Directory Service System with LDAPv3 access that allows authorized access and retrieval of the Certificate Revocation Lists and CSOS CA certificate information.

- A CSOS web site is maintained at http://www.deaecom.gov for posting CSOS public documentation including the CP, Subscriber Manual and other public documentation as appropriate. Access controls are implemented to ensure that the modifications to these documents are limited to authorized personnel only.

- The Certification Authority has implemented administrative access controls to protect the repository information from unauthorized access. The controls are enforced through application configuration and operating system Group Policy Objects (GPOs), in addition to procedural controls that ensure accountability.

- The Certification Authority has implemented system and environmental controls to ensure that a high level of reliability and availability is provided to the using community.

2.2 Publication of Certification Information

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the CA issues;

- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CA certificate;

- The SCA certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

In order to mitigate the risk of aggregated information contributing to the possibility of the diversion of controlled substances, Subscriber certificates are not posted into the CSOS repository.

The following CSOS PKI information is published on the web site at http://www.deaecom.gov:

- A copy of the CSOS System CP;
- A copy of the Subscriber Agreement;
- A copy of the Registrant Agreement;
- The CSOS DEA Registrant Certificate Application Checklist;
- Certificate application forms and instructions;
- Revocation request procedures;
- CSOS Certificate Profile and CSOS Certificate and CRL Profile
- The official list of PMA members;
- Contact details for this CPS and PKI;
- A copy of the CSOS Subscriber Manual.

Changes to items within this CPS, which have minimal or no impact on the Subscriber using certificates and CRLs issued by this CSOS Certification Authority, are made with no change to the CPS version number.

2.3 Time or Frequency of Publication

CRLs issued by the Certification Authority are automatically published in the directory as soon as they are issued. The frequency of CRL issuance is discussed in Section 4.9.7 of this CPS.

Changes to the certificates supported by this CPS as well as changes to items within this CPS which may have significant impact on the Subscriber using certificates and CRLs issued by the CSOS Certification Authority, are made with 30 days notice to the user community, and the version number of this CPS must be increased accordingly.

2.4 Access Controls on Repositories

The CSOS web site enables read-only access to the CP and other public documents contained in the site to Internet users. Only authorized CSOS personnel logged-on locally (interactively) at the Web server are able to modify or post documents on the CSOS web site.

Detailed information on facility and logical access controls are contained in the System Security Plan. Access control policies are covered and included in the Rules of Behavior that are provided to all employees.

Section 3 – Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Names of certificate subjects must be X.500 Distinguished Names (DN) using a set of the following X.520 naming elements: C; O; OU; and CN.

3.1.2 Need for Names to be Meaningful

All certificates issued by the CSOS Certification Authority contain the DN of C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversion Control, OU=E-Commerce, OU=CSOS, OU=”State.” Subscriber certificates include the common name (CN) of the individual using the certificate and a serial number that is unique to the Subscriber. The presence of the unique serial number guarantees that although the CN may not be unique, the DN is always unique to each Subscriber.

The CN is generated according to these rules:

- From the Subscriber’s legal name as it appears on the DEA Form 223.
- If this name cannot be used, the name that Federal or local records refer to that person as (e.g., POA (Power of Attorney) letter, human resources documents, birth certificate or driver’s license) are used.

3.1.3 Anonymity or Pseudonymity of Subscribers

In the event that a person is known by a name that is different then the name used to create the CN, additional CN values maybe added—at the request of the Subscriber—to the CN attribute after the DN has been formed. If these rules cannot resolve any naming issue, the issue is resolved by the PMA according to the procedures in Sections 9.13 and 9.16.4 of this document. The certificate subject field is the identity of the Subscriber who is being assigned the certificate from the issuing CA.

3.1.4 Rules for Interpreting Various Name Forms

DNs and their component Relative Distinguished Names (RDNs) are to be interpreted as defined in the applicable certificate profile and in Section 3.1.4 of this CPS. The *CSOS System Certificate and CRL Profile* document established by the DEA contains the rules for interpreting name forms. These documents may be found at http://www.deaecom.gov.

3.1.5 Uniqueness of Names

Names are unambiguously defined for each Subscriber, as described in the preceding subsections. As stated in Section 3.1.2, the presence of the unique serial number guarantees that although the CN may not be unique, the DN is always unique to each subscriber. Certificates issued from the CA or RA (i.e. service accounts) have the service account name contained in the

CN, however do not include the S/N. It is the responsibility of the CA to resolve all conflicts to ensure that name uniqueness is maintained.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificate subject names issued under this policy are chosen by the CA. The CA is not obligated to research trademarks or resolve trademark disputes. The CA or its agents may refuse to accept a name known to be a trademark of someone else, or deemed inappropriate for use in the certificate.

The OMA refers disputes with names, including disputes involving trademarked names, to the PMA for resolution. The CSOS PMA is ultimately responsible for resolution of any name claim disputes within the CSOS PKI and may direct the revocation and re-issuance of any affected certificates. The CSOS PMA provides the CSOS RA with the results of their decisions who, in turn, notifies the applicant and CSOS Coordinator via email or postal mail.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

CSOS Subscribers generate their own keys within their system as an automatic process described in Section 4.3.2. For signature public keys, the corresponding private key automatically signs the certificate request generated by the Subscriber. Verification of the signature using the public key in the request serves as proof-of-possession of the private key.

The CSOS Certification Authority does not verify the uniqueness of Subscriber public keys during the certificate issuance process. Proof-of-possession of the private key is required before obtaining a certificate from the CA, preventing malicious attempts to re-use a public key. Section 4.1.2 - Enrollment Process and Responsibilities, covers the accountable method for delivering certificates to users requesting certificates. Before being able to obtain a certificate, a DEA Registrant must receive a reference code(s) and authorization code. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the address provided by the CSOS Coordinator on the application in a tamper evident envelope. After receiving the authorization and reference code(s), the DEA Registrant returns to the CSOS web site to retrieve his/her CSOS Certificate(s). Client-side key generation modules are required to be FIPS-validated, which gives a high degree of confidence in the entropy of the random number generation.

3.2.2 Authentication of Organization Identity

CSOS Certification Authority certificates are issued to organizations for the purpose of cross-certification only and require PMA approval in advance of issuance. The RA verifies organizational identity using third-party knowledge broker data, D&B (Dun and Bradstreet, a provider of international and US business credit information and credit reports) listings, etc. and provides the results of this information and the tools used for verification at the time the request is provided to the PMA for review.

3.2.3 Authentication of Individual Identity

3.2.3.1 CSOS Coordinator Identification Process

A Principal Coordinator and optional Alternate Coordinator are identified for each DEA Registrant (as indicated on DEA Form 223) participating in the Controlled Substance Ordering System. The Principal Coordinator serves as an organization's primary recognized CSOS contact for the DEA Registrant(s) identified on their application. The Principal Coordinator applicant may be any individual employed or contracted by the organization designated to serve in that role. If a CSOS DEA Registrant Certificate Application is submitted, the DEA Registrant serves the role of Principal Coordinator unless otherwise indicated on the application.

A CSOS Coordinator application must be received by the CSOS RA along with, or prior to, any CSOS Subscriber certificate applications. CSOS Coordinators submit the following information/credentials to the CSOS RA for identity verification:

- A signed and notarized CSOS Coordinator application obtained from the CSOS web site. This application must be signed by the same individual who has signed the most recent application for DEA Registration (DEA Form 223) or by the person authorized to sign the next application for DEA renewal and authorizes the individual listed on the application to represent the organization in the capacity of the CSOS Coordinator.

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport.

- A copy of a current DEA Registration (Form 223) or the most recent application for DEA registration in the event that application for DEA Registration and a CSOS Coordinator certificate are simultaneously submitted.

- For individuals granted Power of Attorney (POA) to sign orders for controlled substances on behalf of a DEA Registrant, a copy of the POA assignment letter as specified in Title 21 Code of Federal Regulations (CFR), Parts 1300-1399 (commonly referred to as 21CFR, Parts 1300-1299).

The CSOS RA notifies the applicant via e-mail upon receiving the application package and adjudicates the applicant through the following procedures:

- Validates that all required information and documentation has been provided.

- Validates that the Notary information is complete, identification documents match information provided on the application, and through performing an out-of-band telephone verification of employment, position, and location through organization's Human Resource department or with the owner/operator of smaller business entities.

- Validates the DEA Registrant(s) provided information, including business activity, schedules and DEA Registration expiration date against DEA CSA data provided by DEA.

- Verifies the organization mailing address and the employment of the individual at the provided address.

3.2.3.2 CSOS Subscriber Identification Process

Authentication of Subscriber identity is performed by the local organization and requires the delegation of a CSOS Coordinator, who serves as the LRA and organizational point of contact for CSOS issues. Subscribers submit the following information/credentials to their designated CSOS Coordinator for identity verification:

- A CSOS Certificate application, signed by the applicant, stating that the applicant has read and understands the terms of the CSOS CP and has agreed to the statement of Subscriber obligations in the Subscriber Agreement;

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;

- For individuals with power of attorney (POA) to sign orders for controlled substances, a copy of the POA assignment letter as specified in Code of Federal Regulations (CFR).

- A CSOS Certificate Application Registrant List Addendum used for individuals who wish to apply for a CSOS Certificate for more than one DEA Registrant. Up to 5 Addendums may be submitted to specify up to 51 different DEA Registrants. (Practice note: this event occurs when a single individual is granted multiple POA to order for several DEA Registrants (registered locations). An example is with chain pharmacies where a single individual orders controlled substances for all company locations).

The Principal Coordinator/Alternate Coordinator adjudicates the Power of Attorney applicant. This includes validating the following:

- All required information/documentation is provided.

- Applicant identity is adjudicated as specified in the DEA Registrant agreement.

- The Affirmation of Identity Verification section of the application is signed by the Coordinator.

The Coordinator maintains a copy of the application package and the method by which the identity was verified for their records. Upon signing the application, the Coordinator forwards, via postal mail, the application packet to the CSOS RA.

The CSOS RA notifies the applicant and Principal Coordinator/Alternate Coordinator via e-mail upon receiving the application package. The CSOS RA then validates that the application has been properly completed with all required information and documentation provided. The RA then cross-references application information with relevant information from the database.

The required steps the RA Operator must complete for each application type are summarized in Table 3–1, Adjudication Procedures:

Adjudication Procedures			
	Application Type		
Steps	Registrant	Coordinator	POA
1. All of the application fields are complete and valid	✓	✓	✓
2. All required signatures are present.	✓	✓	✓
3. Identification documents provided match the individual represented on the application.	✓	✓	✓
4. The signature on the application is similar to the signature on the identification documents provided.	✓	✓	✓
5. Applicant is presently employed by the organization identified on the application.	✓	✓	
6. Applicant’s place of employ matches business address presented on the application.	✓	✓	
7. The address of the organization must match the organization address provided on the application.		✓	
8. Power of Attorney documentation is present for the DEA Registration(s) identified on the application		✓*	✓
9. Proof of DEA Registration (Form 223 or the application for DEA Registration)	✓	✓	
* POA form is only necessary if Coordinator is applying for a POA certificate.			

Table 3–1. Adjudication Procedures

3.2.3.3 CSOS Subscriber Bulk Enrollment

DEA issues a separate DEA Registration to each location authorized to handle controlled substances. In some business cases, such as with chain pharmacies utilizing a centralized ordering business model, a single individual may be assigned the responsibility for ordering controlled substances for many different locations, some with different authorized controlled substance schedules. Under CSOS, a single individual would need to hold separate digital certificates for each registered location – using that Registrant’s certificate to sign orders for controlled substances authorized for delivery to that location. To accommodate these business cases within CSOS, DEA has established Bulk Enrollment procedures.

In order to participate in CSOS Bulk Enrollment, an organization must currently participate in the DEA Chain Renewal program. The Chain Renewal procedure, described at http://www.deadiversion.usdoj.gov/drugreg/chain_renewal.htm, was developed by DEA to simplify the renewal application process for companies that maintain registrations at multiple locations, for example chain pharmacies. The procedure allows corporations to renew all of their DEA registrations at the same time, thereby eliminating the need for multiple applications. This simplified application process is available to corporations with 50 or more retail pharmacy registrations or distributors with 10 or more registered locations.

To enroll in CSOS under Bulk Enrollment processes, each applicant (DEA Registrant, Principal Coordinator, Alternate Coordinator, and POA) completes his/her application as specified in the above processes, with the exception of how the DEA Registration and POA documentation is submitted. The CSOS RA works with the organization’s primary point of contact for bulk enrollment to ensure the DEA Registration and POA documentation are submitted correctly.

For the DEA Registrations for which the applicant is applying, the organization will provide the following:

- A printed list of the DEA Registrations (including all pertinent information such as DEA Registration Number, name, address and current expiration date) listed in order by DEA Registration Number.
- A CD with the DEA Registration Numbers only in alphanumeric order in ASCII format.
- For POA applicants, the organization will provide a single POA listing all of the DEA Registration Numbers for which the applicant is applying.

3.2.3.4 Authentication of Component Identities

The CSOS SCAs issue administrative digital certificates:

- Through the software application for use by CA personnel.
- To the components:
  - The CSOS Web server, to secure communications using Secure Socket Layer (SSL);
  - The CSOS RA e-mail system, to authenticate messages for Enrollment, Renewal, and Revocation purposes.

These certificates differ from CSOS Subscriber certificates in that they do not assert the CSOS OID and are not populated with DEA extension data. DEA Regulations (specified in the 21 U.S. Code of Federal Regulations) prohibit the use of digital certificates not containing this extension data for controlled substance ordering.

Administrative certificates issued by the CSOS Certification Authority must be associated with a PKI sponsor. Requests for certificates are submitted to the CSOS RA by the Program Manager and include the following information:

- Date of Request
- Employee Name
- Employee ID#
- Certificate Distinguished Name (DN) as the unique identifier for the certificate
- Reason for request
- Transfer of ownership (if applicable)
- If the request is for a component, the request must include the equipment identification information (serial number) or service name (DNS name)
- Contact information to enable the CA or CSOS RA to communicate with the PKI sponsor
- The Program Manager's signature to indicate request approval.

The applicant then provides the signed request form to the CSOS Certification Authority, who generate a certificate request and ensure that the sponsor retrieves the certificate in a manner that guarantees that the private key remains under the sole control of the employee.

Upon retrieval of the certificate, the request form is updated to include the certificate DN as discussed above and the signed request is provided to the Security Officer to file.

Administrative, device, and component certificates are issued for a period not to exceed three years. Upon expiration or update, the user associated with the device or component certificate must complete a new request for a certificate, using the procedure outlined above.

Administrative, device and component certificates are revoked immediately upon the sponsor or individual's employment termination with CSOS or upon notification to the RA of suspected compromise.

The Program Manager completes and signs revocation requests, indicating the date and reason for the request on the original form obtained from the Security Officer and then distributing the form to the CA Operator for action and signature. This form is then provided to the Security Officer to be archived.

Revoked administrator, device and component certificates are added to the CRL in the same manner as CSOS Subscriber certificates.

3.2.4 Non-Verified Subscriber Information

Information that is not verified is not included in certificates.

3.2.5 Validation of Authority

3.2.5.1 CSOS Coordinator Registration

While it is not required that a CSOS Coordinator be a DEA Registrant or have been provided POA to order controlled substances for the Registrant, DEA Registrants and POAs may serve as either CSOS Coordinators or Subscribers, and, in some instances, may be both the CSOS Coordinator and Subscriber. CSOS Coordinators largely consist of regulatory personnel assigned by DEA Registrants; Relying Parties in CSOS are generally comprised of suppliers and manufacturers. It is not anticipated that a business model would arise that would result in a CSOS Subscriber/POA additionally serving in a role as a Relying Party to a transaction signed using a CSOS Subscriber certificate issued to their own DEA Registration.

Applications are identified on the DEA web site and instructions are provided to walk the applicant through the registration process. To be designated a CSOS Coordinator an applicant must:

(i) Complete and submit a signed, notarized CSOS Coordinator application to the CSOS RA, providing all information requested by the CSOS RA without any errors, misrepresentation, or omissions. Send the notarized application to the CSOS Registration Authority at Sterling Park Technology Center/CSOS, 8701 Morrissette Drive, Springfield, VA 22152. This application must be received along with or prior to any CSOS certificate applications. Registrants and POAs applying as the CSOS Coordinator will be given the option to request a CSOS certificate by indicating so on his/her application form.

(ii) Agree to all of the terms and conditions of the CP, Registrant Agreement, and the Subscriber Agreement. The agreement is presented as a “click-through” on the http://www.deaecom.gov site. The Subscriber or Coordinator must accept the terms of the Agreement in order to retrieve their certificate.

3.2.5.2 CSOS Subscriber Registration

CSOS Subscribers must either be DEA Registrants or have been assigned POA by the Registrant to order controlled substances. To obtain a CSOS Subscriber certificate, an applicant must:

(i) Complete and submit a signed CSOS certificate application, providing all information requested by the CSOS RA without any errors, misrepresentation, or omissions. Applications and instructions for registrants, or those who hold POA for registrants, are located on the CSOS web site, http://www.deaecom.gov.

(ii) Agree to all of the terms and conditions of the CP and the Subscriber Agreement. The agreement is presented as a “click-through” on the http://www.deaecom.gov site. The

Subscriber or Coordinator must accept the terms of the Agreement in order to retrieve their certificate.

(iii) Submit the application to their designated CSOS Coordinator for identity verification.

Once a Subscriber has completed the CSOS certificate application and accepted the terms and conditions of the CP and the Subscriber Agreement, the application is submitted to the CSOS Coordinator for identity and authorization verification. The CSOS Coordinator must sign the certificate application, supplying all requested information. The CSOS Coordinator must then submit all verified applications for certificates to the CSOS RA. Applications received directly from the applicant or missing the CSOS Coordinator's signature will not be processed.

Upon receipt of the application packet(s) by the CSOS RA, a CSOS RA Operator verifies the information contained in the CSOS certificate application against DEA's database. The PMA ensures that the database information is readily available for verification.

Upon application approval, the CSOS RA notifies the CA of approval and the CA issues a CSOS certificate to the applicant. If the application is denied, the CSOS RA uses reasonable efforts to notify the applicant and the applicant's CSOS Coordinator by electronic or postal mail of the refusal and reasons for the refusal.

In the event of successful adjudication of a CSOS certificate application, the applicant will receive notice of where to access the CSOS Certification Authority and how to generate the private and public keys and retrieve the CSOS certificate. The applicant's CSOS Coordinator will also receive notice that the applicant has been approved for a CSOS certificate.

3.2.6 Criteria for Interoperation

The CSOS PKI has cross-certified with the FBCA as of August 2005. This cross-certification is in compliance with the U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria which can be found at the URL below:

http://www.cio.gov/fbca/documents/crosscert_method_criteria.pdf.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

3.3.1.1 CSOS Subscribers

The Subscriber, through the CSOS Coordinator, may request that the CSOS Certification Authority issue a new CSOS certificate containing a new serial number with a new key pair, provided that the original certificate has not been revoked and the Subscriber is in good standing with the Certification Authority, continuing to qualify as a DEA registrant or POA, as defined in Section 1.3.3. The CSOS System CP does not permit Subscriber certificate renewal (issuance of a new certificate for an existing key pair).

Re-key requests can be authenticated on the basis of the CSOS Coordinator’s digital signature using the current private key for a total of two certificate requests beyond the initial request. Upon the third certificate request, Subscribers are required to establish identity using the initial registration process described in Section 3.2.

All re-key requests are adjudicated by the CSOS RA and checked to ensure 1) that the digital signature signing the request is validated against the one issued to the Subscriber or Coordinator, 2) checked to ensure that the certificate has not been revoked or suspended, and 3) checked against the database to ensure that the extension data is still valid. After adjudication, the request is entered into the RA database and sent to the CSOS Certification Authority as previously discussed.

DEA updates its database upon the receipt of information changes from the Registrant and from Registration renewal requests from the organization with whom the CSOS Coordinator is associated.

Under normal circumstances, Subscribers and Coordinators not receiving their certificates within 10 business days from the receipt of CSOS RA notification of the submission package can contact the CSOS Help Desk to check status.

Requests for new certificates due to name changes (e.g. due to marriage) require proof of the name change be provided to the CSOS Coordinator, or other designated agent. The CSOS Coordinator serves as the certifier for the name change request submitted to the CSOS RA. Requests for new certificates due to a change of other information present in the Certificate extension data (reduction or addition of controlled substance ordering authorization, Registrant address or DEA Registration number) requires the Subscriber to establish identity using the initial registration process described in Section 3.2.

3.3.1.2 CSOS Certification Authority Re-Key

The CSOS Root CA is a self-signed root, cross-certified with the FBCA. Both the CSOS Root CA and the CSOS SCAs generate and store their private keys using a FIPS 140 level three certified Hardware Security Module (HSM). Re-keying of the CSOS Root CA is completely internal to the Certification Authority and the generation of the CA’s new keys takes place within the HSM. The CSOS Root CA key pair and certificate do not exceed the lifetimes stated in the CP. The Root and CA Key Changeover Schedule is provided in the *CA Operations Guide*.

The CSOS SCA participates in an offline subordination process with the CSOS Root CA at the time of re-key. The subordination process (in which the CSOS Root CA signs the CSOS SCA’s certificate) is done using removable media transferred between the two SCAs. The entire process is contained within the domain of the two SCAs. No outside entities are involved in the subordination process. As with the CSOS Root CA, the CSOS SCA’s certificate and public and private key lifetimes do not exceed the durations set forth in the Diversion CP.

The new public key is posted on the web site at http://www.deaecom.gov and notification of the re-key is provided through a digitally signed email from the CSOS RA to the CSOS Coordinators.

3.3.2 Identification and Authentication for Re-Key After Revocation

In the event of certificate revocation for reason of key compromise, cessation of operation, or as a result of negative action taken against the Registrant or Subscriber by DEA, issuance of a new certificate always requires that the Subscriber go through the initial registration process as described in Sections 3.2. Certificate revocation due to a technical malfunction that makes the private key invalid does not require renewal via initial enrollment provided that the previous adjudication was performed within 60 days of certificate revocation and the renewal request has been approved by the CSOS Coordinator.

3.4 Identification and Authentication for Revocation Request

Requests for certificate revocation require either verbal authentication using a security code known only to the Subscriber and the RA, a signature on the revocation request from a person identified in Section 4.9.2 of this document along with any information covered in Section 4.9 of this CPS.

Electronic revocation requests are authenticated using the certificate’s associated private key, regardless of whether or not the private key has been compromised. The RA uses reasonable efforts to notify the Subscriber, Registrant, or applicable CSOS Coordinator about the revocation of the CSOS certificate via electronic means, mail, or telephone call. Revocation request procedures are described in Section 4.9.3.

Revocations processed as a result of information received in DEA’s database do not require additional authentication.

Section 4 – Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Eligible Subscribers are those who hold a valid DEA registration as defined in Title 21 CFR Parts 1300-1399. All Subscriber applicants submit a completed application and documents substantiating identification in accordance with Section 3.2 above, entering into an initial agreement with the CA evidenced by accepting the applicable DEA Registrant or Subscriber Agreement at the CSOS web site, prior to certificate issuance. Complete application processing information is contained in the RA Section of the Operations Guide.

4.1.2 Enrollment Process and Responsibilities

Certificate application forms and instructions may be obtained from, http://www.deaecom.gov. The applicant follows the procedures in the Subscriber Manual posted on the CSOS web site at, http://www.deaecom.gov, mailing completed applications to the CSOS Registration Authority at Drug Enforcement Administration, Sterling Park Technology Center/CSOS 8701 Morrissette Drive Springfield, VA 22152.

Using the information provided with the application, the CSOS Coordinator performs identity verification according to the requirements specified in the CP and this CPS. Subscriber applications are scanned by the RA and are entered into the RA database prior to adjudication. Based on subsequent verification against the database, the CSOS RA either approves or denies the application. The CSOS RA notifies the Registrant or the Registrant's CSOS Coordinator when the application is received via email. The CSOS RA notes all action taken on the certificate request in the CSOS RA database and retains the certificate request. Should the application be denied, the CSOS RA provides notification of the application denial to the applicant and the applicant's CSOS Coordinator.

The procedures developed and published on the CSOS web site are included in the CSOS Subscriber Manual and are as follows:

1. The Subscriber applicant accepts the CSOS Certification Authority certificates from a link provided on the CSOS web site in order to trust certificates issued by the CSOS Certification Authority.

2. The Subscriber applicant downloads the applicable CSOS enrollment application. Application forms and instructions are provided for the following CSOS Subscribers:

CSOS DEA Registrant Certificate Application –The following steps outline the DEA Registrant Certificate application process:

1. The applicant reads/agrees to the DEA Registrant Agreement, the CSOS Subscriber Agreement and the CSOS Privacy Policy.

2. The DEA Registrant completes the CSOS DEA Registrant Certificate Application and the CSOS Certificate Application Registration List Addendum(s) if applicable.

3. On the application, the DEA Registrant must designate a Principal Coordinator. The Principal Coordinator must be approved prior to the RA processing CSOS Power of Attorney or Alternate Coordinator certificate applications. These Coordinators serve as the organization's LRA.

4. The DEA Registrant has the application and addendum(s) (if applicable) notarized.

5. The DEA Registrant attaches a photocopy (ies) of the DEA Registration Certificate(s) for the DEA Registration(s) identified, and photocopies of their identification documents and then mails the application package to the CSOS RA.

6. The CSOS RA notifies the DEA Registrant via e-mail upon receiving the application package.

7. The RA verifies the identity of the DEA Registrant and validates the DEA Registration(s) identified.

8. Upon approval, the CSOS Certification Authority sends the authorization and reference code(s) to the DEA Registrant. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the address provided by the CSOS Coordinator on the application in a tamper evident envelope.

9. After receiving the authorization and reference code(s), the DEA Registrant returns to the CSOS web site to retrieve his/her CSOS Certificate(s).

<u>CSOS Principal Coordinator/Alternate Coordinator</u>–A Principal Coordinator must be approved prior to the RA processing CSOS Power of Attorney or Alternate Coordinator certificate applications. The following steps outline the CSOS Principal Coordinator / Alternate Coordinator application process:

1. The DEA Registrant designates the CSOS Principal Coordinator/Alternate Coordinator applicant for the DEA Registration(s) identified.

2. The applicant reads/agrees to the DEA Registrant Agreement, the CSOS Subscriber Agreement and the CSOS Privacy Policy.

3. The applicant completes the application and has the application signed by the DEA Registrant.

4. The applicant has the application and addendum(s) (if applicable) notarized.

5. The applicant attaches a photocopy(ies) of the DEA Registration Certificate(s) and Power(s) of Attorney (if applicable) for the DEA Registration(s) identified and

photocopies of their identification documents, and then mails the application package to the RA.

6. Once the RA receives the application package, the RA notifies the applicant via e-mail upon receiving the application package.

7. The RA verifies the identity and applicability of the applicant and validates the DEA Registration(s) identified.

8. Upon approval, the CSOS Certification Authority sends the authorization and reference code(s) to the applicant. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the address provided on the application.

9. After receiving the authorization and reference code(s), the applicant returns to the CSOS web site to retrieve his/her CSOS Certificate(s).

CSOS Power of Attorney Certificate Application–A Principal Coordinator must be approved prior to the RA processing CSOS Power of Attorney or Alternate Coordinator certificate applications. The following steps outline the CSOS Power of Attorney Certificate application process:

1. The applicant reads and agrees to the CSOS Subscriber Agreement and the CSOS Privacy Policy.

2. The applicant completes the CSOS Power of Attorney Certificate Application.

3. The applicant attaches the CSOS Certificate Registration List Addendum(s) (if applicable) and the Power(s) of Attorney for the DEA Registration(s) identified and then forwards the application to either the Principal Coordinator or the Alternate Coordinator.

4. The Principal Coordinator/Alternate Coordinator adjudicates the Power of Attorney applicant as defined in the DEA Registrant Agreement.

5. The Principal Coordinator/Alternate Coordinator forwards the original application package to the RA.

6. Once the RA receives the application package, the RA notifies the applicant and Principal Coordinator/Alternate Coordinator via e-mail upon receiving the application package.

7. The RA validates the application and DEA Registration(s) identified.

8. Upon approval, the RA sends the reference code(s) to the applicant via e-mail. The authorization code(s) is sent by the Principal Coordinator/Alternate Coordinator via

postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code(s) to the applicant.

9. After receiving the authorization and reference code(s), the applicant returns to the CSOS web site to retrieve his/her CSOS Certificate(s).

Bulk Enrollment Applications–In order to participate in CSOS Bulk Enrollment, the applicant must be applying for more than 50 CSOS Certificates and the organization must currently participate in the DEA Chain Renewal program for DEA Registrations. Bulk Enrollment has been established to accommodate organizations that need to obtain a large volume of CSOS Certificates associated with a single applicant. Each applicant, DEA Registrant, Principal Coordinator, Alternate Coordinator, and Power of Attorney, completes his/her application as previously specified with the exception of how DEA Registration and Power of Attorney documentation is submitted. DEA Registration and Power of Attorney documentation will be submitted as described below. The CSOS RA works with the organization's primary point of contact for bulk enrollment to ensure the DEA Registration and Power of Attorney documentation is submitted correctly.

1. For the DEA Registrations for which the applicant is applying, the organization provides the following:

- A printed list of the DEA Registrations (including all pertinent information such as DEA Registration Number, name, address and current expiration date) listed in order by DEA Registration Number.

- A CD with the DEA Registration Numbers in alphanumeric order only, saved as an ASCII text file.

This information is mailed to: Drug Enforcement Administration, Sterling Park Technology Center/CSOS, 8701 Morrissette Drive Springfield, VA 22152. For Power of Attorney applicants, the organization will provide a single Power of Attorney listing all of the DEA Registration Numbers for which the applicant is applying.

1. The Organization provides a contact point including Corporate Name, address, telephone number, fax number, individual contact and alternate contact for the bulk enrollment process.

2. Upon receipt of the package, the CSOS RA validates the application and DEA Registration(s) identified.

3. Upon approval, the CSOS Certification Authority creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrants identified. The reference code file is sent to the applicant via e-mail. The authorization code file is sent on compact disk (CD) to the address provided by the Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code(s) to the applicant.

4. After receiving the authorization and reference code(s), the applicant returns to the CSOS web site to retrieve his/her CSOS certificate(s).

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Subscriber information is verified against a daily extract of DEA Registrant information contained in DEA's database. DEA's database extract is delivered electronically to the CSOS RA through the closed DEA Firebird communications system that prevents external tampering with the file. The file is programmatically retrieved and made available to the CSOS RA database for adjudication purposes.

Upon receipt of the application package from the CSOS Coordinator, the package is validated by the CSOS RA for completeness and then scanned into the CSOS RA database. The fields within the scanned application are automatically parsed and processed against DEA's database extract to validate DEA authorization, business activity and drug schedules that become part of the certificate extensions. Errors detected at this point are reported to the CSOS RA, who, in turn, notifies the applicant and their CSOS Coordinator via email. It is the CSOS Coordinator's responsibility to contact DEA to resolve errors in the database.

The unique identification number of the identifications presented is recorded on the DEA Registrant and Coordinator Applications by the Notary Public and the photocopy of the identification documents are filed with the application and are also contained with the image of the application created during document scanning. Applications and photocopies of identification documents are stored in locked file cabinets with limited access. Access is limited to only individuals with a need to know.

The electronic workflow application maintains custody of the workflow package until completion of the adjudication

4.2.2 Approval or Rejection of Certificate Applications

Based on subsequent verification against the database, the CSOS RA either approves or denies the application. The CSOS RA notifies the Registrant or the Registrant's CSOS Coordinator when the application is received via email. The CSOS RA notes all action taken on the certificate request in the CSOS RA database and retains the certificate request. Should the application be denied, the CSOS RA provides notification of the application denial to the applicant and the applicant's CSOS Coordinator.

4.2.3 Time to Process Certificate Applications

Upon receipt, Registrant applications are examined for completeness. Applications that are incomplete (incorrect information, missing attachments, etc.) are returned to the applicant for correction. Details on the time to process certificate applications can be found in the *RA Ops Guide*, Section 5100.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Upon successful adjudication, the CSOS RA submits applicant information to the CSOS Certification Authority, instructing the CA staff to issue the certificate to the applicant. The Certification Authority provides the individual with one-time use reference and authorization codes. The CA, via an automated script, sends the reference code to the applicant via e-mail. The authorization code is distributed to the Principal Coordinator/Alternate Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code to the applicant. The Subscriber must possess both pieces of information in order to authenticate themselves for certificate use at their initial login. Email notifications are distributed to the CSOS Coordinators and Subscribers. Subscribers are required to use these within 60 calendar days and must not divulge the codes prior to use.

For bulk enrollments, The CSOS RA adjudicates the applicant as previously discussed, and associates the applicant with the Principal Coordinator for the DEA Registrations identified in the RA database. Upon approval, the CSOS Certification Authority creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrations identified. The reference code file is sent to the applicant via e-mail. The authorization code file is sent on a compact disk (CD) to the applicant via the applicant’s designated Coordinate via postal mail.

The CSOS Certification Authority receives its initial subordination certificate signed by the CSOS Root CA during a Key Generation ceremony audited by KPMG.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The Subscriber is mailed a URL and user login and password to an SSL-secured CSOS web site that then launches the certificate retrieval process at the Subscriber’s client. Entering the reference and authorization codes, the applicant’s software generates the key pair in the applicant’s system while accessing the SSL-secured CSOS web site using the access code and password. The public key is then automatically submitted in a certificate request to the CSOS Certification Authority.

The CSOS Certification Authority software automatically verifies the certificate request, signs the signing public key certificate, and stores a copy of the certificate in the CSOS Certification Authority database. The CSOS Certification Authority then provides a copy of the signing public key certificate to the client electronically through the program during the session. Next, the CSOS Certification Authority writes the public certificate into the CSOS repository. The issuance of a certificate by the CSOS Certification Authority indicates the end of the certificate issuance process. Subscriber acceptance of the certificate is covered in the following section.

The DEA-customized certificate specification, described in the CSOS System Certificate and CRL Profile Guide, contains a set of pre-defined values that the CA software uses to validate certification information prior to processing a certificate request. These values include the controlled substance schedules that the Subscriber can order, business activity and DEA Registrant location. CA software is used to automatically validate that the certificate fields, including public key and extensions, are properly and accurately populated in the Subscriber certificates.

The RA workflow and certificate issuance processes are monitored to ensure that these processes continue to compare favorably with baseline performance metrics.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Acceptance of the certificate occurs when the Subscriber uses the auth/ref codes distributed by the RA and their CSOS Coordinator to generate a certificate request and retrieve the certificate. The operation of the secure communications protocol between the Subscriber and the CSOS Certification Authority involves the mutual authentication of the two parties along with both the request and the response operations that constitute acceptance by the Subscriber of the resulting public key certificates. This process is also covered in Section 6.1.3 of this document.

4.4.2 Publication of the Certificate by the CA

The OMA operates and utilizes a variety of mechanisms as required by the CP to ensure that there is a repository where the CSOS Certification Authority certificates and CRLs are published. The mechanisms supported and operated include:

- An X.500 compliant Directory Service System with LDAPv3 access that allows authorized access and retrieval of the Certificate Revocation Lists and the CSOS Certification Authority certificate information.

- A CSOS web site is maintained at http://www.deaecom.gov for posting CSOS public documentation including the CP, Subscriber Manual and other public documentation as appropriate. Access controls are implemented to ensure that the modifications to these documents are limited to authorized personnel only.

- The Certification Authority has implemented administrative access controls to protect the repository information from unauthorized access. The controls are enforced through application configuration and operating system Group Policy Objects (GPOs), in addition to procedural controls that ensure accountability.

The Certification Authority has implemented system and environmental controls to ensure that a high level of reliability and availability is provided to the using community.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the CA issues;
- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS Certification Authority certificate;
- The CSOS Certification Authority certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

CSOS Subscribers are obligated to adhere to the regulations specified in 21CFR, Parts 1300-1399 and the responsibilities specified in the Subscriber Agreement (available at http://www.deaecom.gov).

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties that accept orders for controlled substances are obligated to adhere to the regulations specified in 21CFR, Parts 1300-1399.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

The CSOS RA sends an automatically scheduled email notifying the Subscriber and the Subscriber's CSOS Coordinator 45 days prior to the expiration date of the Subscriber's CSOS certificate. The CSOS Coordinator will receive two notifications at this time, the first notification contains a listing of Subscribers who have renewed twice previously and are now required to renew via the initial enrollment process, and the second notification contains a listing of CSOS Subscribers who are eligible for electronic renewal.

4.6.2 Who May Request Renewal

The Subscriber's CSOS Coordinator may request that the Certification Authority issue a new certificate for a new key pair, provided that the original certificate has not been revoked, the Subscriber name and attributes are unchanged, and the Subscriber is in good standing with the

Certification Authority, continuing to qualify as a DEA registrant, CSOS POA, or agent of a DEA registrant as defined in Section 1.3.3.

4.6.3 Processing Certificate Renewal Requests

After confirming that the information in the listing is accurate, the CSOS Coordinator contacts the CSOS RA and, upon authentication using a digital signature or their CSOS assigned security code, requests that new Subscriber certificates be issued to these Subscribers.

In the event that there is a discrepancy between the data in the database and the Subscriber's data, and provided that the request for a new CSOS certificate has been submitted prior to the DEA's Registration and Subscriber certificate expiration and that it is not the third renewal request:

- The renewing Subscriber's request is placed into an update queue for processing until the database is appropriately updated with the Subscriber's new DEA Registration information. This request is held for a maximum period of 90 days to allow the information to be updated in the database. This, then, does not require the resubmission of a complete application even in the event that the existing Subscriber certificate expires during this period.

- Subscribers and Coordinators receive an email notification that there is a Registration information discrepancy that needs to be resolved with DEA. A second notification is sent from the CSOS RA at 45 days.

- When the database update agrees with the applicant data, and the extract is received by the CSOS RA, the application is automatically removed from its hold status and a notice sent to the Subscriber and CSOS Coordinator with instructions on how to retrieve their new certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

The new public key is posted on the web site at http://www.deaecom.gov and notification of the renewal is provided through a digitally signed email from the CSOS RA to the CSOS Coordinators.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Acceptance of the renewal certificate occurs when the Subscriber uses the auth/ref codes distributed by the RA and their CSOS Coordinator to generate a certificate request and retrieve the certificate. The operation of the secure communications protocol between the Subscriber and the CSOS Certification Authority involves the mutual authentication of the two parties along with both the request and the response operations that constitute acceptance by the Subscriber of the resulting public key certificates. This process is also covered in Section 6.1.3 of this document.

4.6.6 Publication of the Renewal Certificate by the CA

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the CA issues;
- The CSOS Root CA’s self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS SCA certificate;
- The CSOS SCA certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

In order to mitigate the risk of aggregated information contributing to the possibility of the diversion of controlled substances, Subscriber certificates are not posted into the CSOS repository.

The following CSOS PKI information is published on the web site at http://www.deaecom.gov:

- A copy of the CSOS CP;
- A copy of the Subscriber Agreement;
- A copy of the Registrant Agreement;
- The CSOS DEA Registrant Certificate Application Checklist;
- Certificate application forms and instructions;
- Revocation request procedures;
- CSOS Certificate Profile and CSOS Certificate and CRL Profile
- The official list of PMA members;
- Contact details for this CPS and PKI;
- A copy of the CSOS Subscriber Manual.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the Certification Authority issues;
- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS Certification Authority certificate;
- The CSOS Certification Authority certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

4.7.1.1 Routine Re-key

4.7.1.1.1 CSOS Subscribers

The Subscriber, through the CSOS Coordinator, may request that the Certification Authority issue a new CSOS certificate containing a new serial number with a new key pair, provided that the original certificate has not been revoked and the Subscriber is in good standing with the Certification Authority, continuing to qualify as a DEA registrant or POA, as defined in Section 1.3.3. The CSOS System CP does not permit Subscriber certificate renewal (issuance of a new certificate for an existing key pair).

Re-key requests can be authenticated on the basis of the CSOS Coordinator's digital signature using the current private key for a total of two certificate requests beyond the initial request. Upon the third certificate request, Subscribers are required to establish identity using the initial registration process described in Sections 3.2.

The CSOS RA sends an automatically scheduled email notifying the Subscriber and the Subscriber's CSOS Coordinator 45 days prior to the expiration date of the Subscriber's CSOS certificate. The CSOS Coordinator receives two notifications at this time, the first notification contains a listing of Subscribers who have renewed twice previously and are now required to renew via the initial enrollment process, and the second notification contains a listing of CSOS Subscribers who are eligible for electronic renewal. After confirming that the information in the listing is accurate, the CSOS Coordinator contacts the CSOS RA and, upon authentication using a digital signature or their CSOS assigned security code, requests that new Subscriber certificates be issued to these Subscribers.

All re-key requests are adjudicated by the CSOS RA and checked to ensure 1) that the digital signature signing the request is validated against the one issued to the Subscriber or Coordinator, 2) checked to ensure that the certificate has not been revoked or suspended, and 3) checked against the database to ensure that the extension data is still valid. After adjudication, the request is entered into the RA database and sent to the CSOS Certification Authority as previously discussed.

DEA updates its database upon the receipt of information changes from the Registrant and from Registration renewal requests from the organization with whom the CSOS Coordinator is associated.

In the event that there is a discrepancy between the data in the database and the Subscriber's data, and provided that the request for a new CSOS certificate has been submitted prior to the DEA's Registration and Subscriber certificate expiration and that it is not the third renewal request:

- The renewing Subscriber's request is placed into an update queue for processing until the database is appropriately updated with the Subscriber's new DEA Registration information. This request is held for a maximum period of 90 days to allow the information to be updated in the database. This, then, does not require the resubmission of a complete application even in the event that the existing Subscriber certificate expires during this period.

- Subscribers and Coordinators receive an email notification that there is a Registration information discrepancy that needs to be resolved with DEA. A second notification is sent from the CSOS RA at 45 days.

- When the database update agrees with the applicant data, and the extract is received by the CSOS RA, the application is automatically removed from its hold status and a notice sent to the Subscriber and CSOS Coordinator with instructions on how to retrieve their new certificate.

Under normal circumstances, Subscribers and Coordinators not receiving their certificates within 10 business days from the receipt of CSOS RA notification of the submission package can contact the CSOS Help Desk to check status.

Requests for new certificates due to name changes (e.g. due to marriage) require proof of the name change be provided to the CSOS Coordinator, or other designated agent. The CSOS Coordinator serves as the certifier for the name change request submitted to the CSOS RA. Requests for new certificates due to a change of other information present in the Certificate extension data (reduction or addition of controlled substance ordering authorization, Registrant address or DEA Registration number) requires the Subscriber to establish identity using the initial registration process described in Sections 3.2.

4.7.1.1.2 CSOS CA Re-Key

The CSOS Root CA is a self-signed root. Both the CSOS Root CA and the CSOS SCAs generate and store their private keys using a FIPS 140 level three certified Hardware Security Module (HSM). Re-keying of the CSOS Root CA is completely internal to the CA and the generation of the CA's new keys takes place within the HSM. The CSOS Root CA key pair and certificate do not exceed the lifetimes stated in the CP. The Root and CSOS SCA Key Changeover Schedule is provided in the *CA Operations Guide*.

The CSOS SCA participates in an offline subordination process with the CSOS Root CA at the time of re-key. The subordination process (in which the CSOS Root CA signs the CSOS SCA's certificate) is done using removable media transferred between the two CAs. The entire process is contained within the domain of the two CAs. No outside entities are involved in the subordination process. As with the CSOS Root CA, the SCA's certificate and public and private key lifetimes do not exceed the durations set forth in the CSOS CP.

The new public key is posted on the web site at, http://www.deaecom.gov and notification of the re-key is provided through a digitally signed email from the CSOS RA to the CSOS Coordinators.

4.7.1.2 Re-key After Revocation

In the event of certificate revocation for reason of key compromise, cessation of operation, or as a result of negative action taken against the Registrant or Subscriber by DEA, issuance of a new certificate always requires that the Subscriber go through the initial registration process as described in Sections 3.2. Certificate revocation due to a technical malfunction that makes the private key invalid does not require renewal via initial enrollment provided that the previous adjudication was performed within 60 days of certificate revocation and the renewal request has been approved by the CSOS Coordinator.

4.7.2 Who May Request Certification of a New Public Key

Eligible Subscribers are those who hold a valid DEA registration as defined in 21CFR, Parts 1300-1399. All Subscriber applicants submit a completed application and documents substantiating identification in accordance with Section 3.2, entering into an initial agreement with the CA evidenced by accepting the applicable DEA Registrant or Subscriber Agreement at the CSOS web site, prior to certificate issuance. Complete application processing information is contained in the RA Section of the Operations Guide. Certificate application forms and instructions may be obtained from http://www.deaecom.gov. The applicant follows the procedures in the Subscriber Manual posted on the CSOS web site at, http://www.deaecom.gov, mailing completed applications to the CSOS Registration Authority at Drug Enforcement Administration, Sterling Park Technology Center/CSOS 8701 Morrissette Drive Springfield, VA 22152..

4.7.3 Processing Certificate Re-Keying Requests

Using the information provided with the application, the CSOS Coordinator will perform identity verification according to the requirements specified in the CP and this CPS. Subscriber applications are scanned by the RA and are entered into the RA database prior to adjudication. Based on subsequent verification against the database, the CSOS RA either approves or denies the application. The CSOS RA notifies the Registrant or the Registrant's CSOS Coordinator when the application is received via email. The CSOS RA notes all action taken on the certificate request in the CSOS RA database and retains the certificate request. Should the application be denied, the CSOS RA provides notification of the application denial to the applicant and the applicant's CSOS Coordinator.

The procedures developed and published on the CSOS web site are included in the CSOS Subscriber Manual and are as follows:

1. The Subscriber applicant accepts the CSOS Root CA and CSOS SCA certificates from a link provided on the CSOS web site in order to trust certificates issued by the CSOS Certification Authority.

2. The Subscriber applicant downloads the applicable CSOS enrollment application. Application forms and instructions are provided for the following CSOS Subscribers:

CSOS DEA Registrant Certificate Application –The following steps outline the DEA Registrant Certificate application process:

1. The applicant reads/agrees to the DEA Registrant Agreement, the CSOS Subscriber Agreement and the CSOS Privacy Policy.

2. The DEA Registrant completes the CSOS DEA Registrant Certificate Application and the CSOS Certificate Application Registration List Addendum(s) if applicable.

3. On the application, the DEA Registrant must designate a Principal Coordinator. The Principal Coordinator must be approved prior to the RA processing CSOS Power of Attorney or Alternate Coordinator certificate applications. These Coordinators serve as the organization’s Registration Authority (RA).

4. The DEA Registrant has the application and addendum(s) (if applicable) notarized.

5. The DEA Registrant attaches a photocopy(ies) of the DEA Registration Certificate(s) for the DEA Registration(s) identified, and photocopies of their identification documents and then mails the application package to the CSOS RA.

6. The CSOS RA notifies the DEA Registrant via e-mail upon receiving the application package.

7. The RA verifies the identity of the DEA Registrant and validates the DEA Registration(s) identified.

8. Upon approval, the CSOS Certification Authority staff sends the authorization and reference code(s) to the DEA Registrant. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the address provided by the CSOS Coordinator on the application in a tamper evident envelope.

9. After receiving the authorization and reference code(s), the DEA Registrant returns to the CSOS web site to retrieve his/her CSOS Certificate(s).

CSOS Principal Coordinator/Alternate Coordinator–A Principal Coordinator must be approved prior to the RA processing CSOS Power of Attorney or Alternate Coordinator certificate applications. The following steps outline the CSOS Principal Coordinator / Alternate Coordinator application process:

1. The DEA Registrant designates the CSOS Principal Coordinator/Alternate Coordinator applicant for the DEA Registration(s) identified.

2. The applicant reads/agrees to the DEA Registrant Agreement, the CSOS Subscriber Agreement and the CSOS Privacy Policy.

3. The applicant completes the application and has the application signed by the DEA Registrant.

4. The applicant has the application and addendum(s) (if applicable) notarized.

5. The applicant attaches a photocopy(ies) of the DEA Registration Certificate(s) and Power(s) of Attorney (if applicable) for the DEA Registration(s) identified and photocopies of their identification documents, and then mails the application package to the RA.

6. Once the RA receives the application package, the RA notifies the applicant via e-mail upon receiving the application package.

7. The RA verifies the identity and applicability of the applicant and validates the DEA Registration(s) identified.

8. Upon approval, the CSOS Certification Authority staff sends the authorization and reference code(s) to the applicant. The reference code(s) is sent via e-mail. The authorization code(s) is sent via postal mail to the Coordinator’s address provided on the application.

9. After receiving the authorization and reference code(s), the applicant returns to the CSOS web site to retrieve his/her CSOS Certificate(s).

CSOS Power of Attorney Certificate Application–A Principal Coordinator must be approved prior to the RA processing CSOS Power of Attorney or Alternate Coordinator certificate applications. The following steps outline the CSOS Power of Attorney Certificate application process:

1. The applicant reads and agrees to the CSOS Subscriber Agreement and the CSOS Privacy Policy.

2. The applicant completes the CSOS Power of Attorney Certificate Application.

3. The applicant attaches the CSOS Certificate Registration List Addendum(s) (if applicable) and the Power(s) of Attorney for the DEA Registration(s) identified and then forwards the application to either the Principal Coordinator or the Alternate Coordinator.

4. The Principal Coordinator/Alternate Coordinator adjudicates the Power of Attorney applicant as defined in the DEA Registrant Agreement.

5. The Principal Coordinator/Alternate Coordinator forwards the original application package to the RA.

6. Once the RA receives the application package, the RA notifies the applicant and Principal Coordinator/Alternate Coordinator via e-mail upon receiving the application package.

7. The RA validates the application and DEA Registration(s) identified.

8. Upon approval, the RA sends the reference code(s) to the applicant via e-mail. The authorization code(s) is sent by the Principal Coordinator/Alternate Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code(s) to the applicant.

9. After receiving the authorization and reference code(s), the applicant returns to the CSOS web site to retrieve his/her CSOS Certificate(s).

Bulk Enrollment Applications–In order to participate in CSOS Bulk Enrollment, the applicant must be applying for more than 50 CSOS Certificates and the organization must currently participate in the DEA Chain Renewal program for DEA Registrations. Bulk Enrollment has been established to accommodate organizations that need to obtain a large volume of CSOS Certificates associated with a single applicant. Each applicant, DEA Registrant, Principal Coordinator, Alternate Coordinator, and Power of Attorney, will complete his/her application as previously specified with the exception of how DEA Registration and Power of Attorney documentation is submitted. DEA Registration and Power of Attorney documentation will be submitted as described below. The CSOS RA works with the organization’s primary point of contact for bulk enrollment to ensure the DEA Registration and Power of Attorney documentation is submitted correctly.

1. For the DEA Registrations for which the applicant is applying, the organization will provide the following:

   - A printed list of the DEA Registrations (including all pertinent information such as DEA Registration Number, name, address and current expiration date) listed in order by DEA Registration Number.

   - A CD with the DEA Registration Numbers in alphanumeric order only, saved as an ASCII text file.

   This information is mailed to: Drug Enforcement Administration, Sterling Park Technology Center/CSOS 8701 Morrissette Drive Springfield, VA 22152.

2. For Power of Attorney applicants, the organization will provide a single Power of Attorney listing all of the DEA Registration Numbers for which the applicant is applying.

3. The Organization provides a contact point including Corporate Name, address, telephone number, fax number, individual contact and alternate contact for the bulk enrollment process.

4. Upon receipt of the package, the CSOS RA validates the application and DEA Registration(s) identified.

5. Upon approval, the CSOS Certification Authority creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrants identified. The reference code file is sent to the applicant via e-mail. The authorization code file is sent on compact disk (CD) to the address provided by the Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code(s) to the applicant.

6. After receiving the authorization and reference code(s), the applicant returns to the CSOS web site to retrieve his/her CSOS certificate(s).

4.7.4 Notification of New Certificate Issuance to Subscriber

4.7.4.1 Subscriber Certificate Issuance

Subscriber information is verified against a daily extract of DEA Registrant information contained in DEA’s database. DEA’s database extract is delivered electronically to the CSOS RA through the closed DEA Firebird communications system that prevents external tampering with the file. The file is programmatically retrieved and made available to the CSOS RA database for adjudication purposes.

Upon receipt of the application package from the CSOS Coordinator, the package is validated by the CSOS RA for completeness and then scanned into the CSOS RA database. The fields within the scanned application are automatically parsed and processed against DEA’s database extract to validate DEA authorization, business activity and drug schedules that become a part of the certificate extensions. Errors detected at this point are reported to the CSOS RA, who, in turn, notifies the applicant and their CSOS Coordinator via email. It is the CSOS Coordinator’s responsibility to contact DEA to resolve errors in the database.

The unique identification number of the identifications presented is recorded on the DEA Registrant and Coordinator Applications by the Notary Public and the photocopy of the identification documents are filed with the application and are also contained with the image of the application created during document scanning. Applications and photocopies of identification documents are stored in locked file cabinets with limited access. Access is limited to only individuals with a need to know.

The electronic workflow application maintains custody of the workflow package until completion of the adjudication

Upon successful adjudication, the CSOS RA submits applicant information to the CSOS Certification Authority instructing the CA to issue the certificate to the applicant. The CSOS Certification Authority provides the individual with one-time use reference and authorization codes. The CSOS Certification Authority sends the reference code to the applicant via e-mail. The authorization code is distributed to the Principal Coordinator/Alternate Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code to the applicant. The Subscriber must possess both pieces of information in order to authenticate themselves for certificate use at their initial login. Email notifications are distributed to the CSOS Coordinators and Subscribers. Subscribers are required to use these within 60 calendar days and must not divulge the codes prior to use.

For bulk enrollments, The CSOS RA adjudicates the applicant as previously discussed, and associates the applicant with the Principal Coordinator for the DEA Registrations identified in the RA database. Upon approval, the CSOS Certification Authority creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrations identified. The reference code file is sent to the applicant via e-mail. The authorization code file is sent on a compact disk (CD) to the applicant via the applicant's designated Coordinate via postal mail.

The Subscriber is mailed a URL and user login and password to an SSL-secured CSOS web site that then launches the certificate retrieval process at the Subscriber's client. Entering the reference and authorization codes, the applicant's software generates the key pair in the applicant's system while accessing the SSL-secured CSOS web site using the access code and password. The public key is then automatically submitted in a certificate request to the CSOS Certification Authority.

The CSOS Certification Authority software automatically verifies the certificate request, signs the signing public key certificate, and stores a copy of the certificate in the CSOS Certification Authority database. The CSOS Certification Authority then provides a copy of the signing public key certificate to the client electronically through the program during the session. Next, the CSOS Certification Authority writes the public certificate into the CSOS repository. The issuance of a certificate by the CSOS Certification Authority indicates the end of the certificate issuance process. Subscriber acceptance of the certificate is covered in the following section.

The DEA-customized certificate specification, described in the CSOS *System Certificate and CRL Profile Guide*, contains a set of pre-defined values that the CA software uses to validate certification information prior to processing a certificate request. These values include the controlled substance schedules that the Subscriber can order, business activity and DEA Registrant location. CA software is used to automatically validate that the certificate fields, including public key, and extensions are properly and accurately populated in the Subscriber certificates.

The RA workflow and certificate issuance processes are monitored to ensure that these processes continue to compare favorably with baseline performance metrics.

4.7.4.2 CSOS Certification Authority Certificate Issuance

The CSOS SCA received its initial subordination certificate signed by the CSOS Root CA during a Key Generation ceremony audited by KPMG.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Acceptance of the certificate occurs when the Subscriber uses the codes distributed by the RA and their CSOS Coordinator to generate a certificate request and retrieve the certificate. The operation of the secure communications protocol between the Subscriber and the CSOS Certification Authority involves the mutual authentication of the two parties along with both the request and the response operations that constitute acceptance by the Subscriber of the resulting public key certificates. This process is also covered in Section 6.1.3 of this document.

4.7.6 Publication of the Re-Keyed Certificate by the Certification Authority

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the Certification Authority issues;

- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS SCA certificates;

- The CSOS SCA certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

In order to mitigate the risk of aggregated information contributing to the possibility of the diversion of controlled substances, Subscriber certificates are not posted into the CSOS repository.

The following CSOS PKI information is published on the web site at http://www.deaecom.gov:

- A copy of the CSOS CP;

- A copy of the Subscriber Agreement;

- A copy of the Registrant Agreement;

- The CSOS DEA Registrant Certificate Application Checklist;

- Certificate application forms and instructions;

- Revocation request procedures;

- CSOS Certificate Profile and CSOS Certificate and CRL Profile
- The official list of PMA members;
- Contact details for this CPS and PKI;
- A copy of the CSOS Subscriber Manual.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the Certification Authority issues;
- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS SCA certificate;

The CSOS SCA certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS SCA certificate.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Updating a certificate means creating a new certificate that has a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. The CSOS Certification Authority updates Subscriber certificates whose characteristics have changed due to changes in name, affiliation, or prescribing or order authority, as indicated in the daily extracts received from DEA. The old certificate is immediately revoked.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) in order for an updated certificate with the new name to be issued. The CSOS Coordinator will serve as the certifier for the name change request submitted to the CSOS RA. All changes to affiliation or authorized schedules require crosschecking applicant information with relevant information extracted from the database that is verified by DEA daily through the review of a printed list of Registrant changes.

4.8.2 Who May Request Certificate Modification

The DEA CSOS Operational Authority or the FPKI Operational Authority may request certificate modification for currently cross-certified CAs.

4.8.3 Processing Certificate Modification Requests

The DEA CSOS Operational Authority performs certificate modification at the direction of the FPKI PA. The DEA CSOS Operational Authority may also perform certificate modification at the request of the FPKI Operational Authority. Changes may be made for the following reasons:

- Modification of Strong Identification and Authorization (SIA) extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

The validity period associated with the new certificate must not extend beyond the period of the Memorandum of Agreement (MOA).

Proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

4.8.4.1 Subscriber Certificate Issuance

Subscriber information is verified against a daily extract of DEA Registrant information contained in DEA’s database. DEA’s database extract is delivered electronically to the CSOS RA through the closed DEA Firebird communications system that prevents external tampering with the file. The file is programmatically retrieved and made available to the CSOS RA database for adjudication purposes.

Upon receipt of the application package from the CSOS Coordinator, the package is validated by the CSOS RA for completeness and then scanned into the CSOS RA database. The fields within the scanned application are automatically parsed and processed against DEA’s database extract to validate DEA authorization, business activity and drug schedules that become a part of the certificate extensions. Errors detected at this point are reported to the CSOS RA, who, in turn, notifies the applicant and their CSOS Coordinator via email. It is the CSOS Coordinator’s responsibility to contact DEA to resolve errors in the database.

The electronic workflow application maintains custody of the workflow package until completion of the adjudication

Upon successful adjudication, the CSOS RA submits applicant information to the CSOS Certification Authority, instructing the Certification Authority to issue the certificate to the applicant. The Certification Authority provides the individual with one-time use reference and authorization codes. The Certification Authority sends the reference code to the applicant via e-mail. The authorization code is distributed to the Principal Coordinator/Alternate Coordinator via postal mail. The Principal Coordinator/Alternate Coordinator must forward the sealed authorization code to the applicant. The Subscriber must possess both pieces of information in order to authenticate themselves for certificate use at their initial login. Email notifications are distributed to the CSOS Coordinators and Subscribers. Subscribers are required to use these within 60 calendar days and must not divulge the codes prior to use.

For bulk enrollments, The CSOS RA adjudicates the applicant as previously discussed, and associates the applicant with the Principal Coordinator for the DEA Registrations identified in the RA database. Upon approval, the CSOS Certification Authority creates two ASCII files, one containing the reference codes and one containing the authorization codes for the DEA Registrations identified. The reference code file is sent to the applicant via e-mail. The authorization code file is sent on a compact disk (CD) to the applicant via the applicant's designated Coordinate via postal mail.

The Subscriber is mailed a URL and user login and password to an SSL-secured CSOS web site that then launches the certificate retrieval process at the Subscriber's client. Entering the reference and authorization codes, the applicant's software generates the key pair in the applicant's system while accessing the SSL-secured CSOS web site using the access code and password. The public key is then automatically submitted in a certificate request to the CSOS Certification Authority.

The CSOS Certification Authority software automatically verifies the certificate request, signs the signing public key certificate, and stores a copy of the certificate in the CSOS Certification Authority database. The CSOS Certification Authority then provides a copy of the signing public key certificate to the client electronically through the program during the session. Next, the CSOS SCA writes the public certificate into the CSOS repository. The issuance of a certificate by the CSOS Certification Authority indicates the end of the certificate issuance process. Subscriber acceptance of the certificate is covered in the following section.

The RA workflow and certificate issuance processes are monitored to ensure that these processes continue to compare favorably with baseline performance metrics.

4.8.4.2 CSOS Certification Authority Certificate Issuance

The CSOS SCA received its initial subordination certificate signed by the CSOS Root CA during a Key Generation ceremony audited by KPMG.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

Acceptance of the certificate occurs when the Subscriber uses the codes distributed by the RA and their CSOS Coordinator to generate a certificate request and retrieve the certificate. The operation of the secure communications protocol between the Subscriber and the CSOS Certification Authority involves the mutual authentication of the two parties along with both the request and the response operations that constitute acceptance by the Subscriber of the resulting public key certificates. This process is also covered in Section 6.1.3 of this document.

4.8.6 Publication of the Modified Certificate by the CA

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the CA issues;
- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS SCA certificate;
- The CSOS SCA certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

In order to mitigate the risk of aggregated information contributing to the possibility of the diversion of controlled substances, Subscriber certificates are not posted into the CSOS repository.

The following CSOS PKI information is published on the web site at http://www.deaecom.gov:

- A copy of the CSOS System CP;
- A copy of the Subscriber Agreement;
- A copy of the Registrant Agreement;
- The CSOS DEA Registrant Certificate Application Checklist;
- Certificate application forms and instructions;
- Revocation request procedures;
- CSOS Certificate Profile and CSOS Certificate and CRL Profile
- The official list of PMA members;
- Contact details for this CPS and PKI;
- A copy of the CSOS Subscriber Manual.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

The following information is published in the CSOS repository:

- Certificate revocation information for all CSOS certificates that the CA issues;
- The CSOS Root CA's self-signed CA certificate containing the public key, which is used to verify the authenticity of the CSOS SCA certificate;

The CSOS SCA certificate signed by the CSOS Root CA containing the public key, which is used to verify the authenticity of a CSOS certificate.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Subscriber Certificates

A certificate is revoked in accordance with Section 4.9.3 when the binding between the Subscriber and the Subscriber's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Change of identifying information or affiliation components of any names in the certificate (i.e. Subscriber name change);
- Privilege attributes asserted in the Subscriber's certificate are reduced (i.e. controlled substance ordering schedules reduced);
- Compromise or suspected compromise of private keys, private key storage media and/or user password;
- Forgotten password or the Subscriber's private key cannot be accessed for any reason;
- The Subscriber, the DEA Registrant under whose Registration a certificate holder obtained a certificate, or CSOS Coordinator requests that the affiliated Subscriber certificate be revoked;
- It can be demonstrated that the Subscriber has violated the stipulations of the Subscriber Agreement;
- Corporate mergers or takeover;
- DEA posts notice that certificate holder's DEA Registration has been revoked, suspended or restricted, that the Registration information has changed, or that the Registration has been terminated;
- Cessation of CA operations or suspected key compromise of the CSOS Certification Authority or the CSOS Root CA following PMA approval.

Certificates with the following changes to certificate extension data, identified from the updates, are automatically scheduled for revocation on day 60 from the receipt of the updated information.

- DEA Registration name change (i.e. company name);
- Changes to DEA Registration mailing addresses (not physical addresses); and
- Additions to the controlled substance schedules the Registration is authorized to order.

During this 60-day period, the certificate status remains unaffected, allowing the Subscriber to use the certificate until either a new certificate is requested and received or the 60-day period expires and the certificate is revoked.

Certificate revocations resulting from Subscriber name changes (i.e. upon marriage) are processed upon authentication of the new information. Authentication occurs when the Subscriber provides a copy of the marriage license, driver's license, or Social Security Card to the Help Desk confirming the name change. On authentication, the existing certificate is processed for revocation within 18 hours and a new certificate with this updated data is issued. If authentication of the name change is not received within 10 business days, the certificate is processed for revocation within 18 hours without the issuance of a new certificate.

Upon revocation of the Subscriber's certificate, the Subscriber and the CSOS Coordinator are notified via e-mail.

Revoked certificates continue to be included on all new publications of the certificate status information for a period in excess of 60 days beyond certificate expiration. CSOS Relying Parties are permitted under 21CFR Part 1305.09 to fill received orders for 60 days after the execution of the order by the purchaser, provided the order was valid at the time of signing. Continuing to maintain revocation information on the CRL until 60 days beyond expiration ensures that a revoked certificate is not validated during this period. Complete revocation processing information is contained in the *Revocation Process* document.

4.9.1.2 CSOS SCA Certificate

The CSOS SCA certificate can be revoked under the following circumstances:

- When the PMA requests that the certificate be revoked in the event that the PMA determines that the CSOS SCA does not meet policy requirements or that the system is no longer in the best interest of the federal government.
- When the CSOS System PMA determines that an incident has occurred that may impact the integrity of the certificates issued by the CSOS System.
- In the event of suspected key compromise of the CSOS Root CA or CSOS SCA.

In the event of key compromise or under direction of the PMA, the CSOS SCA has the ability to support the secure and authenticated revocation of one or more certificates of one or more Subscribers and provides a means of rapid communication of such revocation through the issuance of daily CRLs (or, if necessary, more frequent CRLs). The SCA's system and processes provide the capability to revoke the set of all certificates issued by the SCA that have been signed with the CSOS SCA's private signing key.

The *CSOS System Key Compromise Plan* details the circumstances and procedures to be implemented by the PMA and OMA when CA key compromise is suspected or other incident occurs that may adversely impact the integrity of the certificates issued by the CA.

The CSOS Certification Authority is not responsible for Subscriber token (hardware or software) maintenance or destruction when a Subscriber ceases its relationship with an organization that sponsored the certificate. Subscribers and organizations have been directed through the

Certificate Policy and Federal Regulations to require the Subscriber to surrender to that organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. They must then zeroize or otherwise destroy promptly upon surrender, protecting the token from malicious use between surrender and zeroization or destruction. If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then the CSOS Coordinator must immediately request that all Subscriber certificates associated with the unretrieved tokens be immediately revoked.

4.9.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- Subscriber
- Subscriber's Sponsoring Organization
- Subscriber's CSOS Coordinator
- CSOS PMA

If an organization's DEA Registration information has changed or the DEA Registration is revoked, every certificate issued for that DEA Registration is revoked.

4.9.3 Procedure for Revocation Request

Subscriber certificate revocation procedures are detailed in the *CSOS Certification Authority Operations Guide* document and are summarized in this section. Revocation requests can be made by digitally signed email to csosrevocation@deaecom.gov**.** Revocation requests due to key compromise may be submitted by telephone to 1-877-DEA-ECOM (332-3266). Revocation requests may also be submitted either verbally or in writing by the Help Desk or by DEA upon observation of inappropriate key management practices. The CSOS RA and its associated Help Desk has been designated by DEA as having the authority to request revocation of the Subscriber's certificate in the event that there is evidence or suspicion of key compromise.

Revocation requests must be authenticated as follows:

Data Collected for Revocation Authentication								
			Cases					
		Method	**Single Cert**		**DEA Reg.**		**Subscriber**	
Field	**Description**	**Phone** **E-mail**	**P**	**E**	**P**	**E**	**P**	**E**
Requestor's CSOS Account Number	The CSOS account number of the individual making the request.	Coord. Reg.	✓		✓		✓	
		Sub.	✓		na	na	✓	
Requestor's Security Code	The security code provided to the RA by the applicant at the time of enrollment. The RA maintains this information in its database for authentication purposes.	Coord. Reg.	✓		✓		✓	
		Sub.	✓		na	na	✓	
Last 4 digits of Requestor's SSN	The last four digits of the individual's social security number. The Social Security Number	Coord. Reg.	✓		✓		✓	

	was provided at the time of enrollment. The RA maintains this information for authentication purposes.	Sub.	✓		na	na	✓	
Revocation Reason	The reason the certificate, registration, or subscriber needs to be revoked.	Coord. Reg.	✓	✓	✓	✓	✓	✓
		Sub.	✓	✓	na	na	✓	✓
** Certificate Serial Number	Serial Number of the Certificate to be Revoked.	Coord. Reg.	✓	✓*			✓	✓
		Sub	✓	✓*	na	na	✓	
** DEA Registration Number	The DEA Number of the Registration identified in the certificate to be revoked or for which all issued certificates should be revoked.	Coord. Reg.	✓	✓*	✓	✓*	✓	
		Sub	✓	✓*	na	na	✓	
** Account number of individual to be revoked	The account number of the individual for which a single certificate or for which all certificates issued to an individual is revoked.	Coord. Reg.	✓	✓*	✓	✓*	✓	
		Sub.	✓	✓*	na	na	✓	
Revocation Case	The type of revocation being requested; single certificate, DEA Registration or subscriber.	Recorded for all submission methods.						

* Only necessary if certificate/registration to be revoked is not the same as the certificate used to sign the e-mail

** Only one of the three, Cert. Serial Number, DEA Registration Number or the Account number of the individual to be revoked is necessary to identify certificates that are revoked in single certificate and individual revocation cases.

The columns labeled P and E indicate either a Telephone (P) or e-mail (E) mail revocation request submission

Exhibit 4–1. Data Collected for Revocation Authentication

All revocation requests include the following information:

- Subscriber's full name;
- Subscriber's work e-mail address (if applicable);
- Date of revocation request;
- Reason for revocation;
- Date of compromise;
- Digital signature of one of the parties identified in Section 4.9.2.

Certificate(s) revocation requests are given priority attention over other certificate actions. Authenticated revocation requests are entered into the RA database and a scripted request is sent through the RA workflow system to be received and processed by the CA Operators such that updated certificate status appears on a CRL within 6 hours of receipt of the key compromise revocation request.

Upon authentication, the RA authorizes the Certification Authority to execute the revocation request. In the event of suspected compromise, the Subscriber, or other authorized person, can request revocation via a telephone call to the RA. The RA authenticates telephone requests by requesting that the CSOS Coordinator provide the last four digits of his SSN and his Security ID that was provided to the CSOS RA at the time of the Coordinator's enrollment. The CSOS Help Desk Operations Guide provides detailed information on processing revocation requests. Certificate revocation is authorized upon receipt of the digitally signed request, or on authenticated phone call. Exhibit 4–2 diagrams the certificate revocation request and authentication flow.

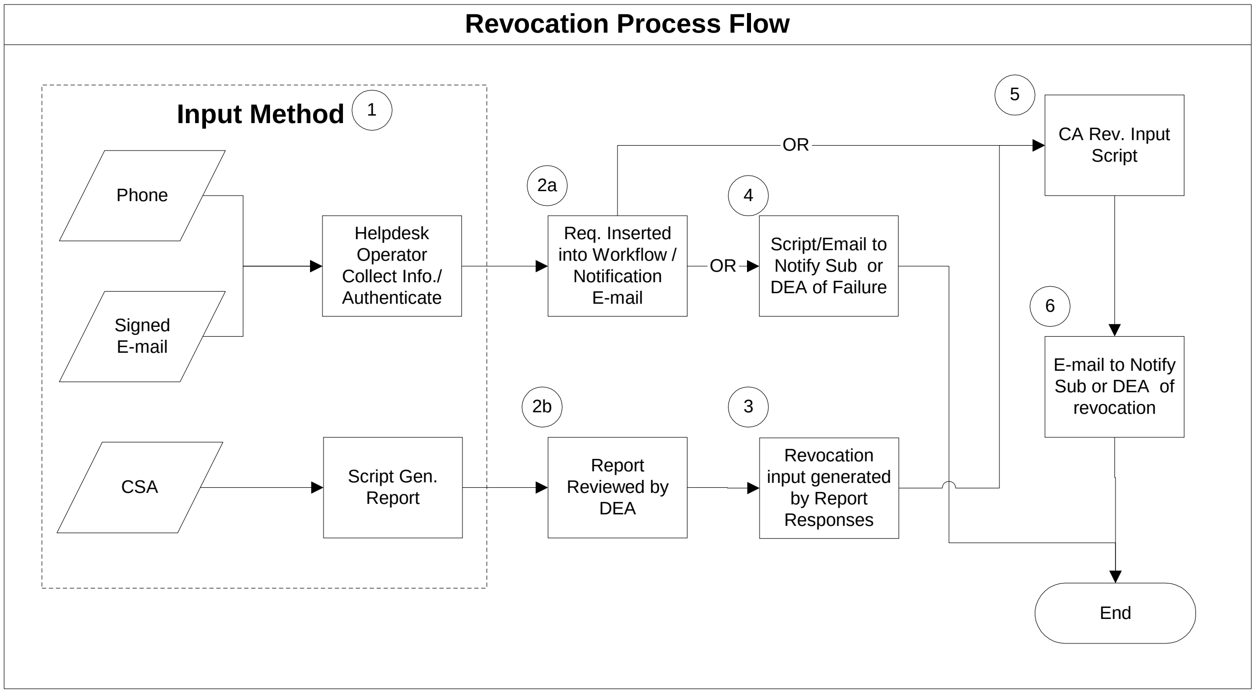

Revocation Process Flow
Input Method
1
Phone
Signed E-mail
CSA
Helpdesk Operator Collect Info./ Authenticate
Script Gen. Report
2a
Req. Inserted into Workflow / Notification E-mail
2b
Report Reviewed by DEA
OR
4
Script/Email to Notify Sub or DEA of Failure
3
Revocation input generated by Report Responses
OR
5
CA Rev. Input Script
6
E-mail to Notify Sub or DEA of revocation
End

Exhibit 4–2. Revocation Process Flow

In all cases, a record is to be retained in the database of the request and approval of the revocation that includes a date stamp on the action.

Revocation reason codes have been developed specifically to meet DEA's business cases. The revocation reason is conveyed by the use of an optional revocation flag that is associated with every certificate placed on the CRL. The following table maps DEA's certificate revocation codes to specific business cases and reasons necessitating revocation:

Reasons for Revocation		
Revocation Reason	**Generated By**	**Certificate Reason Code**
Key Compromise	Subscriber	Key Compromise
Subscriber Name Change	Coordinator or Registrant	Affiliation Change
Subscriber E-mail Address Change	Subscriber	Affiliation Change
DEA Registrant Name Change	CSA	Affiliation Change
DEA Registrant Address Change	CSA, Coordinator or Registrant	Affiliation Change
Schedule Addition / Reduction	CSA	Affiliation Change

Reasons for Revocation		
Revocation Reason	**Generated By**	**Certificate Reason Code**
Change of Business Activity	CSA	Affiliation Change
Registration Surrendered for Cause	CSA	Cessation of Operation
Registration Revoked	CSA	Cessation of Operation
Registration Out of Business	CSA	Cessation of Operation
Registration Suspended	CSA	Certificate Hold
Registration Restricted for Cause/CA Administrative Action	CSA	Superseded
Lost/Forgotten Password	Subscriber	Superseded
Order to show cause	CSA	Certificate Hold

Exhibit 4–3. Revocation Reason Codes

4.9.4 Revocation Request Grace Period

When a key compromise is detected, suspected, or when discovered risk is determined to warrant revocation, all certificate holders/subscribers are required to immediately notify their CSOS Coordinator and CSOS RA so that the certificate can be revoked.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CSOS Certification Authority revokes certificates as quickly as practicable upon receipt of a proper revocation request as described in this section. Revocation requests are processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance are processed before the following CRL is published. Revocation processing times are listed in Section 4.9.7 below.

4.9.6 Revocation Checking Requirements for Relying Parties

The CSOS Certification Authority repository currently supports LDAP-accessible distributed, or partitioned, CRLs. The issuing CA's private key signs all CRLs.

CRLs may be cached and used until they expire unless otherwise notified by the PMA through the DEA CSOS web site at, http://www.deaecom.gov or email or phone call from the CSOS Help Desk to the CSOS Coordinators. CSOS Coordinators must perform a callback to the Help Desk to authenticate the message. In the event that an emergency or other incident prevents the CSOS Certification Authority from publishing a CRL, relying parties may rely on the cached CRL until another CRL is issued. The CSOS Certification Authority Help Desk provides email notification to CSOS Coordinators when CRL services are restored after interruption.

The Relying Party's application software performs CRL checking of certificates at the time the certificate is validated, checking to ensure 1) the certificate was valid at the time of signing, 2) the Subscriber’s certificate was signed by the CSOS SCA, and 3) the CSOS SCA’s certificate is not present on the CSOS System’s Root CA’s ARL.

CRL checking requirements associated with Relying Party acceptance of CSOS Subscriber certificates is specified in Title 21CFR, Parts 1300-1399.

4.9.6.1 Checking Requirements for Other Forms of Revocation

In the event that the CSOS System Root CA or CSOS Certification Authority is unable to publish its revocation list as described in this CPS, the Help Desk provides either a telephone call or digitally-signed email to all CSOS Coordinators with information on an alternative location of the CRL or DEA-authorized procedures for revocation checking. This notification is also posted to the DEA web site at, http://www.deaecom.gov, accessible to all Relying Parties.

4.9.7 CRL Issuance Frequency

The CSOS Certification Authority issues CRLs within a period not to exceed 24-hours/7 days a week, even if there are no changes to be made**.** Changes to certificate status information are posted as follows:

Revocation Reason	**CRL will be issued:**
Revocation due to suspected key compromise, loss of Subscriber’s private key storage media, lost or forgotten password.	6 hours after receiving an authenticated revocation request.
Revocation for reasons other than key compromise or loss.	At least once each day, or within 24 hours of the receipt of an authenticated revocation request.

Exhibit 4–4. CRL Issuance Frequency

New CSOS CRLs are immediately published in the CSOS Certification Authority repository, overwriting the previous CRL. This update reflects the removal of any superseded information. A script copies each CRL written to the repository to a separate location so that all CRLs are archived. Additionally, CRLs (those both in the repository and those written to a separate location) are backed up nightly.

In the event of the CSOS SCA certificate revocation, the CSOS Root CA posts the revoked SCA certificate to the ARL in the CSOS Root CA repository. CSOS RA and Help Desk personnel notifies CSOS Coordinators of the CSOS SCA revocation via a telephone call.

4.9.8 Maximum Latency for CRLs

In the event of key compromise, CRLs/ARLs containing the newly revoked certificate, information is published within 6 hours of authenticated notification. In the event of CA certificate revocation, the CSOS System notifies all other CAs via a digitally signed email and issues an emergency ARL. A CA certificate that is revoked remains on the ARL until the certificate expires.

Superseded certificate status information is removed from the repository system upon posting of the latest certificate status information, with the latest CRL overwriting the expired CRL.

4.9.9 On-line Revocation/Status Checking Availability

The CSOS Certification Authority does not support the Online Certificate Status Checking Protocol (OCSP) capability for its CRLs at this time.

4.9.10 On-line Revocation Checking Requirements

The CSOS Certification Authority does not support any forms of Online Revocation Checking at this time.

4.9.11 Other Forms of Revocation Advertisements Available

The CSOS Certification Authority does not support any other forms of revocation advertisements. Other forms of revocation advertisements are reviewed for applicability on a periodic basis or as requested by the CSOS Registrant community.

4.9.12 Special Requirements Re/Key Compromise

In the event of key compromise or under direction of the PMA, the CSOS Certification Authority has the ability to support the secure and authenticated revocation of one or more certificates of one or more Subscribers and provides a means of rapid communication of such revocation through the issuance of daily CRLs (or, if necessary, more frequent CRLs). The SCA's system and processes provide the capability to revoke the set of all certificates issued by the CSOS SCA that have been signed with the CSOS SCA private signing key.

The *CSOS System Key Compromise Plan* details the circumstances and procedures to be implemented by the PMA and OMA when CA key compromise is suspected or other incident occurs that may adversely impact the integrity of the certificates issued by the CA.

4.9.13 Circumstances for Suspension

At their discretion, the PMA may choose to request Subscriber certificate suspension, rather than revoke the Subscriber certificate. Examples of circumstances under which the PMA may choose suspension include:

- As a result of a discrepancy reported in compliance audit of a subordinate or cross-certified Root CA, the PMA may choose to suspend rather than revoke the CA's certificate until the discrepancy has been corrected.

- Subscriber certificates may be suspended if the status of the Subscriber has changed and the PMA deems it appropriate to suspend rather than revoke the Subscriber certificate.

- Under certain circumstances, such as when an investigation is proceeding against a Subscriber or Registrant, DEA may choose to suspend, rather than revoke, one or more digital certificates associated with the investigation.

4.9.14 Who Can Request Suspension

Only the PMA, CSOS RA, or other DEA authorized entity have the authority to issue a suspension request. Suspension requests received from Subscribers, Registrants or Coordinators are not valid and are not processed. Suspension-related requests received from the PMA are authenticated through a callback to a phone number of record for the identity making the request or by a digitally signed email request.

4.9.15 Procedure for Suspension Request

Suspension requests received from the PMA are processed. Revocation of suspended certificates are processed as discussed in Section 4.9.3, changing the CRLReason code to the appropriate revocation code as previously discussed. The CSOS RA notifies the Subscriber or Subscriber’s CSOS Coordinator via email that the suspended certificate has been revoked.

4.9.16 Limits on Suspension Period

Certificates remain in a suspended status until the PMA concludes their investigation and warrants either revocation or removal from the CRL, as discussed above. Suspended certificates that expire remain on the CRL for a period of at least 60 days beyond certificate expiration.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

New CSOS CRLs are immediately published in the CSOS Certification Authority repository, overwriting the previous CRL. This update reflects the removal of any superseded information. A script copies each CRL written to the repository to a separate location so that all CRLs are archived. Additionally, CRLs (those both in the repository and those written to a separate location) are backed up nightly.

In the event of the CSOS SCA certificate revocation, the CSOS Root CA posts the revoked CSOS SCA certificate to the ARL in the CSOS Root CA repository. CSOS RA and Help Desk personnel notify CSOS Coordinators of the CSOS SCA revocation via a telephone call.

4.10.2 Service Availability

The CSOS Certification Authority issues Certificate Revocation Lists (CRLs) in accordance with the CRL profile provided in the *CSOS System Certificate and CRL Profile* document provided on the CSOS web site. The contents of the CRLs are checked prior to posting to the CSOS Repository to ensure information accuracy using mechanisms provided by the CA software. Repository performance is managed using automated reporting tools that alert a System Administrator in the event that the repository fails. Repository performance metrics are monitored to ensure reliability.

4.10.3 Operational Features

The CSOS Certification Authority publishes the following information to an online repository or a web site (http://www.deaecom.gov) that is available to Subscribers and relying parties:

- A CRL;
- The CA's certificate;
- A copy of this CP, including any waivers granted to the CA by the PMA.

The Root CA's certificate and ARLs associated with SCAs are made publicly available in the repository.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CSOS Root CA's and CSOS SCA's private keys are not escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

Section 5 – Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The location and construction of the facility housing CA equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, combined with other physical security protection mechanisms such as guards and intrusion sensors, provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

5.1.2.1 Physical Access Controls

Access into the CA Server cabinet in the computer room requires 2-person access. The computer room implements two-factor factor authentication to enter. Unescorted access to the computer room is limited to authorized personnel. Unescorted access to the CA cabinet is limited to the system administrators and CA operators only and must comply with the two person required rule. RA staff members are escorted by individuals who are allowed unescorted access. Security officers provide oversight to operations providing an additional level of security within the space.

Unescorted access into all spaces requires a DEA/DOJ clearance. All visitor, vendor and employee access is approved by the CSOS Security Officer prior to entry into the facility. External facility management/maintenance personnel require escorted access at all times.

Two-factor authentication is required by authorized employees to gain access to the CA space. Authorized employees gain access to the CA space using their DEA issued badge with two-factor authentication mentioned above. There is a visitor’s log maintained at the facility entrance that is used by all approved visitors. The Security Officer performs daily reviews of the visitor’s log.

In the unforeseen event that all personnel vacate the facility for an extended period of time, the Security Officer on duty performs a security check of the facility, ensuring that only essential equipment (e.g. the repository, load-balancers, firewalls, IDS, etc.) is powered-on. A log is maintained in which personnel are required to initial at each check, initialing a sign-out sheet as the last person leaves the facility. This sign-out sheet indicates the date and time and contains an assertion that “all necessary physical protection mechanisms are in place and activated.” These protection mechanisms include the cryptographic modules, the security containers, the physical security controls, and the environmental controls. Upon returning to the facility, the Security Officer checks the automatic card-key logs upon returning to ensure that unauthorized entry did not occur during that period.

5.1.3 Power and Air Conditioning

The temperature in the CA room is maintained at 69 +/-2 degrees and CA equipment and is monitored regularly. There are two air-conditioning systems, each capable of supporting the temperature requirements alone. The uninterruptible power supply system ensures that the temperature is appropriately maintained in the facility in the event of a power outage.

5.1.4 Water Exposures

CA equipment is installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Water exposure from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

The fire resistance of the primary location is high and the fire protection and suppression facilities available to the building are rated to a level where the risk of substantial destruction as a result of fire of the equipment located in the building is low.

5.1.6 Media Storage

Removable cryptographic modules are inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment are placed in secure containers. Activation data are either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and are not stored with the cryptographic module.

5.1.7 Waste Disposal

Certification Authority storage media and devices containing storage media are inspected to ascertain if they contain sensitive data prior to disposal or reuse. Items found to contain sensitive information are physically destroyed or securely overwritten at least three times, using a disk formatting utility designed especially for the permanent removal of data from media, prior to reuse. Items whose contents cannot be determined are physically destroyed. Storage media used by the Certification Authority are protected from environmental threats of temperature, humidity and magnetism.

5.1.8 Off-site Backup

Full system backups, sufficient to recover from system failure, are made on a periodic basis, described in this CPS. Backups are performed and stored off-site not less than once per week. At least one full backup copy is stored at an offsite location (separate from the CA equipment). Only the latest full backup is retained. The backup is stored at a site with physical and procedural controls commensurate to that of the CA.

Media that contain audit, archive, or backup information are duplicated and stored in a location separate from the CAs.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is be one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. To ensure that one person acting alone cannot circumvent safeguards, CA responsibilities and authority are divided between multiple roles and individuals.

The people selected to fill these roles are extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles are successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes functions among more than one person, so that any malicious activity requires collusion. The primary trusted roles defined in this policy are directly mapped to the FBCA and Certificate Issuing and Management (CIMC) Protection Profile developed by NIST as follows: CA Operator (maps to the Administrator role), RA Operator (maps to the Officer role), Security Officer (maps to the Auditor role), and System Administrator (maps to the Operator role). While DEA-approved CAs have different name designations for these roles, it is expected that the separation and distribution of functions are consistent with this policy and are employed at all CA and RA locations.

Shareholders

The Shareholder role serves to ensure multi-person control of sensitive CA information by safeguarding hardware that is essential to the creation of the CA keys. As such, Shareholders do not hold an account on any of the systems. Shareholders are required to participate in any task that requires authentication to or activation of the CA’s private signing key.

CA Operators (Administrator)

The CA Operator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

CA Operators have no part in Subscriber certificate adjudication and adequate controls are in place to prevent the CA Operator from issuing unauthorized Subscriber certificates.

RA Operator (Officer)

The RA Operator's role and corresponding procedures are defined in the CPS. The officer role is responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the certificate issuance process;
- Requesting, approving and executing the certificate revocation process.

Security Officer (Auditor)

The Security Officer's role is responsible for:

- Reviewing, maintaining, and archiving CA audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

System Administrator (Operator)

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

Other Trusted Roles

The CPS lists other relevant trusted roles and their responsibility not specifically cited in this CP.

5.2.2 Number of Persons Required per Task

Two or more persons are required for CAs operating at the Medium Level of Assurance for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup.

Where multiparty control for logical access is required, at least one of the participants is an Administrator. All participants serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access is not achieved using personnel that serve in the Auditor Trusted Role.

Physical access to the CAs does not constitute a task as defined in this section. Therefore, two-person physical access control is attained as required in Section 5.1.2.

5.2.3 Identification and Authentication for Each Role

Individuals identify and authenticate themselves before being permitted to perform any actions involved in a trusted role. User access is initiated and terminated through a registration procedure. Accounts and passwords are issued and managed in a manner ensuring the integrity of the system. User rights and privileges are limited to the duties and responsibilities of the individual to which they are issued. User's access rights are reviewed regularly. Policies regarding password length, complexity, and use are strictly adhered to.

5.2.4 Roles Requiring Separation of Duty

Individual CA personnel are specifically designated to the four roles defined in Section 5.2.1 above. Individuals only assume one of the RA Operator (Officer), CA Operator (Administrator), Security Officer (Auditor), or System Administrator (Operator) role. The CA system identifies and authenticates its users and ensures that no user identity can assume both a CA Operator (Administrator) and RA Operator (Officer), assume both the CA Operator (Administrator) and Security Officer (Auditor) roles, or assume both the Security Officer (Auditor) and RA Operator (Officer) role. No individual is assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The CA identifies at least one individual or group responsible and accountable for the operation of the CA. The individual assuming the role of CA Operator exhibits loyalty, trustworthiness, and integrity, and demonstrates a high degree of security and awareness in their daily activities. All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens.

All CA personnel:

- Are not assigned other duties that would interfere with their regular duties and responsibilities;
- Have not knowingly been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Are appointed in writing by an approving authority;
- Receive proper training in the performance of their duties.

5.3.2 Background Check Procedures

All Certification Authority Certification Authority personnel are required to undergo a DEA Sensitive background investigation. All background checks are performed by DEA in accordance with DEA Personnel Security Policies and are performed at the time an offer is extended to the applicant. Positions are contingent on DEA acceptance and successful clearance adjudication. All Certification Authority Certification Authority personnel are U.S. Citizens.

5.3.3 Training Requirements

CA employees receive training in the organizational policies, CA/RA security principles and mechanisms, all PKI software versions in use on the CA system, all PKI duties they are expected to perform, and disaster recovery and business continuity procedures. Training is an ongoing and documented process. Any significant change to CA operations contains a training (awareness) plan, and the execution of this plan is documented. Documentation is maintained identifying all personnel who received training and the type of training completed.

Personnel performing duties with respect to the operation of a CA receive:

- Training in the operation of the software and/or hardware used in the CA system;
- Training in the duties they are expected to perform;
- Briefing on stipulations of the CA’s CPS and this CP;
- Ongoing training in security procedures and policies.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles are aware of changes in the DEA CSOS CA operation. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented. Examples of such changes: DEA CSOS CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The DEA Diversion Control Technology Section Chief or Program Manager suspends an individual’s access to the CA system if that individual has performed actions involving the CA not authorized in this CP or the CA’s CPS.

Breach of this CPS whether through negligence or with malicious intent, is subject to privilege revocation, administrative discipline, and/or criminal prosecution.

Employee Termination Controls

Once an employee holding a position of trust or any level of system access leaves the organization, their physical access and system access is revoked upon receipt of termination documentation to ensure system integrity.

5.3.7 Independent Contractor Requirements

Contractor personnel employed operating any part of the CSOS System meet all applicable requirements set forth in the CP or this CPS and are cleared to the level of the role performed as identified in Section 5.3.1.

5.3.8 Documentation Supplied To Personnel

This CP and relevant parts of the CPS are made available to the CA and associated RA personnel. Operation manuals are made available to CA personnel to facilitate the operation and maintenance of the CA.

Personnel Security Controls for End Entities

In addition to the CP, Subscribers are provided with information on the use and protection of the software used within CSOS domain. The CA provides a technical help desk support for all Subscribers.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

For audit purposes, the CA logs operational events pertaining to Subscriber enrollment and certificate management. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used.

The CA records the events identified in the NIST-developed CIMC Protection Profile for Level 3 components. All security auditing capabilities of the CA operating system and CA PKI applications are enabled. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of entry;
- The date and time the event occurred;
- A success or failure indicator when executing the CA’s signing process;
- A success or failure indicator when performing certificate revocation; and
- Identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA is an auditable event; the message includes the message date and time, source, destination, and contents.

Procedures specifying integrity controls, event record lifetime and event record access are implemented and maintained. The audit log is reviewed for abnormalities in support of any suspected violation and for events such as repeated failed actions, requests for privileged information, attempted access of system files, and certificate and revocation/suspension requests that fail authentication and validation criteria. A review of event entries is performed regularly and follow up actions are taken for suspicious events or omissions.

5.4.2 Frequency of Processing Log

The CA establishes procedures within its CPS for the daily review of audit log files wherein a statistically significant set of security audit data generated by the CA since the last review is examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. All significant and notable events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs that might indicate potential compromise. Actions taken as a result of these reviews are documented.

The CA makes audit log summaries available to the PMA for review upon request.

5.4.3 Retention Period for Audit Log

Audit logs are retained onsite for at least two months as well as retained in the manner described below. At the end of this period, the security audit log information is moved to a safe, secure storage location separate from the CA equipment and are retained as archive records in accordance with Section 5.5.

The individual who removes audit logs from the CA system is an official different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

CA system configuration and procedures are implemented together to ensure that only authorized persons read, archive or delete security audit data. The entity performing security audit data archive does not have modify access. Procedures are implemented to protect archived data from disclosure, deletion, modification or destruction prior to the end of the security audit data retention period. CA systems are configured so that audit logs are not overwritten if the log becomes full.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up at least monthly. Adequate backup procedures are in place to comply with archive requirements identified in Section 5.5 and to recover audit log data in the event of a system failure. A copy of the audit log is sent off-site in accordance with the CPS on a monthly basis.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is internal to the CA system. Audit processes are invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the CA ceases operations except for revocation processing until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

Operational staff perform self-assessments of the security controls at the time of initial installation and configuration of the DEA Diversion Control CSOS System PKI components. Periodic vulnerability assessments are performed quarterly, upon notification of updates to vulnerability scanning software signature files, or following a system configuration change with the potential for effecting system security (e.g., hardware, software, or network changes or upgrades).

5.4.8 Vulnerability Assessment

Vulnerability assessments are routinely conducted and performed prior to initial production or after any configuration changes to identify potential vulnerabilities or events that would affect the integrity and operation of the CA. The CA and other operating personnel are watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel.

5.5 Records Archival

5.5.1 Types of Records Archived

CA archive records are sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data is recorded for archive:

- CA accreditation (if applicable);
- Certificate Policy;
- Certification Practices Statement;
- WebTrust for CA accreditation;
- Contractual obligations;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- All certificates issued or published;
- Record of Re-key;
- Certificate requests;

- Revocation requests;
- Subscriber Identity Authentication data as per Section 3.1;
- Documentation of receipt and acceptance of certificates;
- Documentation of receipt of tokens;
- All certificates issued or published;
- Record of Entity CA Re-key;
- All ARLs and CRLs issued and/or published;
- All audit logs and computer security audit data (in accordance with Section 5.4);
- Other data or applications to verify archive contents;
- Documentation required by compliance auditors.

5.5.2 Retention Period for Archive

Archival of the recorded events in Section 5.5.1 is retained and protected against modification or destruction for a period specified in the CPS. Applications required for processing the archive data are maintained for the same period as the archival records.

5.5.3 Protection of Archive

The media on which the archive is stored must be protected at a level required to maintain and protect Subscriber information from disclosure, modification or destruction either by physical security alone, or a combination of physical security and cryptographic protection. It should also be adequately protected from environmental threats such as temperature, humidity and magnetism. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media is defined by the archive site. Alternatively, data is retained using procedures that have been approved by the U.S. National Archives and Records Administration (NARA) for that category of documents.

The contents of the archive are not released except as determined by the DEA Diversion Control CSOS System PMA or as required by law. Records of individual transactions are released upon authenticated request of any Subscribers involved in the transaction or their legally recognized agents.

5.5.4 Archive Backup Procedures

CA backup procedures are in place and establish the proper operation of the CA, or validity of any certificate (including those revoked or expired) issued by the CA.

5.5.5 Requirements for Time-Stamping of Records

CA archive records are automatically time-stamped as they are created. The CPS describes how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

No Stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized personnel are permitted to access the archive.

5.6 Key Changeover

CA keys are changed while sufficient life remains on the certificate to allow uninterrupted validity of all Subscribers. If keys are changed due to changes in software or hardware, the current keys are maintained for a sufficient period to allow uninterrupted validity of all subordinate subjects. New keys are generated as per Section 4.7.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The members of the DEA CSOS PKI Policy Authority are notified if any of the following cases occur:

- suspected or detected compromise of the DEA CSOS systems;
- physical or electronic attempts to penetrate DEA CSOS systems;
- denial of service attacks on DEA CSOS components;
- any incident preventing the DEA CSOS from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

This will allow member entities to protect their interests as Relying Parties.

The DEA CSOS Operational Authority reestablishes operational capabilities as quickly as possible in accordance with procedures set forth in the DEA CSOS CPS.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, the CSOS Certification Authority responds as follows:

- Before returning to operation, ensure that the system's integrity has been restored
- If the CA signature keys are not destroyed**,** CA operation is reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.

If the CA signature keys are destroyed**,** CA operation is reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity Private Key Compromise Procedures

In the event the CSOS SCA private key is compromised, the CSOS Certification Authority implements the *CSOS System Key Compromise Plan*. A summary of steps that are followed include:

1. The CA immediately revokes all of the certificates it has issued and its own certificate and posts its CRL in the repository and on DEA's web site.
2. The CA generates a new CSOS Certification Authority private key.
3. A digitally signed email is forwarded to all Subscribers via their CSOS Coordinators informing them of certificate revocation and re-enrollment procedures.

The compromise is investigated per procedures listed in the *Incident Response Plan* and reported to the PMA.

5.7.4 Business Continuity Capabilities After a Disaster

The CA has an appropriate contingency plan, disaster recovery plan, or business resumption plan in place that is capable of resuming services in accordance with this CP. If CA equipment is damaged or rendered inoperative, but CA signature keys are not destroyed, CA operations are reestablished, giving priority to the ability to generate certificate status information, such that ARL/CRLs can be posted within 24 hours of the event. The CA reestablishes revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. The CA addresses long-term interruption restoration procedures in its CPS and Contingency Plan.

Recovery/resumption plans are in place for all potential scenarios (e.g. inadvertent destruction/corruption of critical systems/data, natural disaster, and terrorism) recognized in a current risk assessment. The CA identifies redundant capabilities (e.g. back-up systems, location of archived data, records/key availability, and off-site facilities/personnel). A list of key personnel and their contact information is easily accessible in the event of an emergency.

5.8 CA or RA Termination

In the event of CSOS CA termination, the PMA oversees the termination process. The CA Help Desk staff works to notify CSOS Coordinators of the CSOS CA cessation of operation via telephone call or digitally signed email. All certificates issued by the CSOS CA are revoked no later than the time of termination. Prior to CA termination, all archived data is provided to an archival facility under the supervision of the Security Officer and Program Manager. The *PMA Operations Guide* describes the PMA's responsibilities during the termination process.

Section 6 – Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information by the DEA CA and entity CAs are generated in FIPS 140 validated cryptographic modules. The cryptographic modules for the DEA CA meet Security Level 3.

CA key pair generation creates a verifiable audit trail that verifies that the security requirements for procedures are followed. For all levels of assurance, the documentation of the procedure is detailed enough to show that appropriate role separation is used. An independent third party validates the process.

If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process is not restarted and continues.

6.1.1.2 Subscriber Key Pair Generation

Key generation is performed using a FIPS approved method or equivalent international standard.

For Medium assurance, validated software is used for key generation.

6.1.2 Private Key Delivery to Subscriber

No private keys are transferred or exchanged. All entities generate their own private keys and do not require delivery.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber’s public key is transferred to the RA or CA in a way that ensures:

- It has not been altered during transit;
- The sender possesses the private key that corresponds to the transferred public key;
- The sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of the CA signing key pair is delivered to end entities in a secure fashion. The new public key is distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g. cross-) certificate obtained from the issuer(s) of the current CA certificate.

The CA posts the certificate it issues in the CA repository or CA web site.

6.1.5 Key Sizes

All FIPS-approved signature algorithms are considered acceptable; additional restrictions on key sizes are detailed below:

The DEA CA and subordinate or cross-certified CA signature keys is FIPS 186-2 approved of at least 2048 bits (standard) for RSA or Digital Signature Algorithm (DSA), and at least 283 (elliptical) bits for Elliptic Curve Digital Signature Algorithm (ECDSA).

CAs that generate certificates and CRLs under this policy use Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186-2. Signatures on certificates and CRLs that are issued after 1/1/09 are generated using SHA-256.

Subscriber keys that expire before 12/31/08 are at least 1024 bit RSA with a FIPS 186-2 approved hashing function. Subscriber keys that expire on or after 12/31/08 contain public keys that are at least 2048 bit RSA, in accordance with FIPS 186-2.

Use by the CA of Secure Socket Layer (SSL), Transport Layer Security (TLS), or another protocol providing similar security to accomplish any of the requirements of this CP require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/08. Use of SSL, TLS, or another protocol providing similar security to accomplish any of the requirements of the CP require, at a minimum, Advanced Encryption Standard (AES) 128 bits or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/08.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters prescribed in the Digital Signature Standard (DSS) are generated in accordance with FIPS 186-2.

Parameter quality checking (including testing for prime numbers) are performed in accordance with FIPS 186-2.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

CA and Subscriber signing keys are only used for digital signature and non-repudiation; CA signing keys are used for certificate and CRL signing as specified in the *CSOS System Certificate and CRL Profile* document.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

At a minimum, DEA Bridge and subordinate or cross-certified CA cryptographic modules are validated to the latest version of FIPS 140 series - Level 3 (hardware).

At a minimum, CSOS Subscriber cryptographic modules are validated to the latest version of FIPS 140 series -Level 1 (hardware or software).

6.2.2 Private Key (n out of m) Multi-Person Control

A minimum of two persons are required for all CA operations activities.

6.2.3 Private Key Escrow

A key used to support non-repudiation services is not allowed to be escrowed by a third party.

6.2.4 Private Key Backup

CA private signature keys are backed up under the same multi-person control as the original signature key. Such backup creates only a single copy of the signature key at the CA location; a second copy is kept at the CA backup location. All copies of the backed-up key must be handled in an accountable manner that protects against unauthorized access and unauthorized use. Procedures to affect this are included in the CPS.

Backup of the Subscriber’s private key is prohibited.

6.2.5 Private Key Archival

Subscriber private signature keys are not archived, escrowed, or copied.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The CA signing private key pair is generated and handled by cryptographic modules in a manner compliant with FIPS 140-1 level 3 or 140-2 level 3.

6.2.7 Private Key Storage on Cryptographic Module

The CA signing private key pair is generated and handled by cryptographic modules in a manner compliant with FIPS 140-1 level 3 or 140-2 level 3.

6.2.8 Method of Activating Private Key

Authorized personnel log on to the CA systems to activate CA private signing keys in accordance with Section 5.2. The means of authentication is dual-factor. Acceptable means of authentication include, but are not limited to, pass-phrases, Personal Identification Numbers (PINS) or biometrics (fingerprint, iris or retinal scan, facial or voice recognition). Entry of activation data is protected from disclosure (i.e., the data should not be displayed while it is entered).

CSOS Subscribers are authenticated to the cryptographic module before the activation of any private key(s). Approved means of authentication include pass-phrases, PINs or biometrics (fingerprint, iris or retinal scan, facial or voice recognition).

For all Subscribers, entry of activation data is protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

After use, the CA cryptographic module is deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity. Subscriber cryptographic modules that have been activated are not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module is deactivated (e.g., via a manual logout procedure, or automatically after a period of inactivity). Hardware cryptographic modules are maintained under the control of the Subscriber.

6.2.10 Method of Destroying Private Key

The specific mechanism for destroying CA private keys is defined in the CPS and is approved by the PMA.

Subscriber private signature keys are destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated in Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA public key is archived in accordance to the procedures described in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage period for a CA key pair is a maximum of six years. CA private keys are used to generate certificates for the first half of the usage period (3 years), and the public key is used to validate certificates for the entire usage period. If the CA private key is used to sign CRLs, it is used to sign CRLs for the entire usage period.

Subscriber certificates expire upon the expiration of the Subscriber’s DEA registration and are limited to a maximum of three years. Subscribers renew their CSOS certificates to continue to conduct CSOS business electronically.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Where CAs use passwords as activation data for the CA signing key, at a minimum, the activation data is changed upon CA re-key.

The activation data (password) used to unlock the CA or the Subscriber’s private key, in conjunction with any other access control, is generated in conformance with FIPS112 and results in a high level of strength for the keys or data to be protected. CAs document their rules on password selection in their CPS.

Subscriber activation data is user selected and generated in conformance with FIPS-112. If the activation data must be transmitted, it is done via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Activation data used to unlock the CA or Subscriber private key is securely protected against modification and disclosure by a combination of cryptographic and physical access control mechanisms. Activation data for private keys associated with certificates asserting individual identities is never shared.

Activation data is either memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and is not stored with the cryptographic module. If activation data is written down, it is secured at the level of the data that the associated cryptographic module is used to protect, and is not stored with the cryptographic module.

The CA activation data protection mechanism includes a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA Security Controls: The computer security functions are provided by the operating system or through a combination of operating system, software, and physical safeguards and are outlined in a CA Security Plan. The CA operating system enforces the identification, authentication, auditing, and separation of roles of all users. A secure logon process is used to access the CA's systems. An access control policy and an account management process is implemented to restrict access to information and system functions. Isolation of sensitive systems to a dedicated computing environment is required. Malicious software detection and prevention controls are implemented and are kept current. This is an ongoing task. Procedures exist to address prevention, removal, recovery, and documentation.

Subscriber System Security Controls: The system employs an inactivity time-out period of no greater than ten minutes after which the certificate holder re-authenticates to access the private key.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA uses software that has been designed and developed under a formal, documented development methodology. Hardware and software procured to operate the CA is purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

Hardware and software developed specifically for the CA is developed in a controlled environment, and the development process is defined and documented. The CA demonstrates that security requirements were achieved through a combination of software verification &

validation, structured development approach, and controlled development environment.

Where open source software is utilized, the CA/RA demonstrates that security requirements are achieved through software verification & validation and structured development/lifecycle management.

All hardware is shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.

New equipment and software, including patches and updates, are thoroughly tested on a separate platform for functionality and vulnerabilities prior to being implemented on operational systems. Operational systems are physically and logically separate from developmental systems and systems used for testing software patches and updates to maintain integrity of services provided. Risks are examined as a part of the configuration management process and vulnerability assessments are conducted on operational systems after the installation of software patches, updates, or modifications that result in significant changes to configuration settings. Procedures for implementation on operational systems are developed during testing on isolated systems.

Proper care is taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA are obtained from sources authorized by local policy. All hardware and software are scanned for malicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

A security document exists that details security controls that have been implemented to the system. This document provides guidance for the secure operation of the CA and for ensuring the integrity of its operating environment. Responsible individuals implement and maintain the security policy.

The configuration of the CA and supporting systems, as well as any modifications and upgrades are documented and controlled through formal change management processes. There is a mechanism for detecting unauthorized modification to CA software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

See Section 6.6.1.

6.7 Network Security Controls

CAs employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Access to unused ports and services are denied to prevent misuse. Any boundary control devices used to protect the network on which PKI equipment is hosted denies all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. Users are provided access only to services that they are specifically authorized to use from terminals designated for that function. Connections to services from network paths other than those specified for that function are refused. Dial-up or external access to the CA via system administration interface is prohibited. External threats are mitigated by controls such as firewalls, network intrusion detection systems and router access lists to protect the internal network. Any network software present on the CA equipment is necessary to the functioning of the CA. The CA documents security attributes of all network services.

6.8 Time-Stamping

Asserted times are accurate to within three minutes. Electronic or manual procedures are used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

Section 7 – Certificate, CRL, and OSCP Profiles

7.1 Certificate Profile

The CSOS Certification Authority issues X.509v3 certificates in accordance with the *DEA CSOS System Certificate and CRL Profile*.

The CSOS Certification Authority uses the following fields of the X.509v3 certificate format:

- **Version:** version field is set to v3
- **Serial number:** when a new certificate is created, a unique serial number within the CA security domain is generated by the CA
- **Signature:** identifier for the algorithm used by the CA to sign the certificate.
- **Issuer:** CA Distinguished Name
- **Validity:** certificate validity period – the notBefore start date and notAfter end date are specified
- **Subject:** certificate subject distinguished name
- **Subject public key information:** includes the signing algorithm identifier and public key
- **Extensions:** see Section 7.1.2 below

The following fields of the X.509 version 3-certificate format are not used in this PKI:

- issuer unique identifier
- subject unique identifier

7.1.1 Version Number(s)

The DEA and subordinate or cross-certified CAs issue X.509 version 3 certificates.

7.1.2 Certificate Extensions

A number of X.509v3 certificate extensions are included in certificates issued by this Certification Authority as well as two private extensions defined by this Certification Authority. These are outlined below. The X.509 version 3 certificate extensions, which are not present in certificates issued by this Certification Authority, are also outlined below.

The following certificate extensions are used by this Certification Authority:

X.509 v3 Certificate Extension	Critical/Non Critical	Required/ Optional	Notes
AuthorityKeyIdentifier	Non critical	Optional	Used where user may have multiple keys for signing. Identifies which key is used
SubjectKeyIdentifier	Non critical	Required	For chain building, and identifying certificates that contain a particular public key
BasicConstraints	Critical	Required	cA Boolean equals true
CRLDistributionPoints	Non critical	Optional	only 1 distribution point name is included in each certificate only element [0] (distributionPoint) is used and includes the full DN
KeyUsage	Critical	Required	Restricts how keys may be used. A subset of the following must be present: digitalSignature(required), NonRepudiation (optional), KeyCertSign (optional), and/or CRLSign (optional).
CertificatePolicies	Critical	Required	Indicates the policies under which the certificate has been issued.
VersionInfo	Non critical	Required	Certificate extension representing version
PrivateKeyUsagePeriod	Non critical	Required	This extension indicates the period of use of the private key corresponding to the certified public key
AuthorityInfoAccessSyntax	Non Critical	Optional	Used for non-CRL revocation methods
ExtKeyUsageSyntax	Non Critical	Optional	Extendable uses of public key, in addition to key usage

The following X.509 version 3 certificate extensions are not used in this CA:

- policy mappings
- name constraints
- policy constraints
- issuer alternative name
- subject directory attributes
- subject alternative name

7.1.3 Algorithm Object Identifiers

Algorithm	Object Identifier	Issuing Authority
sha1WithRSAEncryption	1 2 840 113549 1 1 5	RSADSI
DSA-with-SHA1	1 2 840 10040 4 3	X9-57
ECDSA with SHA-1	1 2 840 10045 1	ANSI-X9-62

7.1.4 Name Forms

Every DN and subject DN fields contain the full X.500 DN of the CA..

7.1.5 Name Constraints

Subject and Issuer DNs must comply with CSOS standards and be present in all certificates.

7.1.6 Certificate Policy Object Identifier

This CPS supports the CSOS Certificate Policy. This certificate policy applies to public key certificates issued for digital signature applications.

7.1.7 Usage of Policy Constraints Extension

The CSOS Certification Authority does not use policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

CSOS Subscriber certificates have the policyQualifier extension populated with an explicit text notice as follows:

This is a DEA CSOS Digital Certificate. It is specifically intended for use in signing controlled substance orders - any other signing uses are at the discretion of the certificate holder.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

CSOS Certification Authority certificates under this policy mark the certificate policy extension as non-critical. Critical extensions are interpreted as defined in the IETF RFC 3280.

7.2 CRL Profile

The following fields of the X.509v2 CRL format are used in this CA:

- **Version:** set to v2
- **Signature:** identifier of the algorithm used to sign the CRL
- **Issuer:** the full Distinguished Name of the CA
- **This update:** time of CRL issuance
- **Next update:** time of next expected CRL update
- **Revoked certificates:** list of revoked certificate information

7.2.1 Version Number(s)

The CSOS Certification Authority issues X.509v2 CRLs in accordance with the *DEA CSOS Certificate and CRL Profile*.

7.2.2 CRL and CRL Entry Extensions

A number of X.509v2 CRL and CRL entry extensions that are used in this PKI are outlined below. The X.509v2 CRL and CRL entry extensions that are never present in CRLs issued by this CA are also outlined below. The following exhibit identifies the CRL and CRL entry extensions that are used in this Certification Authority:

X.50v2 CRL Extension	Critical/Non Critical	Required/ Optional	Notes
authorityKeyIdentifier	Non critical	Required	only element [0] (authorityKeyIdentifier) is filled in contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	Non critical	Required	Incremented each time a particular CRL/ARL is changed
deltaCRLIndicator	Critical	Optional	Improves processing time for applications that store revocation info. in a format other than the CRL
issuingDistributionPoint	Critical	Required	element [0] (distributionPoint) includes the full DN of the distribution point element [1] (onlyContainsUserCerts) is included for CRLs element [2] (onlyContainCACerts) is included for ARLs element [1] and [2] are never present together in the same revocation list elements [3] and [4] are not used
ReasonCode	Non critical	Required	CRL entry extension - supports all reason codes
holdInstructionCode	Non critical	Optional	CRL entry extension
InvalidityDate	Non critical	Required	CRL entry extension

certificateIssuer	Critical	Required	CRL entry extension

Exhibit 7-1. CRL and CRL Entry Extensions

The following X.509v2 CRL extension is not used in this Certification Authority:

- Issuer alternative name.

7.3 OCSP Profile

If implemented, Certificate Status Servers (CSS) sign responses using algorithms designated for CRL signing.

7.3.1 Version Number(s)

Not applicable .

1.3.2 OCSP Extensions

Not applicable

Section 8 – Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

The OMA arranges full and formal initial and annual audits to validate that the PKI is operating in accordance with the security practices and procedures described in this CPS. Results of the audits are provided to the PMA.

The PMA may order a compliance audit or inspection at any time of the CSOS Certification Authority, RA or any Local RA services being provided by CSOS Coordinators in order to validate that these entities are operating in accordance with the security practices and procedures described in the CPS.

8.2 Identity/Qualifications of Assessment

Auditors are selected through competitive bidding processes. The PMA establishes the qualifications for the selection of entities seeking to perform a compliance audit. The qualifications are in compliance with the Federal PKI Policy Management Authority guidelines for such compliance as stipulated in the FPKIPA *Audit Letter of Compliance,* which can be found at (http://www.cio.gov/fpkipa/documents/audit_guidance.pdf). Selected auditors are, at a minimum, qualified to perform either an American Institute of Certified Public Accountants (AICPA) audit to the WebTrust® Principles and Criteria for Certification Authorities ("CA Trust") or NIST Special Publication 800 series compliant certifications and accreditations., though both qualifications are desirable. Performing system audits must be the selected auditor's primary responsibility.

Selected auditors are provided with copies of the policy documents and security plans in order to familiarize themselves with the requirements that the PMA imposes on the issuance and management of the CSOS certificates as provided in the CP prior to conducting the audit.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor is a contractor that is sufficiently independent from the DEA, PMA or OMA to provide an unbiased, independent, and repeatable evaluation.

8.4 Topics Covered by Assessment

The PMA may elect to have a NIST-compliant Special Publication 800-53 Certification and Accreditation (C&A) performed on the CSOS system. FISMA-compliant C&A protocols are followed completely and include this CPS, the CP and other CA security policies and procedures. The auditors adhere to the scope established by the PMA.

The PMA may elect to have a WebTrust® audit performed. For such an audit, the auditors use the *American Institute of Certified Public Accountants (AICPA) WebTrust® for Certification Authorities* criteria and adhere to the scope established by the PMA. The audit investigates all aspects of the CA operations to ensure compliance with this CPS, the CP and other CA security policies and procedures. The AICPA/CICA WebTrust® Program for Certification Authorities is consistent with standards being developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF). *The WebTrust for Certification Authority Principles and Criteria* can be found at http://www.webtrust.org/CertAuth_fin.htm.

The PMA may, at its discretion, elect to have both a NIST-compliant Special Publication 800-53 Certification and Accreditation and a WebTrust® audit performed on the CSOS system.

8.5 Actions Taken as a Result of Deficiency

Should the compliance auditor find a discrepancy between the Certification Authority's operation and the stipulations contained in the CP or CPS, the following must occur:

- The compliance auditor notes the discrepancy;
- The Certification Authority provides written notification of the audit results to the PMA and OMA, specifically identifying any deficiencies noted as a result of the compliance audit, within 3 business days;

- Once notified, the PMA and OMA have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken.

- Based on the findings of the compliance audit, appropriate remedies may include:
  - Warn the Certification Authority in writing and specify a time period during which the discrepancy must be resolved;
  - Immediately suspend the Certification Authority's authority to issue new certificates;
  - Revocation of the CSOS Certification Authority. Due to the negative financial impact on the CSOS community, the CA certificates and the CSOS Subscriber certificates are not immediately revoked as a result of negative audit findings provided by the third-party auditor against the CSOS Certification Authority, unless findings indicating Key Compromise have been substantiated and the PMA majority vote deems it necessary to implement the Key Compromise Plan. Suspension of new certificates until audit discrepancies are resolved, however, may be directed by the PMA. Several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate-using community.
- The implementation of proposed remedies, including a time for their completion, are communicated in a written report to the PMA.

Upon correction of the discrepancy, the Certification Authority may request reauthorization. A special audit may be required to confirm the implementation and effectiveness of the remedy. The *PMA Operations Guide* details the PMA's responsibilities and procedures for making and implementing such determinations.

8.6 Communications of Results

Notification of compliance audit failure, the topics of failure, reasons for failure, and possible remedies are provided within 24 hours, upon the conclusion of the compliance audit, in a written form (signed e-mail or letter) to the PMA and OMA. A full, written, notification of the audit results are provided to the PMA and the OMA within 3 business days. The report contains a summary table of topics covered, areas in which the CSOS Certification Authority was found to be non-compliant, a brief description of the problem(s) for each area of non-compliance, a brief description of the problem(s) for each area of non-compliance, and possible remedies for each area. The report also contains the detailed results of the compliance audit for all topics covered, including the topics in which the CSOS Certification Authority passed and the topics in which the CSOS Certification Authority failed.

In the case of a deficiency action, the PMA makes an effort, as they deem appropriate, to ensure that all CSOS PKI Subscribers are informed of the action. Communication to users to inform them of any deficiency and action is performed via email if possible through the CSOS Coordinators. If a CSOS Coordinator does not have e-mail access, then a letter is sent to the Subscriber.

Section 9 – Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DEA does not charge fees for the issuance of CSOS Subscriber certificates or for status checking information (CRLs), nor will the CA impose any fees to end entities for the reading of the Certificate Policy, this CPS, or any other document incorporated by reference.

The OMA, with the approval of the PMA, will determine the fees, if any, for other CSOS services. The OMA reserves the right to charge fees for the issuance of certificates as well as for access to certificate status information, subject to agreement between the CA and the Subscriber and/or between the CA and the Relying Party, in accordance with a fee schedule that would, at that time, be posted onto the CSOS web site.

9.1.2 Certificate Access Fees

DEA does not charge fees for the issuance of CSOS Subscriber certificates or for status checking information (CRLs), nor will the CA impose any fees to end entities for the reading of the Certificate Policy, this CPS, or any other document incorporated by reference.

The OMA, with the approval of the PMA, will determine the fees, if any, for other CSOS services. The OMA reserves the right to charge fees for the issuance of certificates as well as for access to certificate status information, subject to agreement between the CA and the Subscriber and/or between the CA and the Relying Party, in accordance with a fee schedule that would, at that time, be posted onto the CSOS web site.

9.1.3 Revocation or Status Information Access Fees

DEA does not charge fees for the issuance of CSOS Subscriber certificates or for status checking information (CRLs), nor will the Certification Authority impose any fees to end entities for the reading of the Certificate Policy, this CPS, or any other document incorporated by reference.

The OMA, with the approval of the PMA, will determine the fees, if any, for other CSOS services. The OMA reserves the right to charge fees for the issuance of certificates as well as for access to certificate status information, subject to agreement between the Certification Authority and the Subscriber and/or between the Certification Authority and the Relying Party, in accordance with a fee schedule that would, at that time, be posted onto the CSOS web site.

9.1.4 Fees for Other Services

The OMA, with the approval of the PMA, will determine the fees, if any, for other CSOS services. The OMA reserves the right to charge fees for the issuance of certificates as well as for access to certificate status information, subject to agreement between the CA and the Subscriber and/or between the CA and the Relying Party, in accordance with a fee schedule that would, at that time, be posted onto the CSOS web site.

9.1.5 Refund Policy

If fees are charged for any of the services described above, the Certification Authority will clearly post a refund policy on their web site.

9.2 Financial Responsibility

The U.S. Government shall bear no financial responsibility, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

Issuance of certificates in accordance with this CP does not make the CSOS Root CA an agent, fiduciary, trustee, or other representative of the subordinate or cross-certified CAs or their Subscribers.

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that is not included in the certificates is protected and access is restricted as defined in the following subsections.

Each Subscriber’s private signing key is private to that Subscriber. The Certification Authority and RA are not provided any access to these keys.

Information held in Certification Authority audit trails is considered confidential to the DEA and is not released outside the organization, unless required by law.

9.3.2 Information Not Within the Scope of Confidential Information

Information included in the CP, public certificates, and CRLs issued by the CSOS Certification Authority is not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CSOS Operational Authority conducts a Privacy Impact Assessment. If deemed necessary, the CSOS Operational Authority has a Privacy Plan to protect personally identifying information from unauthorized disclosure. The CSOS Policy Authority approves the Privacy Plan.

For Entity CAs, no stipulation.

9.4.2 Information Treated as Private

Personal and agency information held by the Certification Authority, other than that which is explicitly published as part of a certificate, CRL, CP or this CPS is considered private and is not released outside the DEA, unless required by law. The Subscriber information is used only for the purpose collected and such information is not released without the prior written consent of the Subscriber, unless otherwise required by law. The results of audits are kept confidential, with exceptions as deemed appropriate by the PMA.

9.4.3 Information Not Deemed Private

Information included in the CP, public certificates, and CRLs issued by the CSOS Certification Authority is not considered private.

When the CA revokes a certificate, a revocation reason is included in the CRL entry for the revoked certificate. This revocation reason code is not considered private and can be shared with all other users and relying parties. However, no other details concerning the reason for revocation are disclosed.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to Use Private Information

The CSOS Operational Authority is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Information released to law enforcement officials is in accordance with applicable laws and regulations and is processed according to 41 CFR 105-60.605.Any request for release of Subscriber information is authenticated. The authentication consists of validating the identity of the requester using two forms of photo identification.

9.4.7 Other Information Disclosure Circumstances

Subscriber information from this system may be disclosed to the following parties:

- To federal, state or local agencies along with state medical and licensing boards responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when the DEA Office of Diversion Control, Technology Section becomes aware of a violation or potential violation of civil or criminal law or regulation.
- To a member of Congress or to a congressional staff member in response to a request from the person who is the subject of the record.
- To a DEA employee, an expert consultant, or contractor of DEA in the performance of a federal duty to which the information is relevant.
- Persons registered under the Controlled Substances Act (P.L. 91-513) for the purpose of verifying the registration of customers and practitioners.

Unless otherwise required by law and under the conditions stated above, Subscriber information is only used for the purpose collected and agreed and such information is not released without the prior written consent of the Subscriber. Any request for release of Subscriber information is authenticated. The authentication consists of validating the identity of the requester using two forms of photo identification. In the case where a Subscriber’s information is provided to a third party – the third party’s authority to obtain the information is validated using at least one of the following means:

- The individual has the duly executed court order from a Federal court;
- The individual has a duly executed request from the respective Agency Office of Inspector General.

Information that may be reviewed includes only that information pertaining to the individual subscriber submitting the request that is maintained by the DEA in a system of records.

Detailed instructions for making requests for access to records are provided on the CSOS web site. In response to a proper request for access, CSOS notifies the requesting individual subscriber whether the CSOS system of records contains any records pertaining to him or her, and, if records exist, the manner in which those records may be reviewed.

9.5 Intellectual Property Rights

Subscriber private signature keys are treated as the sole property of the legitimate holder of the corresponding public key identified in a CSOS certificate.

Certificates and CRLs issued by the CSOS Root CA and CSOS Certification Authority are the exclusive property of the U.S. Government.

The CP, this CPS, and CSOS Object Identifiers (OID) are the exclusive property of the U.S. Government.

9.6 Representations and Warranties

The U.S. Government is not liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.6.1 CA Representations and Warranties

CSOS certificates are issued and revoked at the sole discretion of the DEA CSOS PKI Policy Authority.

9.6.2 RA Representations and Warranties

Not applicable.

9.6.3 Subscriber Representations and Warranties

Subscribers are required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers shall agree to the following:

- Accurately represent themselves in all communications with the PKI authorities.

- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.

- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the Certification Authority's CPS.

- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

9.6.4 Relying Party Representations and Warranties

None.

9.6.5 Representations and Warranties of Other Participants

None.

9.7 Disclaimers of Warranties

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

Issuance of certificates in accordance with this CPS shall not make the CSOS Root CA an agent, fiduciary, trustee, or other representative of the subordinate or cross-certified CAs or their Subscribers.

9.8 Limitations of Liability

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9 Indemnities

The PMA, CSOS Root CA, and CSOS Certification Authority assume no financial responsibility for improperly used certificates.

9.10 Term and Termination

9.10.1 Term

This CPS becomes effective when approved by the DEA CSOS Policy Authority. This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of the DEA CSOS Policy Authority.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

The DEA CSOS PMA establishes appropriate procedures for communications with Entity CAs via contracts or memoranda of agreement as applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA submits for processing any recommended changes communicated to the contact identified in Section 1.5. Updates to this CPS may be proposed at any time, however the OMA submits all draft changes to the PMA for approval before incorporation into the CPS.

9.12.2 Notification Mechanism and Period

Changes to items within this CPS, which have no or minimal impact on the Subscriber using certificates and CRLs issued by this CSOS Certification Authority, are made with no change to the CPS version number.

Changes to the certificates supported by this CPS as well as changes to items within this CPS which may have significant impact on the Subscriber using certificates and CRLs issued by this CSOS Certification Authority, are made with 30 days notice to the user community, and the version number of this CPS must be increased accordingly.

9.12.3 Circumstances Under Which OID Must be Changed

OIDs are changed if the CSOS Policy Authority determines that a change in the CPS reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

Disputes are submitted in writing to the PMA Chair for resolution. The PMA Chair makes the determination on whether an out-of-cycle PMA meeting should be held to address the dispute, or whether the dispute is added to the agenda at the next regularly scheduled PMA meeting. Prior to the meeting in which the dispute is addressed, the Chair ensures that all voting members have received notification and information regarding the matter in dispute. Any PMA voting member may request to have the parties involved attend the meeting to provide more discussion. Every attempt should be made to resolve the dispute by negotiation; however the PMA has the sole authority for the resolution of any disputes by quorum vote of the membership. Further information on PMA procedures may be found in the *PMA Operations Guide*.

9.14 Governing Law

U.S. Government laws govern the enforceability, construction, interpretation, and validity of this CPS.

9.15 Compliance with Applicable Law

The CSOS Certification Authority is required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Should it be determined that one section of this CPS is incorrect or invalid, the other sections remain in effect until the document is updated. Requirements for updating this CPS are described in Section 9.12.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CPS is incorrect or invalid, the other sections remain in effect until the document is updated. Requirements for updating this CPS are described in Section 9.12.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Disputes are submitted in writing to the PMA Chair for resolution. The PMA Chair makes the determination on whether an out-of-cycle PMA meeting should be held to address the dispute, or whether the dispute should be added to the agenda at the next regularly scheduled PMA meeting. Prior to the meeting in which the dispute is addressed, the Chair ensures that all voting members have received notification and information regarding the matter in dispute. Any PMA voting member may request to have the parties involved attend the meeting to provide more discussion. Every attempt should be made to resolve the dispute by negotiation; however the PMA has the sole authority for the resolution of any disputes by quorum vote of the membership. Further information on PMA procedures may be found in the *PMA Operations Guide*.

9.17 Other Provisions

No stipulation.