Controlled Substance Ordering System

Certificate Policy (CP)

Version 4.1
January 2015

PREPARED FOR THE DRUG ENFORCEMENT ADMINISTRATION
STERLING PARK TECHNOLOGY CENTER/CSOS
8701 MORRISSETTE DRIVE
SPRINGFIELD, VA 22152

Change Control

Date	Version	Change Description
1/6/2012	4.0	Minor updates and corrections
1/31/2014	4.1	Updated sections based on FBCA change proposals, SHA-2 transition, and FPKIMA feedback. Updated document formatting throughout.
5/15/2014	4.1	Updated sections based on additional FPKIMA feedback.
1/15/2015	4.1	2015 cover page updated, no changes.

Table of Contents

1.0 Introduction

The Drug Enforcement Administration (DEA) regulates the manufacture, distribution and dispensing of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. The DEA presently operates the Controlled Substance Ordering System (CSOS) under the CSOS Certification Authority (referred to as the "DEA CA" in this document).

DEA's CSOS program allows the electronic ordering of controlled substances between controlled substance manufacturers, distributors, pharmacies, and other DEA authorized ordering entities, using Public Key Infrastructure (PKI) technology to digitally sign the electronic transactions. The CSOS Certification Authority (CA) serves as the central element responsible for establishing a trust relationship between these trading partners, instituting the security services of authenticity, integrity and non-repudiation into the DEA's controlled substance electronic ordering system.

The CSOS CA shall be operated under the authority of the DEA Office of Diversion Control Policy Management Authority (PMA) as a subordinate CA to the DEA CA. CSOS end entity (Subscriber) certificates are issued only by the CSOS CA. These Subscriber certificates identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating that the Subscriber is operating under the authority of the DEA CSOS program. Subscribers must demonstrate acceptance of the CSOS System Certificate Policy (CP) by signing a Subscriber Agreement.

The *CSOS Certificate and CRL Profile* document, produced under separate cover, provides the necessary guidance for certificate profiles within the CSOS System.

This CSOS System CP is consistent with the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework.

The terms and provisions of this CP shall be interpreted under and governed by applicable Federal and State Law. The United States Government disclaims any liability that may arise from the use of this CP.

1.1 Overview

This document, along with the *CSOS Certificate and CRL Profile* document, defines the creation and management of certificates for use in electronic ordering applications for controlled substances. This document establishes the level of assurance and trust that can be placed in the authenticity and integrity of the public keys contained in certificates issued by authorized CAs. The word "assurance" used in this CP indicates to what extent a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate.

The associated CSOS Certification Practice Statement (CPS) describes the practices of CSOS and its CAs. It shall be used to establish the level of assurance and trust that can be placed in the authenticity and integrity of the public keys contained in certificates that are issued by the CA. Due to the sensitive nature of the security controls described within the CPS, the document is not made publicly available in its entirety, however a sanitized version is provided at http://www.deaecom.gov. This CP 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 CP, and (3) the minimum requirements for the issuance and management of digital certificates used in verifying transactions and digital signatures in CSOS applications.

1.2 Document Identification

This CP addresses CSOS certificates that are defined in subsequent sections of this document. This CP is registered with the National Institute of Standards and Technology (NIST). This CP provides substantial assurance concerning the identity of certificate subjects. Certificates issued in accordance with this CP shall assert one of the following OIDs in the certificate policy extension:

CSOS Certificates	**dea-csos-cp**	**::= { 2.16.840.1.101.3.2.1.9.3}**
CSOS Device Certificates	**dea-csos-cp-mediumDevice**	**::= { 2.16.840.1.101.3.2.1.9.4}**

The foregoing OIDs may not be used except as specifically authorized by this policy.

1.3 PKI Entities

The following sections discuss the roles relevant to the administration and operation of the CSOS System.

1.3.1 PKI Authorities

1.3.1.1 Policy Management Authority (PMA)

The CSOS PMA has been tasked by the Office of Diversion Control (OD) to be the governing body responsible for the PKI initiative. PMA membership consists of selected individuals working within the DEA Office of Diversion Control, Technology Section (ODT), Liaison and Policy Section (ODL), Registration and Program Support section (ODR), Office of Diversion Regulatory Section (ODG), the PKI Operations Management Authority (OMA), the DEA CIO or his or her representative and the

Contracting Officer's Representative (COR) supervising contractor activities relating to the CSOS System.

The mission of the CSOS PMA is to establish, interpret, and enforce policy for the CSOS PKI initiatives in accordance with all applicable U.S. laws and regulations. Additional responsibilities include:

- Approving the CSOS CP;
- Approving the CSOS CPS;

1.3.1.2 Operations Management Authority (OMA)

The CSOS Operations Management Authority, or OMA, reports to the PMA and is responsible for the daily operation and maintenance of the DEA Electronic Commerce PKI systems. The OMA also provides planning guidance and directs the activities of the DEA Electronic Commerce PKI Manager and the PKI manager's staff.

1.3.1.3 Principal Certification Authority (DEA Root CA)

The DEA Root CA shall be established by the DEA. It shall be operated and maintained by the DEA or by an authorized DEA contractor. The DEA Root CA shall operate in accordance with the provisions of its Certification Practice Statement. The DEA Root CA shall perform the following functions:

- Issue and manage cross-certification certificates as approved by the PMA, including external CAs, such as the Federal Bridge CA;
- Issue and manage the CSOS Subordinate Certification Authority approved by the PMA, as defined in this CP; and
- Publish subordinate and cross-certified CA certificate status information.

1.3.1.4 Subordinate Certification Authority (CSOS CA)

The CSOS CA 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. It shall be operated and maintained by the DEA or by an authorized DEA contractor. The CSOS CA is responsible for all aspects of the issuance and management of a certificate, including: the registration process, the identification and authentication process, the certificate manufacturing process, the revocation of certificates, and for ensuring that all aspects of the CA services and CA operations and infrastructure related to the certificates issued under the *CSOS Certificate Policy* are performed in accordance with the requirements, representations, and warranties of this CP. The CSOS CA shall conform to the stipulations of this CP definition and publish a CPS that supports and includes references to this CP.

1.3.2 Registration Authorities (RA)

A Registration Authority is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificates.

The CSOS RA shall process applications of CSOS Coordinators and Subscribers, verifying the information that is to be entered into the Subscriber's public certificate and shall operate according to the stipulations of this CP. Individuals applying for CSOS Certificates are required to do so through their CSOS Coordinator.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate issued by an authorized CSOS System CA, who attests that it uses its key and certificate in accordance with the CP asserted in the certificate. CSOS Subscribers are limited to approved DEA Registrants and those individuals that hold Power of Attorney (POA) for DEA Registrants. A registrant is a person or entity who is authorized to handle controlled substances or List 1 chemicals.

1.3.4 Relying Parties

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 uses the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

1.3.5 Other Participants

A DEA Registrant must appoint a CSOS Coordinator who will serve as that Registrant's recognized agent regarding issues pertaining to the issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration. These individuals serve as knowledgeable liaisons between one or more DEA registered locations and the CSOS Certification Authority (CA). The coordinators will collect applications, ensure that they include all of the required information, have the package notarized, and send it to the CA.

A CSOS Principal Coordinator may be any individual employed by the organization, however unless otherwise indicated, the person who signed the most recent DEA Registration application shall serve the role of CSOS Principal Coordinator.

A CSOS Alternate Coordinator shall serve as an organization's secondary CSOS contact for the DEA Registration(s) identified on their application. A CSOS Alternate Coordinator may be any individual employed by the organization. Establishment of a CSOS Alternate Coordinator is optional.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

CSOS Subscriber certificates shall only be 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.

CSOS certificates are appropriate for use with other applications requiring a Medium level of assurance or below, as defined by the Federal Bridge Certification Authority (FBCA). This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

1.4.2 Prohibited Certificate Uses

CSOS certificates may **not** be used for the signing of electronically transmitted controlled substance prescriptions.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The CSOS System PMA has been tasked by the Office of Diversion Control (OD) to be the governing body responsible for the PKI initiative and all aspects of this CP.

1.5.2 Contact Person

Direct all questions regarding this CP to the Chair of the Policy Management Authority, whose contact information can be found at http://www.deaecom.gov. Written communications may be sent to the following address:

Drug Enforcement Administration
Sterling Park Technology Center/CSOS
Attn: Chair, Policy Management Authority
8701 Morrissette Drive
Springfield, VA 22152

1.5.3 Person Determining CPS Suitability for the Policy

The CSOS PMA shall determine the CPS suitability of any CA operating under this CP, based on a compliance analysis performed by the PMA itself or a party independent from the CA.

1.5.4 CPS Approval Procedures

All CAs shall submit a CPS to the CSOS PMA for approval. The CSOS PMA shall make the determination that a CPS complies with this policy.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
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.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

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 generic term in the context of this CP that applies to an entity authorized by the DEA to issue CSOS certificates (x.509 certificates) and vouches for the binding between the data items in a certificate. This term is used in this CP to sometimes refer to the DEA CA, as well as the subordinate CAs or cross-certified CAs that would be operated by DEA or other entities in compliance with DEA regulations.

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 Practice Statement (CPS)	A statement of the practices that a CA employs in its certificate management operations (e.g., 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 Bridge Certification Authority (FBCA)	The U.S. Federal Government's mechanism for enabling trust domain interoperability at a level of assurance satisfying E-Authentication levels 1 through 4 using public key certificates.
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 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 Authority, 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 system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users
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 shall exploit 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 CA. The DEA CA shall operate in accordance with the provisions of its Certification Practices Statement. The DEA CA shall also perform 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)	A Subordinate CA is a CA authorized by the PMA to create, sign, and issue public key certificates to authorized CSOS Subscribers. Subordinate CAs operates in a hierarchical PKI, subordinate to the DEA 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.

1.6.2 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
COR	Contracting Officer's Representative
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
CSOS	Controlled Substance Ordering System
CSS	Certificate Status Servers
DEA	Drug Enforcement Administration
DN	Distinguished Names
DNS	Domain Name System
DSA	Digital Signature Algorithm

Acronym	Description
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
OMA	Operations Management Authority
PINS	Personal Identification Numbers
PKCS	Public Key Cryptography Standards

Acronym	Description
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
SIA	Strong Identification and Authorization
SHA	Secure Hash Algorithm
SO	Security Officer
SSL	Secure Socket Layer
TLS	Transport Layer Security

2.0 Publication and Repository Responsibilities

Each CA shall ensure that there is a repository where the DEA CA certificate and revocation lists are published and available for status checking. CSOS Subscriber certificates shall not be made publicly available. The repository shall be an X.500 compliant directory supporting the Lightweight Directory Access Protocol (LDAP) for access. The CA shall assert a high level of reliability and availability of the repository. Authority Revocation Lists (ARLs) and Certificate Revocation Lists (CRLs) must be published in accordance with this CP. The DEA CA shall publish this CP on DEA's web site at http://www.deaecom.gov. All CAs shall make this CP publicly available either in an online repository or a web site that is available to Subscribers and Relying Parties.

2.1 Repositories

The location of the repositories shall be appropriate to the certificate-using community and must be specified in the CPS.

2.1.1 Repository Obligations

The OMA shall use a variety of mechanisms for posting information into a repository as required by this CP. The mechanisms shall include:

- An X.500 compliant Directory Service System with LDAP access that allows authorized access and retrieval of the Certificate Revocation Lists and CSOS CA certificate information.
- Availability of the certificate information as required by the information publication and retrieval stipulations of this CP, and
- Access controls mechanisms needed to protect repository information.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- CRLs issued by the CA;
- CA certificates (shall only contain valid Uniform Resource Identifiers ("URIs");
- End Entity certificates (shall only contain valid Uniform Resource Identifiers ("URIs");
- A copy of this CP

Subscriber certificates shall not be made publicly available in the repository.

2.2.2 Publication of CA Information

The CSOS CP shall be publicly available on the CSOS DEAECOM web site (see www.deaecom.gov).

2.3 Frequency of Publication

Mechanisms and procedures shall be designed to ensure CA Certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99.9% availability overall per year, and scheduled down-time not to exceed 0.5% annually.

All information to be published in the repository shall be published according to the parameters established within this CP.

Only editorial changes or typographical corrections may be made to this specification without notification. Any item in this CP may be changed with 90 day notice. Changes to items, which shall not materially impact a substantial majority of the CAs or relying parties using this CP, may be changed with 30 day notice.

Thirty days prior to major changes to this CP, a notification of the upcoming changes shall be posted and conveyed to subordinate or cross-certified CA organizations.

2.4 Access Controls on Repositories

DEA issued CA certificates and CRLs that are published shall be publicly available through the Internet. There shall be no access controls on the reading of this CP. CAs shall implement appropriate access controls restricting who can write or modify policies, certificates, certificate status or ARLs/CRLs. Access to Subscriber certificates located in the repositories is restricted to CA personnel. Subscriber certificates shall not be made publicly available in the CSOS repository.

3.0 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

A CA shall only generate and sign Certificates that contain a non-null subject Distinguished Name (DN) complying with the X.500 standard. Certificates may also include other name forms in the subject alternative name forms field provided the field is marked as non-critical. The Common Name (CN) must be the same as the Subscriber's legal name, such as that which Federal or local records use (e.g., POA letter, agent practitioner authorization letter for agent practitioners, human resources documents, birth certificate, or driver's license) to refer to that person.

For device certificates, device naming is described within Section 3.2.5.3 Device Registration.

3.1.2 Need for Names to be Meaningful

The subject name listed in a certificate shall identify the Subscriber using the Subscriber's legal name as it appears on the DEA Form 223 (DEA Registration Certificate). If this name cannot be used, the name that Federal or local records refer to that person (e.g., POA letter, human resources documents, birth certificate or driver's license) will be used. The CA must describe in its CPS how the DN will always be unique to each Subscriber.

CSOS Subscriber certificates issued by the CSOS CA shall 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"

and will include the CN of the individual using the certificate and a serial number that is unique to the Subscriber.

CSOS Device certificates issued by the CSOS CA shall be assigned either a geo-political name or an Internet domain component name. Devices shall take the following form

C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversion Control, OU=E-Commerce, OU=CSOS, OU="State", cn=device name

where device name is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity or pseudonymity is not allowed. Each Subscriber must be uniquely identified as discussed in section 3.1.2 above and section 3.1.5 below.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are established by the PMA. These rules are contained in the *CSOS Certificate and CRL Profile* document. These documents may be found at http://www.DEAecom.gov.

3.1.5 Uniqueness of Names

The CSOS PMA is responsible for ensuring CAs enforce name uniqueness in certificates issued by the CA. The DN shall be unique for each Subscriber and will include the CN of the individual using the certificate and a serial number that is unique to the Subscriber. The CN will be 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 (e.g., POA letter, human resources documents, birth certificate or driver's license) used to refer to that person will be used.

In the event that a person is known by a name that is different than the name used to create the CN, additional CN values may be added—at the request of the Subscriber—to the CN attribute after the DN has been formed. In the event that an alternate name form is used for any reason, a CSOS PMA is responsible for ensuring name uniqueness. A CA shall document in its CPS how they shall allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if "Joe Smith" leaves a CA's community of Subscribers, and a new "Joe Smith" enters the community of Subscribers, how shall these two individuals be provided unique names).

3.1.6 Recognition, Authentication, and Role of Trademarks

CAs will document in their CPS the process by which they will resolve name claim disputes, attempting to resolve all such disputes locally. The PMA shall resolve any name collisions brought to its attention that may affect interoperability.

The CA shall choose certificate subject names issued under this CP. The CA shall not knowingly issue a certificate including a name that a court of authorized jurisdiction has determined infringes the trademark of the rightful owner. A CA is not obligated to research trademarks or resolve trademark disputes. Any CA may refuse to accept a name known to be a trademark of someone else, or deemed inappropriate for use in the certificate.

3.2 Initial Identity Validation

CSOS Registration

Application processes must be established for the identification of DEA Registrants, CSOS Coordinators and Subscriber. CSOS Coordinator and Subscriber applications and instructions can be found at DEA's web site at http://www.DEAecom.gov.

CSOS Coordinator Registration

A notarized CSOS Coordinator or DEA Registrant application must be received along with or prior to any CSOS POA certificate applications. Registrants and POAs applying as the CSOS Coordinator shall be given the option to receive a CSOS certificate on the CSOS Coordinator application form.

CSOS Subscriber Registration

CSOS Subscribers shall be DEA registrants who are listed in good standing in the CSA database, or holders of a valid power of attorney for those registrants, and shall enter into a binding agreement with the CSOS CA.

Subscriber applications are submitted to the CSOS Coordinator. The CSOS Coordinator is responsible for the initial verification of the Subscriber's identity and authorization for a CSOS certificate and submission of the application package to the CSOS RA.

Organizations not utilizing chain renewal require that the registrant, or registrant's POA, submit a duly notarized application packet to the CSOS RA. Upon receipt of the application package, the CSOS RA shall cross-reference application data with the DEA's CSA database. The PMA shall ensure that CSA database information is readily available for verification.

CSOS Subscriber Bulk Enrollment

Bulk Enrollment processes have been established to accommodate organizations that need to obtain a large volume of CSOS certificates associated with a single applicant, such as chain pharmacies utilizing centralized ordering wherein one individual has been assigned the responsibility of ordering controlled substances for delivery to multiple locations – each order requiring a Subscriber to hold a digital certificate for that DEA Registrant. In order to participate in CSOS Bulk Enrollment, an organization must currently participate in the DEA Chain Renewal program described at http://www.deadiversion.usdoj.gov/drugreg/chain_renewal.htm. This procedure 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. Each applicant (DEA Registrant, Principal Coordinator, Alternate Coordinator, and POA), will complete his/her application as specified in the above processes with the exception of how the DEA Registration and POA documentation is submitted. Enrollment instructions exist on the CSOS web site at http://www.DEAecom.gov. The CSOS RA will work with the organization's primary point of contact for bulk enrollment to ensure the DEA Registration and POA documentation are submitted correctly.

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request. This may be done by the entity using its private key to sign a value and providing that value to the CA. The CA shall then validate the signature using the party's public key. The DEA PMA may allow other mechanisms that are at least as secure as those cited here, provided the CA has specified the method in their CPS.

In the case where a key is generated directly on the party's hardware or software token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer.

If the party is not in possession of the token when the key is generated, then the token (e.g., a smart card or a Public Key Cryptography Standard (PKCS) #12 – Personal Information Exchange Syntax - encoded message) shall be delivered to the subject via an accountable method specified in the CA's CPS and approved by the DEA PMA.

When keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The CA must maintain a record of validation for receipt of the token by the subject.

3.2.2 Authentication of Organization Identity

Requests for CA certificates in the name of an organization or business shall include the organization name, address, and documentation of the existence of the organization. The RA shall verify the information in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization. The CPS shall detail the procedure used for authenticating subordinate and cross-certified CAs.

3.2.3 Authentication of Individual Identity

CSOS Subscriber certificates containing the OIDs referenced in this policy shall be issued only to individuals with controlled substance prescribing or ordering authority as previously defined in Section 1 and to CSOS Coordinators holding local registration responsibility.

All certificates and requests/upgrades are performed within 30 days.

3.2.4 Non-Verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

3.2.5.1 CSOS Coordinator Registration

A separate application process shall be established for the identification of an organization's CSOS Coordinator. The CSOS RA must receive a CSOS Coordinator application in advance of, or concurrently with, the submission of CSOS Subscriber certificate applications. CSOS Coordinators shall 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 at http://www.DEAecom.gov containing the signature of the individual who signed the most recent application for DEA Registration or the individual authorized to sign the most recent application for DEA Registration authorizing that individual 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 certificate (form 223) of the applicant or the most recent application for DEA registration.
- For individuals with POA to sign orders, a copy of the power of attorney form as specified in Code of Federal Regulations (CFR).

3.2.5.2 CSOS Subscriber Registration

Authentication of CSOS Subscriber identity shall be performed by the local organization and requires the identification of a CSOS Coordinator, who serves as the Local Registration Authority (LRA) and organizational point of contact for CSOS issues. Subscribers shall 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 this CP and has agreed to the statement of Subscriber obligations that the CA provided and acknowledging acceptance of Section 843(a)(4)(A) of Title 21, United States Code, which states that any person who knowingly or intentionally furnishes false or fraudulent information in the application is subject to imprisonment for not more than four years, a fine of not more than $30,000.00 or both;
- 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 POA to sign orders, a copy of the power of attorney form as specified in CFR.

The CSOS Coordinator shall complete Section 3 of the Subscriber's application, providing the following information in the Subscriber's packet:

- Signed Affirmation of Identity Verification in accordance with the DEA Registrant Agreement and Section 843(a)(4)(A) of Title 21, United States Code.

- The CSOS Coordinator's first and last name, signature and date signed as the individual who has performed Subscriber identity verification;
- Copies of the identification documents, application and letter assigning POA furnished by the Subscriber.

Upon receipt of the packet from the CSOS Coordinator, the CSOS RA shall validate that the application information is complete and consistent with the information received by the Registrant. All supporting documentation shall be scanned and entered into the system, including the unique identifying information from the identification documents. The CSOS RA shall also verify that the application was received from an approved CSOS Coordinator by matching the data and signatures against information in the Controlled Substance Act (CSA) database supplied by DEA and using the previously submitted CSOS Coordinator's application data and signature.

Authentication of Component Identities

CA personnel, who are not authorized to order and receive CSOS Subscriber certificates, may receive special purpose administrative certificates. These certificates shall not contain the CSOS OIDs or authorized schedule extension data referenced in this policy and shall be issued only for the purposes of signing electronic files and communications. Management of these special purpose administrative certificates will be described in the CPS. These certificates may not be used for controlled substance orders.

3.2.5.3 Device Registration

Computing and communications components (routers, firewalls, servers, Web servers, etc.) may be issued special purpose device certificates in order to secure communications with the CA. These certificates shall not contain the CSOS OIDs or authorized schedule extension data referenced in this policy.

The following OID shall be assigned to Devices which are mapped at a Medium level of assurance:

CSOS Device Certificates: dea-csos-cp ::= { 2.16.840.1.101.3.2.1.9.4}

In such cases, each component shall be named as the certificate subject and must have a human sponsor. The PKI sponsor is responsible for providing the following information:

- Equipment identification (e.g., serial number) or service name (e.g., Domain Name System (DNS) name);
- Equipment public keys;
- Equipment authorizations and attributes (if any are to be included in the certificate);

- Contact information to enable the CA or RA to communicate with the sponsor when required.

These Certificates shall be issued only to Devices under the sponsor's control (i.e., require Registration and validation that meets all issuing CA requirements, as well as requiring re-validation prior to being re-issued). In the case the Sponsor is changed, the new Individual shall review the status of each Device under his/her sponsorship to ensure it is still authorized to receive Certificates. The CA CPS shall describe procedures to ensure that Certificate accountability is maintained.

The Registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested. For Certificates at the medium Device policy, registration information shall be verified commensurate with the Medium level of assurance. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the Sponsor (using certificates of equivalent or greater assurance than that being requested), and
- In-person Registration by the Sponsor, with the identity of both the Individual and any Affiliated Organization confirmed in accordance with the requirements of Section 3.2.2 and 3.2.3.

3.2.6 Criteria for Interoperation

The FPKIPA shall determine the criteria for cross-certification with the FBCA. See also the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology Document (http://www.idmanagement.gov/criteria-and-methodology)

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

CSOS Subscriber renewal shall always result in a new certificate with a different serial number and new associated public and private keys. The CA shall notify the Subscriber 45 days prior to the expiration date of the Subscriber's certificate. The Subscriber's CSOS Coordinator may request that the CA 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 CA, continuing to qualify as a DEA registrant, CSOS POA, or agent of a DEA registrant as defined in Section 1. Electronic requests must be digitally signed using the Subscriber's or CSOS Coordinator's CSOS-issued certificate and shall be authenticated on the basis of the Subscriber's or Coordinator's digital signature using the private key for a total of two certificate re-keys. The third request shall require Subscribers to establish identity using the initial registration process described in Sections 3.2 and 4. Identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

CAs shall ensure that the Subscriber's identity information and public key are properly bound on all digital requests. Changes to a Subscriber's name, prescribing or ordering authority, or affiliation shall result in certificate revocation as specified in Section 4.

For medium Device certificates, identity may be established through the use of current signature key or using means commensurate with the strength of the certificate being requested, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.

CAs must go through the original registration process to obtain a new certificate. That CA shall notify all CAs, RAs, and Subscribers who rely on the CA's certificate that it has been changed. For self-signed ("Root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

The DEA CA key pair and certificate will not exceed the lifetimes stated in this CP. At re-key, the DEA CA will post the new public key on the web site at http://www.DEAecom.gov.

CAs will document their re-key procedures in their CPS.

3.3.2 Identification and Authentication for Re-Key After Revocation

In the event of certificate revocation due to 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 shall require that the Subscriber go through the initial registration process as specified in Sections 3.2 and 4.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated by the CA. Requests to revoke a certificate may be authenticated via manual signature, telephone call-back and security code verification or by using that certificate's associated private key to digitally sign the request, regardless of whether the private key has been compromised. Request authentication procedures must be described in the CPS. Revocation request procedures are described in Section 4.

4.0 Certificate Life-Cycle

4.1 Certificate Application

4.1.1 Submission of Certificate Application

Eligible Subscribers are those who hold a valid DEA registration as defined in Title 21 CFR Part 1300. All Subscriber applicants shall submit a completed Subscriber application obtained from the CSOS CA in accordance with this CP, entering into an initial agreement with the CA. Upon successful completion of the Subscriber identification and authentication process in accordance with this CP, the applicant shall generate a key pair and demonstrate to the CA that it is a functioning key pair as defined in the CPS.

4.1.2 Enrollment Process and Responsibilities

CSOS Subscribers may obtain Certificate application forms and instructions from http://www.deaecom.gov. The applicant will follow the procedures in the Subscriber Manual posted on the CSOS web site at http://www.deaecom.gov, mailing completed applications to:

Drug Enforcement Administration
Sterling Park Technology Center/CSOS
8701 Morrissette Drive
Springfield, VA 22152

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Upon receipt of a Subscriber's application for certificate, the CA shall confirm the Subscriber's identity against the CSA database extract supplied by DEA. The CA must ensure that this extract content is protected from unauthorized modification. To the extent practical, certificates, once created, shall be checked to ensure that all certificate fields and extensions are properly populated with the data obtained from the CSA database extract. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

4.2.2 Approval or Rejection of Certificate Applications

Using the information provided with the application, and verification against the CSA database, the CSOS RA either approves or denies the application. The CSOS RA will notify the Subscriber and the Subscriber's Coordinator via email when the application is approved. Should the application be

denied, the CSOS RA will provide notification of the application denial to the applicant and the applicant's CSOS Coordinator.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Public keys must be delivered for certificate issuance in a way that binds the entity's verified identification to their public key. In all cases, the method used for public key delivery shall be set forth in the CPS. If cryptography is used, it must be at least as strong as that employed in certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request.

Upon receipt of a Subscriber's application for certificate, the CA shall confirm the Subscriber's identity against the CSA database extract supplied by DEA. The CA must ensure that this extract content is protected from unauthorized modification. To the extent practical, certificates, once created, shall be checked to ensure that all certificate fields and extensions are properly populated with the data obtained from the CSA database extract. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

Subordinate CAs

Upon approval of a subscribing subordinate CA's CPS, the DEA CA shall process the certificate request and return a public key certificate. The subscribing subordinate CA must demonstrate the ability to generate valid Subscriber certificates by issuing a test certificate to the DEA CA. The test certificate must be revoked immediately after generation.

Hardware tokens containing subordinate CA private signature keys may be backed-up in accordance with security audit requirements defined Section 5.4.

Cross-Certified CAs

The DEA Root CA shall be issued a unilateral cross certificate from the FBCA. Upon receiving a certificate request from an approved CA, the DEA Root CA shall sign and issue a cross-certificate to the entity CA, using a secure non-electronic means. The cross-certified CA must demonstrate the ability to generate valid Subscriber certificates by issuing a test certificate to the DEA CA, which

shall be revoked immediately after generation. At this time, there are no unilateral cross certificates between the DEA Root CA and other CAs, with the exception of the FBCA.

4.3.2 Notifications to Subscriber of Certificate Issuance

Upon completion of the certificate application process, the CA shall issue the requested Subscriber certificate and notify the applicant in accordance with procedures specified in its CPS. The CA shall make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or made available for pickup by, the approved certificate applicant only. All Subscribers shall generate their own private keys, and shall not require delivery of their private keys.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

By accepting a CSOS certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate and reaffirms that he or she agrees to the terms and conditions contained in this CP definition and the applicable Subscriber Agreement.

4.4.2 Publication of the Certificate by the CA

Each CA shall ensure that there is a repository where the DEA CA certificate and revocation lists are published and available for status checking. CSOS Subscriber certificates shall not be made publicly available. The repository shall be an X.500 compliant directory with the Lightweight Directory Access Protocol (LDAP) access. The CA shall assert a high level of reliability and availability of the repository. ARLs and CRLs must be published in accordance with this CP. The DEA CA shall publish this CP on DEA's web site at http://www.DEAecom.gov. All CAs shall make this CP publicly available either in an online repository or a web site that is available to Subscribers and Relying Parties.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
- A copy of this CP

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA CA repository.

Subscriber certificates shall not be made publicly available in the repository.

4.5 Key Pair and Certificate Usage

CSOS certificates are appropriate for use with other applications requiring a Medium level of assurance or below, as defined by the FBCA. This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

4.5.1 Subscriber Private Key and Certificate Usage

CSOS Subscriber certificates shall only be 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. CSOS certificates may **not** be used for the signing of electronically transmitted controlled substance prescriptions.

In all cases, prior to releasing or publishing a CSOS certificate, the CA shall ensure that the Subscriber named in the certificate has signed a Subscriber Agreement agreeing to be bound by this CP as a Subscriber and obligating the Subscriber to:

- Protect their private key in accordance with this CP and as stipulated in their certificate acceptance agreement, taking all reasonable measures to prevent its loss, disclosure, modification, or unauthorized use;
- Acknowledge that by accepting the certificate, the Subscriber is warranting that all information and representations made by the Subscriber included in the certificate are true;
- Use the certificate only for authorized and legal purposes, consistent with this CP;
- Notify the issuing CA in accordance this CP if they suspect that their private key is compromised or lost;
- Abide by all terms, conditions, and restrictions levied upon the use of their private keys and certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are responsible for performing checks for validity of each digitally signed prescription as required by applicable federal and state regulations. Relying parties are responsible for examining the CP to understand all of their rights and obligations under the CP.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

CSOS Subscriber renewal shall always result in a new certificate with a different serial number and new associated public and private keys. CSOS Subscriber certificates will not be re-keyed or modified. The validity period of the certificate must meet the requirements specified in Section 6.3.2.

The CA shall notify the Subscriber 45 days prior to the expiration date of the Subscriber's certificate.

4.6.2 Who May Request Renewal

The Subscriber's CSOS Coordinator may request that the CA 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 CA, continuing to qualify as a DEA registrant, CSOS POA, or agent of a DEA registrant as defined in Section 1.

4.6.3 Processing Certificate Renewal Requests

CAs shall ensure that the Subscriber's identity information and public key are properly bound on all digital requests. Changes to a Subscriber's name, prescribing or ordering authority, or affiliation shall result in certificate revocation as specified in Section 4.

CAs must go through the original registration process to obtain a new certificate. That CA shall notify all CAs, RAs, and Subscribers who rely on the CA's certificate that it has been changed. For self-signed ("Root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

The DEA CA key pair and certificate will not exceed the lifetimes stated in this CP. At re-key, the DEA CA will post the new public key on the web site at http://www.DEAecom.gov.

CAs will document their re-key procedures in their CPS.

4.6.4 Notification of New Certificate Issuance to Subscriber

Upon receipt of a Subscriber's application for certificate, the CA shall confirm the Subscriber's identity against the CSA database extract supplied by DEA. The CA must ensure that this extract content is protected from unauthorized modification. To the extent practical, certificates, once created, shall be checked to ensure that all certificate fields and extensions are properly populated with the data obtained from the CSA database extract. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

Upon completion of the certificate application process, the CA shall issue the requested Subscriber certificate and notify the applicant in accordance with procedures specified in its CPS. The CA shall make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or made available for pickup by, the approved certificate applicant only. All Subscribers shall generate their own private keys, and shall not require delivery of their private keys.

Public keys must be delivered for certificate issuance in a way that binds the entity's verified identification to their public key. In all cases, the method used for public key delivery shall be set forth in the CPS. If cryptography is used, it must be at least as strong as that employed in certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

By accepting a CSOS certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate and reaffirms that he or she agrees to the terms and conditions contained in this CP definition and the applicable Subscriber Agreement.

4.6.6 Publication of the Renewal Certificate by the CA

Each CA shall ensure that there is a repository where the DEA CA certificate and revocation lists are published and available for status checking. CSOS Subscriber certificates shall not be made publicly available. The repository shall be an X.500 compliant directory with the LDAP access. The CA shall assert a high level of reliability and availability of the repository. ARLs and CRLs must be published in accordance with this CP. The DEA CA shall publish this CP on DEA's web site at http://www.DEAecom.gov. All CAs shall make this CP publicly available either in an online repository or a web site that is available to Subscribers and Relying Parties.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
- A copy of this CP

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA CA repository.

Subscriber certificates shall not be made publicly available in the repository.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

The Subscriber's CSOS Coordinator may request that the CA issue a new certificate with a new key pair, if the public key has not reached the end of its validity period, the original certificate has not been revoked, the Subscriber name and attributes are unchanged, and the Subscriber is in good standing with the CA, continuing to qualify as a DEA registrant, CSOS POA, or agent of a DEA registrant as defined in Section 1. Electronic requests must be digitally signed using the Subscriber's or CSOS Coordinator's CSOS-issued certificate and shall be authenticated on the basis of the Subscriber's or Coordinator's digital signature using the private key for a total of two certificate re-keys. The third request shall require Subscribers to establish identity using the initial registration process described in Sections 3.1 and 4. Identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

CAs shall ensure that the Subscriber's identity information and public key are properly bound on all digital requests. Changes to a Subscriber's name, prescribing or ordering authority, or affiliation shall result in certificate revocation as specified in Section 4.

CAs must go through the original registration process to obtain a new certificate. The new public key will be posted on the web site, http://www.deaecom.gov and notification of the re-key and change will be conveyed to CSOS coordinators in a secure fashion to preclude malicious substitution attacks.

The DEA CA key pair and certificate will not exceed the lifetimes stated in this CP. At re-key, the DEA CA will post the new public key on the web site at http://www.DEAecom.gov.

CAs will document their re-key procedures in their CPS.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber's CSOS Coordinator may request that the CA 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 CA, continuing to qualify as a DEA registrant, CSOS POA, or agent of a DEA registrant as defined in Section 1. Electronic requests must be digitally signed using the Subscriber's or CSOS Coordinator's CSOS-issued certificate and shall be

authenticated on the basis of the Subscriber's or Coordinator's digital signature using the private key for a total of two certificate re-keys. The third request shall require Subscribers to establish identity using the initial registration process described in Sections 3.2 and 4. Identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

CSOS Subscribers may obtain Certificate application forms and instructions from http://www.DEAecom.gov. The applicant will follow the procedures in the Subscriber Manual posted on the CSOS web site at http://www.DEAecom.gov, mailing completed applications to the Drug Enforcement Administration, Sterling Park Technology Center/CSOS, 8701 Morrissette Drive, Springfield, VA 22152. Using the information provided with the application, and verification against the CSA database, the CSOS RA either approves or denies the application. The CSOS RA will notify the Registrant and the Registrant's CSOS Coordinator when the application is received via email when the application is received. Should the application be denied, the CSOS RA will provide notification of the application denial to the applicant and the applicant's CSOS Coordinator.

4.7.3 Processing Certificate Re-Keying Requests

CAs shall ensure that the Subscriber's identity information and public key are properly bound on all digital requests. Changes to a Subscriber's name, prescribing or ordering authority, or affiliation shall result in certificate revocation as specified in Section 4.

CAs must go through the original registration process to obtain a new certificate. That CA shall notify all CAs, RAs, and Subscribers who rely on the CA's certificate that it has been changed. For self-signed ("Root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

The DEA CA key pair and certificate will not exceed the lifetimes stated in this CP. At re-key, the DEA CA will post the new public key on the web site at http://www.DEAecom.gov.

CAs will document their re-key procedures in their CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

Upon receipt of a Subscriber's application for certificate, the CA shall confirm the Subscriber's identity against the CSA database extract supplied by DEA. The CA must ensure that this extract content is protected from unauthorized modification. To the extent practical, certificates, once created, shall be checked to ensure that all certificate fields and extensions are properly populated with the data obtained from the CSA database extract. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

Upon completion of the certificate application process, the CA shall issue the requested Subscriber certificate and notify the applicant in accordance with procedures specified in its CPS. The CA shall

make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or made available for pickup by, the approved certificate applicant only. All Subscribers shall generate their own private keys, and shall not require delivery of their private keys.

Public keys must be delivered for certificate issuance in a way that binds the entity's verified identification to their public key. In all cases, the method used for public key delivery shall be set forth in the CPS. If cryptography is used, it must be at least as strong as that employed in certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

By accepting a CSOS certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate and reaffirms that he or she agrees to the terms and conditions contained in this CP definition and the applicable Subscriber Agreement.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Each CA shall ensure that there is a repository where the DEA CA certificate and revocation lists are published and available for status checking. CSOS Subscriber certificates shall not be made publicly available. The repository shall be an X.500 compliant directory with the LDAP access. The CA shall assert a high level of reliability and availability of the repository. ARLs and CRLs must be published in accordance with this CP. The DEA CA shall publish this CP on DEA's web site at http://www.deaecom.gov. All CAs shall make this CP publicly available either in an online repository or a web site that is available to Subscribers and Relying Parties.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
  A copy of this CP

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA CA repository.

Subscriber certificates shall not be made publicly available in the repository.

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. CAs must update Subscriber certificates whose characteristics have changed due to changes in name, affiliation, or prescribing or order authority, as indicated in the daily CSA extracts received from DEA. The old certificate must be 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 CSA database that is verified by DEA daily through the review of a printed list of Registrant changes.

4.8.2 Who May Request Certification Modification

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

4.8.3 Processing Certificate Modification Requests

The DEA CSOS Operational Authority shall perform 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 Management Authority. Changes may be made for the following reasons:

- Modification of the subjectInformationAccess (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

Upon receipt of a Subscriber's application for certificate, the CA shall confirm the Subscriber's identity against the CSA database extract supplied by DEA. The CA must ensure that this extract content is protected from unauthorized modification. To the extent practical, certificates, once created, shall be checked to ensure that all certificate fields and extensions are properly populated with the data obtained from the CSA database extract. This may be done through software that

scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

Upon completion of the certificate application process, the CA shall issue the requested Subscriber certificate and notify the applicant in accordance with procedures specified in its CPS. The CA shall make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or made available for pickup by, the approved certificate applicant only. All Subscribers shall generate their own private keys, and shall not require delivery of their private keys.

Public keys must be delivered for certificate issuance in a way that binds the entity's verified identification to their public key. In all cases, the method used for public key delivery shall be set forth in the CPS. If cryptography is used, it must be at least as strong as that employed in certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

By accepting a CSOS certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate and reaffirms that he or she agrees to the terms and conditions contained in this CP definition and the applicable Subscriber Agreement.

4.8.6 Publication of the Modified Certificate by the CA

Each CA shall ensure that there is a repository where the DEA CA certificate and revocation lists are published and available for status checking. CSOS Subscriber certificates shall not be made publicly available. The repository shall be an X.500 compliant directory with the LDAP access. The CA shall assert a high level of reliability and availability of the repository. ARLs and CRLs must be published in accordance with this CP. The DEA CA shall publish this CP on DEA's web site at http://www.deaecom.gov. All CAs shall make this CP publicly available either in an online repository or a web site that is available to Subscribers and Relying Parties.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
- A copy of this CP

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA CA repository.

Subscriber certificates shall not be made publicly available in the repository.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the Subscriber and the Subscriber's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- An audit indicating that the CSOS CA has violated stipulations of this CP, or its CPS. CSOS Subscriber certificates may not be revoked, however suspension of new certificates may be directed by the PMA until audit discrepancies are resolved;
- It can be demonstrated that the Subscriber has violated the stipulations of the Subscriber Agreement;
- Identifying information or affiliation components of any names in the certificate become invalid or organizational affiliation terminates relationship with the DEA;
- Privilege attributes (prescribing or ordering authority) asserted in the Subscriber's certificate are reduced;
- The private key is lost or cannot be accessed for any reason; or compromise is suspected;
- 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;
- DEA posts notice in their daily extract of CSA data that the certificate holder's DEA Registration has been revoked, suspended or restricted, that the Registration information has changed, or that the Registration has been terminated.

CAs who issue CSOS Subscriber certificates are required to validate Subscribers against the daily CSA extract provided from DEA to determine if changes to the DEA Registration information warrant revocation. The following revocation processing times shall apply:

Table 1: Revocation Processing Frequency

Revocation Reason	Revocation Must Occur Within:
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.
CSA Extract Data: DEA Registration changes to the physical location or reductions to the controlled substance schedules that the Registration is authorized to order	18 hours from receipt of CSA data
CSA Extract Data: DEA Registration name change (company name), DEA Registration mailing addresses (not physical addresses); or additions to the controlled substance schedules the Registration is authorized to order During this 60-day period, the certificate status shall remain 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, whichever event occurs first.	60 days from receipt of CSA data
Revocation for reasons other than those stated above.	18 hours of the receipt of an authenticated revocation request.

CRL issuance times must be in accordance with Section 4.9.5 of this CP. CAs must describe their process for validating existing Subscribers against the daily CSA database extract in their CPS.

Circumstances for Revocation of Subordinate CA Certificates

Circumstances under which a CA certificate or cross-certificate to an approved DEA CA can be revoked include: 1) upon the direction of the CSOS System PMA, 2) upon an authenticated request by a previously designated authorized official of the CA's organization (such officials must be designated in the MOA between DEA and the organization or outlined in the organization's CPS), or 3) when the CSOS System PMA determines that an emergency has occurred that may impact the integrity of the certificates issued by the CSOS System.

In the event that the CA ceases operations, any certificate issued to the CA, and all certificates issued by the CA, must be revoked prior to the date that the CA ceases operations.

4.9.2 Who Can Request Revocation

A Subscriber, the PMA, or other DEA-approved entity may request revocation of the Subscriber's certificate at any time for any reason. A Registrant may request revocation of the certificate of its agent at any time, for any reason. The issuing CA may also revoke a Subscriber's certificate upon the failure of the Subscriber (or the Sponsor, where applicable) to meet its obligations under this CP or any other agreement, regulation, or law applicable to the certificate that may be in force.

4.9.3 Procedure for Revocation Request

A certificate revocation request shall identify the certificate to be revoked and provide the reason for its revocation. If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the revocation request must so indicate. Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. All revocation requests shall be authenticated as described in the CA's CPS. Electronic requests may be authenticated using the digital signature of the requestor. CSA extract information is considered authenticated at the time the file is distributed to the CSOS RA.

CA Certificate Revocation

Revocation of a CA's certificate shall take effect upon the publication of status information in the ARL. Upon revocation, the CA (e.g., DEA CA) shall immediately generate and publish status information in the ARL identifying the certificate being revoked and the reason for its revocation. A CA certificate that is revoked shall remain on the ARL until the certificate expires.

Subscriber Certificate Revocation

In all instances, if a Subscriber leaves an organization, DEA requires that the CA be immediately notified so that all certificates associated with the Subscriber can be revoked. Revocation of Subscriber certificates shall take effect upon the publication of status information identifying the reason for the revocation within the time limits specified in Section 4.9.5.

A Subscriber shall, upon ceasing its relationship with an organization that sponsored the certificate, prior to departure, or upon revocation of a certificate associated with a hardware cryptographic token, surrender to that organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

CSOS Subscriber Certificates

Relying Parties are permitted under Title 21 CFR 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. In order to ensure that a revoked certificate that has expired within this 60-day time frame is not

accepted, the CA shall continue to maintain Subscriber certificate revocation information on its CRL for a minimum period of **60 days beyond** certificate expiration.

4.9.4 Revocation Request Grace Period

The Subscriber must immediately notify their CSOS Coordinator and CSOS RA when a key compromise is detected, suspected, or when discovered risk is determined to warrant revocation.

4.9.5 Time Within Which CA Must Process the Revocation Request

The DEA CSOS CA will revoke certificates as quickly as practical upon receipt of a proper revocation request as described in this section. Revocation requests shall be 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 shall be processed before the following CRL is published. Revocation processing times are listed in Section 4.9.1.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties must validate every CSOS certificate received in connection with a transaction against a valid and unexpired CRL as required by applicable federal and state regulations. Certificates shall include pointers to CRLs identified in the certificate's cRLDistributionPoints extension field. CRLs and ARLs may be cached and relied upon until they expire, unless otherwise notified by the PMA. In the event that the DEA CA or CSOS CA is unable to publish its revocation list as described in this CP, the Help Desk will provide notification to all affected CSOS Coordinators using either email or a phone call. CSOS Coordinators must perform a callback to the Help Desk to authenticate the message. This notification will also be posted to the DEA web site at www.deaecom.gov, accessible to all Relying Parties. Notification via email or telephone call will also be provided by the Help Desk to CSOS Coordinators when CRL service has been restored after an interruption of greater than 24 hours.

4.9.7 CRL Issuance Frequency

Only the DEA CA is authorized to issue CA certificates under this policy. The DEA CA that issues CA certificates shall be operated in an off-line manner. The DEA CA shall publish CRLs for all certificates for all assurance levels. ARLs and CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. The CSOS CA shall publish a complete CRL within 4 hours of generation. The DEA CA shall publish a complete Authority Revocation List (ARL) every 31 days or sooner, even if there are no changes to be made.

4.9.8 Maximum Latency for CRLs

In the event of key compromise, CRLs/ARLs containing the newly revoked certificate information shall be published within 6 hours of authenticated notification. In the event of CA certificate revocation, the CSOS System shall notify all other CAs via a digitally signed email and shall issue an emergency ARL.

Superseded certificate status information shall be 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

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
- A copy of this CP

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA CA repository.

4.9.10 On-Line Revocation Checking Requirements

Relying parties must validate every CSOS certificate received in connection with a transaction against a valid and unexpired CRL as required by applicable federal and state regulations. Certificates shall include pointers to CRLs identified in the certificate's cRLDistributionPoints extension field. CRLs and ARLs may be cached and relied upon until they expire, unless otherwise notified by the PMA. In the event that the DEA CA or CSOS CA is unable to publish its revocation list as described in this CP, the Help Desk will provide notification to all affected CSOS Coordinators using either email or a phone call. CSOS Coordinators must perform a callback to the Help Desk to authenticate the message. This notification will also be posted to the DEA web site at www.deaecom.gov, accessible to all Relying Parties. Notification via email or telephone call will also be provided by the Help Desk to CSOS Coordinators when CRL service has been restored after an interruption of greater than 24 hours.

4.9.11 Other Forms of Revocation Advertisement Available

CAs may use Online Certificate Status Protocol (OCSP), to distribute status information in addition to CRLs, provided:

- OCSP provides authentication and integrity services commensurate with the Assurance Level of the Certificate being verified.
- The latency of certificate status information and publishing frequency meets or exceeds the requirements for CRLs as stated in Section 4.9.7 and Section 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

In the event of certificate revocation due to 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 shall require that the Subscriber go through the initial registration process as specified in Sections 3.1 and 4.

4.9.13 Circumstances for Suspension

Certificate suspension is allowable under the following conditions:

- As a result of a discrepancy reported in compliance audit of a subordinate or cross-certified 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.

4.9.14 Who Can Request Suspension

Only the PMA, CSOS RA, or other DEA-authorized entity may request certificate suspension under the circumstances discussed in Section 4.9.13.

4.9.15 Procedure for Suspension Request

The DEA PMA may request the suspension, rather than revocation, of a Subscriber's certificate at their discretion. CSOS Subscriber certificate suspension requests will be made to the CSOS System Help Desk via the Technology Section Chief or the CSOS Program Manager.

Certificate suspension will be supported by including the suspended certificate in the CA's ARL or CRL. The CRL shall use the CRLReason code specified as 'certificateHold'.

4.9.16 Limits on Suspension Period

The suspended certificate shall remain on the CA's ARL or CRL until the PMA makes the request through the DEA CSOS System Help Desk that the certificate should no longer be suspended. Requests to remove a certificate from suspension must be authenticated.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

The information in the DEA CA directory shall be publicly available through the Internet. There shall be no access controls on the reading of this CP. CAs shall implement appropriate access controls restricting who can write or modify policies, certificates, certificate status or ARLs/CRLs. Access to Subscriber certificates located in the repositories is restricted to CA personnel. Subscriber certificates shall not be made publicly available in the CSOS repository.

4.10.3 Optional Features

Each CA shall publish the following information to either an online repository or a web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
- A copy of this CP

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA CA repository.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Under no circumstances shall a subscriber's signature key be held by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

All CA equipment including CA cryptographic modules shall be protected from unauthorized access at all times.

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

CA equipment, as well as hardware, shall be protected from unauthorized access. The computer room housing the CA shall require two-factor authentication to access the room. Electronic monitoring shall be used to protect against unauthorized intrusion at all times. Access to the CA and cryptographic modules, which reside in a locked server cabinet, shall require 2 person physical access control. A CA access log shall be maintained to record names of individuals who unlock and access the CA cabinet and shall be inspected periodically by the Security Officers. Unescorted access to the computer room shall be limited to authorized personnel. Unescorted access to the CA cabinet shall be limited to authorized personnel and must comply with the two person required rule. RA staff shall be escorted by individuals who are allowed unescorted access. Security officers shall be identified to provide oversight to operations providing an additional level of security within the space. A visitor's access log shall be maintained at the facility entrance and must be signed by all approved visitors.

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

Two-factor authentication (e.g., badge + PIN) shall be required by authorized employees to gain access to the CA space. A CA access log shall be maintained and record names of individuals who unlock and access the CA cabinet. The Security Officer shall perform periodic reviews of both the CA access log and visitor's access log.

In the unforeseen event that all personnel must vacate the facility for an extended period of time, the Security Officer on duty will perform 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 shall be 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 shall indicate the date and time and an assertion that "all necessary physical protection mechanisms are in place and activated." Upon returning to the facility, the Security Officer shall check the automatic card-key logs upon returning to ensure that unauthorized entry did not occur during that period.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.3 Power and Air Conditioning

The temperature in the CA room shall be maintained at 69 +/-2 degrees. There shall be air-conditioning systems capable of supporting the temperature requirements. The uninterruptible power supply system will ensure that the temperature is appropriately maintained in the facility in the event of a power outage. The CA shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

CA equipment shall be 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 shall be high and the fire protection and suppression facilities available to the building shall be rated to a level where the risk of substantial destruction as a result of fire of the equipment located in the building shall be low.

5.1.6 Media Storage

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, CA media, and CA equipment shall be placed in secure containers and protected from

unauthorized physical access. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

5.1.7 Waste Disposal

CA storage media and devices containing storage media shall be inspected to ascertain if they contain sensitive data prior to disposal or reuse. Items found to contain sensitive information must be 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 must be physically destroyed. Storage media used by the CA shall be protected from environmental threats of temperature, humidity and magnetism.

5.1.8 Off-site backup

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

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

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role shall 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 shall be divided between multiple roles and individuals.

The people selected to fill these roles must be 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 shall be taken to increase the likelihood that these roles can be successfully carried out. The first shall ensure that the person filling the role is trustworthy and properly trained. The second shall distribute functions among more than one person, so that any malicious activity would require collusion. The primary trusted roles defined in this policy will be 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 may have different name designations for these roles, it is expected that

the separation and distribution of functions shall be consistent with this policy and shall be employed at all CA and RA locations.

5.2.1.1 Administrator

The Administrator (e.g., CA Operator) role shall be 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 shall have no part in Subscriber certificate adjudication and adequate controls shall be in place to prevent the CA Operator from issuing unauthorized Subscriber certificates.

5.2.1.2 Officer

The Officer (e.g., RA Operator) role and corresponding procedures shall be defined in the CPS. The officer role shall be 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.

5.2.1.3 Auditor

The Auditor (e.g., Security Officer) role shall be 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.

5.2.1.4 Operator

The Operator (e.g., System Administrator) role shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Shareholders

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

5.2.1.6 Other Trusted Roles

The CPS shall list 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 shall be 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 shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access shall not be 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 shall be attained as required in Section 5.1.2.

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Separation of Roles

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals shall only assume one of the RA Operator (Officer), CA Operator (Administrator), Security Officer (Auditor), but any individual may assume the System Administrator (Operator) role. The CA system shall identify and authenticate its users and shall ensure 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 shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

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

All CA personnel shall:

- Not be assigned other duties that would interfere with their regular duties and responsibilities;
- Not knowingly been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be 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 personnel shall be required to undergo a DEA Sensitive background investigation. All background checks shall be performed by DEA in accordance with DEA Personnel Security Policies and shall be performed at the time an offer is extended to the applicant. Positions shall be contingent on DEA acceptance and successful clearance adjudication. All Certification Authority personnel must be U.S. Citizens.

DEA ensures that it assigns a risk designation to all positions and establishes screening criteria for individuals filling these positions in accordance with DOJ 2610.2A.

DOJ Order 2610.2A establishes a screening criteria for individuals filling organizational positions. Policy requires that all positions be reviewed in terms of their sensitivity.

5.3.3 Training Requirements

CA employees must 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 must be an ongoing and documented process. Any significant change to CA operations shall have a training (awareness) plan, and the execution of this plan shall be documented. Documentation shall be maintained identifying all personnel who received training and the type of training completed.

Personnel performing duties with respect to the operation of a CA shall 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 shall be aware of changes in the DEA CSOS CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes: DEA CSOS CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be 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 Technology Section Chief or Program Manager may suspend 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 CP or the CPS whether through negligence or with malicious intent, is subject to privilege revocation, administrative discipline, and/or criminal prosecution.

5.3.7 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 shall be revoked upon receipt of termination documentation to ensure system integrity.

5.3.8 Independent Contractor Requirements

Contractor personnel acting as representatives of DEA, employed to operate any part of the DEA CA and CSOS CA, shall be subject to the same personnel requirements as set forth in this CP. Contractor personnel must also undergo the same background checks as

U.S. Government personnel, and shall be cleared to the level of the role performed.

5.3.9 Documentation Supplied to Personnel

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

5.3.10 Personnel Security Controls for End Entities

In addition to the CP, Subscribers shall be provided with information on the use and protection of the software used within CSOS domain. The CA shall provide 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 shall log operational events pertaining to Subscriber enrollment and certificate management. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. The specific procedures for auditing the system shall be stated in the CPS.

The CA shall record 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 shall be enabled. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- Type of event;
- 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 must include the message date and time, source, destination, and contents.

Procedures specifying integrity controls, event record lifetime and event record access shall be implemented and maintained. The audit log should be 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 must be performed regularly and follow up actions must be taken for suspicious events or omissions.

Detailed audit requirements are listed below:

SECURITY AUDIT:

- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Obtaining a third-party time-stamp

IDENTIFICATION AND AUTHENTICATION:

- Successful and unsuccessful attempts to assume a role
- The value of maximum authentication attempts is changed
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from password to biometrics

LOCAL DATA ENTRY:

- All security-relevant data that is entered in the system

REMOTE DATA ENTRY:

- All security-relevant messages that are received by the system

DATA EXPORT AND OUTPUT:

- All successful and unsuccessful requests for confidential and security-relevant information

KEY GENERATION:

- Whenever the CA generates a key (not mandatory for single session or one-time use symmetric keys)

PRIVATE KEY LOAD AND STORAGE:

- The loading of Component private keys
- All access to certificate subject private keys retained within the CA for key recovery purposes

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:

- All changes to the trusted public keys, including additions and deletions

SECRET KEY STORAGE:

- The manual entry of secret keys used for authentication

PRIVATE AND SECRET KEY EXPORT:

- The export of private and secret keys (keys used for a single session or message are excluded)

CERTIFICATE REGISTRATION:

- All certificate requests

CERTIFICATE REVOCATION:

- All certificate revocation requests

CERTIFICATE STATUS CHANGE APPROVAL:

- The approval or rejection of a certificate status change request

CA CONFIGURATION:

- Any security-relevant changes to the configuration of the CA

ACCOUNT ADMINISTRATION:

- Roles and users are added or deleted
- The access control privileges of a user account or a role are modified

CERTIFICATE PROFILE MANAGEMENT:

- All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT

- All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Appointment of an individual to a Trusted Role
- Designation of personnel for multiparty control
- Installation of the Operating System
- Installation of the CA
- Installing hardware cryptographic modules
- Removing hardware cryptographic modules
- Destruction of cryptographic modules
- System Startup
- Logon Attempts to CA Apps
- Receipt of Hardware / Software
- Attempts to set passwords
- Attempts to modify passwords

- Backing up CA internal database
- Restoring CA internal database
- File manipulation (e.g., creation, renaming, moving)
- Posting of any material to a repository
- Access to CA internal database
- All certificate compromise notification requests
- Loading tokens with certificates
- Shipment of Tokens
- Zeroizing tokens
- Rekey of the CA
- Configuration changes to the CA server involving:
    - Hardware
    - Software
    - Operating System
    - Patches
    - Security Profiles

PHYSICAL ACCESS / SITE SECURITY

- Personnel Access to room housing CA
- Access to the CA server
- Known or suspected violations of physical security

ANOMALIES

- Software Error conditions
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure
- Obvious and significant network service or access failures
- Violations of Certificate Policy
- Violations of Certification Practice Statement
- Resetting Operating System clock

5.4.2 Frequency of Processing Log

The CA shall establish 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 shall be 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 shall be 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 shall be documented.

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

5.4.3 Retention Period for Audit Log

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

The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key. These audit logs shall be made available during compliance audits.

5.4.4 Protection of Audit Log

CA system configuration and procedures must be implemented together to ensure that only authorized persons read, archive or delete security audit data. The entity performing security audit data archive shall not have modify access. Procedures must be implemented to protect archived data from disclosure, deletion, modification or destruction prior to the end of the security audit data retention period. CA systems must be 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 shall be backed up at least monthly. Adequate backup procedures must be 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 shall be 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 may be internal or external to the CA system. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the CA shall cease operations except for revocation processing until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

Operational staff shall perform self-assessments of the security controls at the time of initial installation and configuration of the CSOS System PKI components. Periodic vulnerability

assessments shall be 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 Assessments

Vulnerability assessments shall be 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 shall be 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 Events Archived

CA archive records shall be 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 shall be recorded for archive:

- CA accreditation (if applicable);
- Certificate Policy;
- Certification Practice Statement;
- Compliance Auditor Reports;
- 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;
- All certificate compromise notifications
- Subscriber Identity Authentication data as per Section 3.1;
- Subscriber Agreements
- Documentation of receipt and acceptance of certificates;
- Documentation of receipt of tokens;
- All certificates issued or published;
- Record of Entity CA Re-key;
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All ARLs and CRLs issued and/or published;
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited

- Any attempt to delete or modify the Audit logs
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement
- 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 shall be retained and protected against modification or destruction for a period specified in the CPS, at least ten years & six months (Medium Assurance). Applications required for processing the archive data shall also be 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 shall be defined by the archive site. Alternatively, data may be retained using procedures that have been approved by the U.S. National Archives and Records Administration (NARA) for that category of documents.

5.5.4 Archive Backup Procedures

CA backup procedures must be in place and shall be sufficiently detailed to establish the proper operation of the CA, or validity of any certificate (including those revoked or expired) issued by the CA in accordance with the CA Operations Guide.

5.5.5 Requirements for Time-Stamping of Records

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

Asserted times shall be accurate. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.5.1.

5.5.6 Archive Collection System (Internal vs. External)

No Stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

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

Procedures detailing how to create, verify, package, transmit, and store CA archives shall be published in the CA's CPS. Only authorized personnel shall be permitted to access the archive.

5.6 Key Changeover

CA keys shall be changed while sufficient life remains on the certificate to allow uninterrupted validity of all Subscribers. If keys must be changed due to changes in software or hardware, the current keys shall be maintained for a sufficient period to allow uninterrupted validity of all subordinate subjects. New keys shall be 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 shall be 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 shall reestablish 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 DEA CSOS CA shall respond 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 shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.8.
- If the CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event the CSOS CA private key is compromised, the CSOS CA will implement the *CSOS System Key Compromise Plan*. A summary of steps that shall be followed include:

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

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

5.7.4 Business Continuity Capabilities After a Disaster

The CA shall have in place an appropriate contingency plan, disaster recovery plan, or business resumption plan 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 shall be 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 shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. The CA shall address long-term interruption restoration procedures in its CPS and Contingency Plan.

Recovery/resumption plans shall be 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 shall identify 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 shall be easily accessible in the event of an emergency.

5.8 CA and RA Termination

In the event of CSOS CA termination (e.g., disaster where CA installation is physically damaged), the PMA shall oversee the termination process. The CA Help Desk staff shall work 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 shall be revoked no later than the time of termination. Prior to CA termination, all archived data shall be 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.

6.0 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 Root or Subordinate CAs shall be generated in FIPS 140 validated cryptographic modules. For DEA CA, the modules shall meet or exceed Security Level 2.

CA key pair generation must create a verifiable audit trail that verifies that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

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 need not be restarted but may continue.

6.1.1.2 Subscriber Key Pair Generation

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

For Medium assurance, either validated software or validated hardware cryptographic modules shall be used for key generation.

6.1.2 Private Key Delivery to Subscriber

Private keys shall not be transferred or exchanged. All entities shall generate their own private keys, and shall not require delivery.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's public key must be 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 shall be delivered to end entities in a secure fashion. The new public key may be 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 shall post the certificate it issues in the CA repository or CA web site.

6.1.5 Key Sizes

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

The DEA CA and subordinate or cross-certified CA signature keys must be 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 shall use Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186-2. Signatures on certificates and CRLs that are issued after 12/31/13 shall be generated using SHA-256.

Subscriber keys that expire before 12/31/08 must be at least 1024 bit RSA with a FIPS 186-2 approved hashing function. Subscriber keys that expire on or after 12/31/08 shall 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 shall 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 this CP shall 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) shall be generated in accordance with FIPS 186-2.

Parameter quality checking (including testing for prime numbers) shall be 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 must only be used for digital signature and non-repudiation; CA signing keys may also be used for certificate and CRL signing as specified in the *CSOS 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, the DEA Root CA, Subordinate CA or cross-certified CA cryptographic modules must be validated to at least the latest version of FIPS 140 series - Level 2 (Hardware).

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

6.2.2 Private Key Multi-Person Control

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

6.2.3 Private Key Escrow

Under no circumstances shall a key used to support non-repudiation services be escrowed by a third party.

6.2.4 Private Key Backup

CA private signature keys shall be backed up under the same multi-person control as the original signature key. Such backup shall create only a single copy of the signature key at the CA location; a second copy may be 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 shall be included in the CPS.

Backup of the Subscriber's private key may be backed up or copied, but must be held in the Subscriber's control.

Device private keys may be backed up or copied, but must be held under the control of the device's human sponsor or other authorized administrator.

6.2.5 Private Key Archival

Subscriber private signature keys shall not be archived or escrowed. See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The CA signing private key pair shall be generated and handled by cryptographic modules in a manner compliant with a minimum FIPS 140-1 level 2 (Hardware).

6.2.7 Private Key Storage on Cryptographic Module

The CA signing private key pair shall be generated and handled by cryptographic modules in a manner compliant with FIPS 140-1 level 2 (Hardware).

Backed up subscriber private signature keys shall not be stored in plain text form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the device's cryptographic module.

6.2.8 Method of Activating Private Keys

Authorized personnel shall log on to the CA systems to activate CA private signing keys in accordance with Section 5.2. The means of authentication shall be dual-factor and shall be described in the CPS. 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 shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

CSOS Subscribers must be 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 shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Keys

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

6.2.10 Method of Destroying Private Keys

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

Subscriber private signature keys shall be 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 6.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The CSOS CA must not issue subscriber certificates that extend beyond the expiration date of their own certificate and public keys. The usage period for a CA key pair is a maximum of six years. CA private keys may be used to generate certificates for the first half of the usage period (3 years), and the public key may be used to validate certificates for the entire usage period. If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.

Subscriber certificates shall expire upon the expiration of the Subscriber's DEA registration and shall be limited to a maximum of three years. Subscribers must 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 shall be 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, shall be generated in conformance with FIPS112 and shall result in a high level of strength for the keys or data to be protected. CAs shall document their rules on password selection in their CPS.

Subscriber activation data must be user selected and be generated in conformance with FIPS-112. If the activation data must be transmitted, it shall be 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 shall be 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 shall never be shared. The protection mechanisms for CAs shall be described in their CPS.

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

associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

The CA activation data protection mechanism shall include 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 may be provided by the operating system or through a combination of operating system, software, and physical safeguards and must be outlined in a CA Security Plan. The CA operating system shall enforce the identification, authentication, auditing, and separation of roles of all users. A secure logon process shall be used to access the CA's systems. An access control policy and an account management process shall be 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 must be implemented and must be kept current. This is an ongoing task. Procedures must exist to address prevention, removal, recovery, and documentation.

Subscriber System Security Controls: The system must employ an inactivity time-out period of no greater than ten minutes after which the certificate holder must re-authenticate 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 shall use software that has been designed and developed under a formal, documented development methodology. Hardware and software procured to operate the CA shall be 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 shall be developed in a controlled environment, and the development process shall be defined and documented. The CA shall demonstrate that security requirements were achieved through a combination of software

verification & validation, structured development approach, and controlled development environment.

Where open source software has been utilized, the CA/RA shall demonstrate that security requirements were achieved through software verification & validation and structured development/lifecycle management.

All hardware must be 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, must be thoroughly tested on a separate platform for functionality and vulnerabilities prior to being implemented on operational systems. Operational systems must be physically and logically separate from developmental systems and systems used for testing software patches and updates to maintain integrity of services provided. Risks must be examined as a part of the configuration management process and vulnerability assessments must be 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 shall be developed during testing on isolated systems.

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

6.6.2 Security Management Controls

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

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

6.6.3 Life Cycle Security Ratings

See Section 6.6.1.

6.7 Network Security Controls

CAs, RAs, and CA Directories shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Access to unused ports and services must be denied to prevent misuse. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. Users shall be 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 must be refused. Dial-up or external access to the CA via system administration interface is prohibited. External threats shall be 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 shall be necessary to the functioning of the CA. The CA shall document security attributes of all network services.

6.8 Time-Stamping

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

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The CA certificate shall be issued in the X.509 format, and shall include a reference to the OID for this CP within the Certificate Policies field. Supported certificate extensions shall be identified in the CPS. CAs must issue Subscriber certificates as specified within the *CSOS Certificate and CRL Profile* document established by the DEA.

7.1.1 Version Number(s)

The DEA Root CA and Subordinate CA shall issue X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate extensions used by authorized participants shall conform to the *CSOS Certificate and CRL Profile* document established by the DEA.

7.1.3 Algorithm Object Identifiers

At a minimum, one of the following algorithms must be used and/or supported by CAs and End-Entities for signing and verification:

Algorithm	Object Identifier
Sha256WithRSAEncryption	1 2 840 113549 1 1 11
DSA-with-SHA2	2 16 840 1 101 3 4 3 2
ecdsa-with-SHA-256	1 2 840 10045 4 3 2

7.1.4 Name Forms

In a certificate, the issuer DN and subject DN fields shall contain the full X.500 Distinguished Name of the CA.

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

CAs must ensure that the appropriate CSOS System CP OID is contained within the Subscriber and subordinate or cross-certified CA certificates.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

CSOS Subscriber certificates must 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

CAs issuing certificates under this CP shall mark the CP extension as non-critical. Critical extensions shall be interpreted as defined in IETF RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.2 CRL Profile

7.2.1 Version Number(s)

The DEA Root CA shall issue X.509 version 2 CRLs in accordance with the *CSOS Certificate and CRL Profile* document.

7.2.2 CRL and CRL Entry Extensions

All Entity PKI software must correctly process all ARL/CRL extensions identified in the *CSOS Certificate and CRL Profile*. ARLs/CRLs shall be issued in a format that is consistent with the [FPKI-PROF].

7.3 OSCP Profile

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

7.3.1 Version Number(s)

No stipulation.

7.3.2 OSCP Extensions

No stipulation.

8.0 Compliance Audit and Other Assessment

8.1 Frequency of Audit or Assessments

Certification Authorities (including RAs) shall undergo a compliance audit prior to initial certification as an authorized CA to demonstrate compliance with this CP and their CPS. Re-certification shall be required no less than once per year.

As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the "Compliance Audit Requirements" document at www.idmanagement.gov/fpkipa.

The PMA shall be responsible for ensuring audits are conducted for all PKI functions and reserves the right to conduct periodic and unscheduled compliance audits or inspections of the DEA CA and subordinate or cross-certified CAs, RAs or any Local RA services being provided in order to validate that the these entities are operating in accordance with the security practices and procedures described in their respective CPS.

8.2 Identity and Qualifications of Assessor

The auditor seeking to perform a compliance audit must be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The auditor must be qualified to perform an (American Institute of Certified Public Accountants) AICPA audit and must be thoroughly familiar with the requirements that the PMA defines for the issuance and management of CSOS certificates as provided in this CP. The compliance auditor must perform such compliance audits as a primary responsibility.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor, who is a private firm that is independent from the entity being audited, shall have sufficient organizational independence to ensure an unbiased, independent, and repeatable evaluation.

8.4 Topics Covered by Assessment

The purpose of the compliance audit shall be to verify that the CA has a system in place to ensure that its operational policies and procedures are consistent with the requirements stated in this CP and its CPS, as well as any MOAs between the Entity PKI and any other PKI.

8.5 Actions Taken as a Result of Deficiency

Should the compliance auditor find a discrepancy between a CA's operation and the stipulations in this CP or its CPS, the following must occur:

- The compliance auditor shall note the discrepancy;
- The CA shall provide written notification of the audit results to the PMA, specifically identifying any deficiencies noted as a result of the compliance audit, within 3 business days;
- Once notified, the PMA and OMA shall have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken. 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

Based on the findings of the compliance audit, appropriate remedies that the PMA may take may include any of the possible following actions:

- Warn the CA in writing and specify a time period during which the discrepancy must be resolved;
- Immediately suspend the CA's authority to issue new certificates;
- Revoke the CA's certificate.

Upon correction of the discrepancy, the CA may request reauthorization. A special audit may be required to confirm the implementation and effectiveness of the remedy.

8.6 Communications of Results

If the CA is found to be non-compliant with the CPS or this CP, the PMA may take action as specified in the section above. Required remedies shall be defined and communicated to the CA as soon as possible to limit the risks identified.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

The CAs shall not impose any fees to end entities for the reading of this CP or any other document incorporated by reference. The CA may charge fees for the issuance of certificates, subject to agreement between the CA and Subscriber and/or between the CA and Relying Party, and in accordance with a fee schedule publicly published by the CA in its CPS and on its web site.

9.1.2 Certificate Access Fees

The CAs shall not impose any fees to end entities for the reading of this CP or any other document incorporated by reference. The CA may charge fees for the access to certificates, subject to agreement between the CA and Subscriber and/or between the CA and Relying Party, and in accordance with a fee schedule publicly published by the CA in its CPS and on its web site.

9.1.3 Revocation or Status Information Access Fee

The CAs shall not impose any fees to end entities for the reading of this CP or any other document incorporated by reference. The CA may charge fees for the access to certificate status information, subject to agreement between the CA and Subscriber and/or between the CA and Relying Party, and in accordance with a fee schedule publicly published by the CA in its CPS and on its web site.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

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

9.2 Financial Responsibility

The PMA, DEA CA, and CSOS CA assume no financial responsibility for improperly used certificates.

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

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The CA shall keep all Subscriber information confidential with the exception of information that is included in the certificate. 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 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 shall be used only for the purpose collected and agreed and such information shall not be released without the prior written consent of the Subscriber. Any request for release of Subscriber information shall be authenticated.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The DEA CSOS Operational Authority shall conduct a Privacy Impact Assessment. If deemed necessary, the DEA CSOS Operational Authority shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The DEA CSOS Policy Authority shall approve the Privacy Plan.

For Entity CAs, no stipulation.

9.4.2 Information Treated as Private

The DEA CSOS program shall protect subscribers' personally identifying information from unauthorized disclosure. The contents of the archives maintained by the DEA CSOS Operational Authority shall not be released except as required by law.

9.4.3 Information Not Deemed Private

Information included in DEA CSOS certificates is not subject to protections outlined in Section 9.4.2.

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 DEA 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/Administrative Process

The DEA CSOS Operational Authority shall not disclose private information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Intellectual Property Rights

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in the CSOS Certificate. This CP and associated OIDs are the exclusive property of U.S. Government. CAs may only use associated OIDs in accordance with the provisions of this CP.

9.6 Representations and Warranties

The obligations described below pertain to the DEA CSOS CA (and, by implication, the DEA CSOS Operational Authority). The obligations applying to Principal (Root) or other CAs pertain to their activities as issuers of certificates.

9.6.1 CA Representations and Warranties

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

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

Subscribers shall be 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 CA'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 Representation and Warranties of Other Participants

None.

9.7 Disclaimers of Warranties

The DEA CSOS OA may not disclaim any responsibilities described in this CP.

9.8 Limitation 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, DEA CA, and CSOS CA assume no financial responsibility for improperly used certificates.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

Termination of this CP 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 PA shall establish appropriate procedures for communications with Entity CAs via contracts or memoranda of agreement as applicable.

For all other communications, no stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA shall review this CP at least once every year. Errors, updates, or changes to this CP shall be communicated to subordinate and cross-certified CAs. All policy changes under consideration by the PMA shall be disseminated to interested parties. All interested parties shall provide their comments to the PMA in a fashion to be prescribed by the PMA.

The PMA shall make the determination that a CPS complies with this policy.

9.12.2 Notification Mechanism and Period

Only editorial changes or typographical corrections may be made to this specification without notification. Any item in this CP may be changed with 90 day notice. Changes to items, which shall not materially impact a substantial majority of the CAs or relying parties using this CP, may be changed with 30 day notice.

Thirty days prior to major changes to this CP, a notification of the upcoming changes shall be posted and conveyed to subordinate or cross-certified CA organizations.

9.12.3 Circumstances Under Which OID Must Be Changed

OIDs will be changed if the DEA CSOS Policy Authority determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

Every attempt should be made to resolve the dispute by negotiation; however the PMA shall have the sole authority for the resolution of any disputes by quorum vote of the membership. CAs must describe dispute resolution procedures in their CPS. The PMA shall resolve any dispute arising out of this CP unless precluded by governing law or other agreement. Disputes requiring PMA resolution should be provided in writing to the PMA at the address specified in Section 1.

9.14 Governing Law

The laws of the United States of America and the laws of the states in which the Subscriber and Relying Party are domiciled shall govern the enforceability, construction, interpretation, and validity of this CP.

9.15 Compliance with Applicable Law

The DEA CSOS CAs are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

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

No stipulation.

9.17 Other Provisions

No stipulation.