



Operational Research Consultants, Inc.

External Certification Authority (ECA)

Key Recovery Practice Statement (KRPS)

Version 1.1

June 30, 2004

© Copyright 2004, Operational Research Consultants, Inc.
All Rights Reserved

*This document is proprietary and may not be disclosed to other parties, be it pursuant to the
Freedom of Information Act or to any other law or regulation.*

This Page intentionally left blank.

Table of Contents

1	INTRODUCTION	1
1.1	OVERVIEW	1
1.2	IDENTIFICATION	1
1.3	COMMUNITY AND APPLICABILITY	1
1.3.1	Key Recovery System Roles	2
1.3.2	OEC ECA Key Recovery System (KRS) Components	3
1.3.3	Applicability	4
1.4	CONTACT DETAILS	4
1.4.1	Key Recovery Policy Administration Organization	4
1.4.2	Contact Office	4
1.4.3	Person Performing Policy/Practice Compatibility Analysis	4
1.4.4	Contact Person Personnel	5
2	GENERAL PROVISIONS	5
2.1	OBLIGATIONS	5
2.1.1	ORC ECA KRS Obligations	5
2.1.2	KRA Obligations	6
2.1.3	KRO Obligations	6
2.1.4	Requestor Obligations	7
2.1.5	Subscriber Obligations	8
2.2	LIABILITY	9
2.2.1	Warranties and Limitations on Warranties	9
2.2.2	Damages Covered and Disclaimers	9
2.2.3	Loss Limitations	10
2.2.4	Other Exclusions	10
2.2.5	US Federal Government Liability	10
2.3	FINANCIAL RESPONSIBILITY	10
2.3.1	Indemnification by Relying Parties and Subscribers	10
2.3.2	Fiduciary Relationships	10
2.3.2	Administrative Processes	11
2.4	INTERPRETATION AND ENFORCEMENT	11
2.4.1	Governing Law	11
2.4.2	Severability of Provisions, Survival, Merger, and Notice	11
2.4.3	Conflict Provision	11
2.4.4	Dispute Resolution Procedures	11
2.5	FEES	11
2.6	PUBLICATION AND REPOSITORY	11
2.7	COMPLIANCE AUDIT	12
2.7.1	Frequency of Entity Compliance Audit	12
2.7.2	Identity/Qualifications of Compliance Auditor	12
2.7.3	Compliance Auditor's Relationship to Audited Party	12
2.7.4	Topics Covered by Compliance Audit	12

© Copyright 2004, Operational Research Consultants, Inc.

All Rights Reserved

This document is proprietary and may not be disclosed to other parties, be it pursuant to the Freedom of Information Act or to any other law or regulation.

2.7.5	Actions Taken as a Result of Deficiency	13
2.7.6	Communication of Results	13
2.8	CONFIDENTIALITY	13
2.8.1	Type of Information to be Protected	13
2.8.2	Information Release Circumstances	14
2.9	INTELLECTUAL PROPERTY RIGHTS	14
3	IDENTIFICATION AND AUTHENTICATION	14
3.1	IDENTITY AUTHENTICATION	14
3.2	REQUESTOR	15
3.2.1	Requestor Authentication	15
3.2.2	Requestor Authorization Verification	15
3.3	SUBSCRIBER	15
3.3.1	Subscriber Authentication	15
3.3.2	Subscriber Authorization Verification	16
3.4	KRA AND KRO AUTHENTICATION	16
3.4.1	KRA	16
3.4.2	KRO	16
4	OPERATIONAL REQUIREMENTS	17
4.1	ESCROWED KEY RECOVERY REQUESTS	17
4.1.1	Who Can Request Recovery of Escrowed Keys	17
4.1.2	Requirements for Requesting Escrowed Key Recovery	17
4.2	PROTECTION OF ESCROWED KEYS	17
4.2.1	Key Recovery through KRA	17
4.2.2	Automated Self-Recovery	18
4.3	CERTIFICATE ISSUANCE	18
4.4	CERTIFICATE ACCEPTANCE	18
4.5	SECURITY AUDIT PROCEDURES	18
4.5.1	Types of events recorded	18
4.5.2	Audit Log Processing	19
4.5.3	Audit Log Retention Period	19
4.5.4	Audit Log Protection	19
4.5.5	Audit Log Back Up Procedures	20
4.5.6	Audit Log Collection System (Internal vs. External)	20
4.5.7	Subscriber Audit Notification	20
4.5.8	Vulnerability Assessments	20
4.6	RECORDS ARCHIVAL	20
4.6.1	Types of information recorded	21
4.6.2	Archive Retention Period	21
4.6.3	Archive Protection	21
4.6.4	Archive backup procedures	21
4.6.5	Requirements for time-stamping of records	21
4.6.6	Archive Collection System (Internal vs. External)	21
4.6.7	Procedures to obtain and verify archive information	22

4.7	KRA KEY CHANGEOVER	22
4.8	KED COMPROMISE AND DISASTER RECOVERY	22
4.8.1	KED Compromise	22
4.8.2	Disaster Recovery	23
4.8.3	KRA or KRO Key Compromise	23
4.8.4	KRA or KRO Certificate Revocation	23
4.9	KRA TERMINATION	23
5	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	23
5.1	PHYSICAL CONTROLS	23
5.2	PROCEDURAL CONTROLS	24
5.2.1	Trusted roles	24
5.2.2	Separation of Roles	26
5.3	PERSONNEL CONTROLS	26
5.3.1	Background, qualifications, experience, and clearance requirements	26
5.3.2	Background check procedures	26
5.3.3	Training requirements	26
5.3.4	Retraining frequency and requirements	27
5.3.5	Job rotation frequency and sequence	27
5.3.6	Sanctions for unauthorized actions	27
5.3.7	Contracting personnel requirements	27
5.3.8	Documentation supplied to personnel	27
6	TECHNICAL SECURITY CONTROLS	27
6.1	PROTOCOL SECURITY	27
6.1.1	KED Protocol Security	28
6.1.2	KRA - KRO Protocol Security	28
6.1.3	Escrowed Key Distribution Security	28
6.2	KED, KRA AND KRO PRIVATE KEY PROTECTION	28
6.2.1	Standards for Cryptographic Modules	28
6.2.2	Private Key Control	28
6.2.3	KED Key Backup	29
6.2.4	Private Key Generation and Transport	29
6.2.5	Method of Activating Private Key	29
6.2.6	Method of Deactivating Private Key	29
6.2.7	Method of Deactivating Storage Key	29
6.3	PRIVATE KEY ACTIVATION DATA	30
6.4	COMPUTER SECURITY CONTROLS	30
6.4.1	KED	30
6.4.2	KRA and KRO Workstation	30
6.4.3	Anomaly Detection	30
6.5	LIFE CYCLE TECHNICAL CONTROLS	31
6.6	NETWORK SECURITY CONTROLS	31
6.7	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	31

© Copyright 2004, Operational Research Consultants, Inc.

All Rights Reserved

This document is proprietary and may not be disclosed to other parties, be it pursuant to the Freedom of Information Act or to any other law or regulation.

7	<i>POLICY ADMINISTRATION</i>	31
7.1	POLICY CHANGE PROCEDURES	31
7.2	PUBLICATION AND NOTIFICATION POLICIES	31
7.3	POLICY APPROVAL PROCEDURES	31
<i>Appendix A: References</i>		32
<i>Appendix B: Acronyms and Abbreviations</i>		33

This Page intentionally left blank.

1 INTRODUCTION

Operational Research Consultants, Inc. (ORC) is one of the commercial companies authorized to operate as an External Certification Authority (ECA) in support of the United States (US) Government ECA program. The ORC ECA has been established as a subordinate CA to the US Government ECA Root CA. The ORC ECA will allow rapid support certification services to US Government contractors that are supporting specified programs currently requiring or will require PKI support. One aspect of the ORC ECA Public Key Infrastructure (PKI) is the ability to escrow and recover private keys from key encipherment (or key exchange) public/private key pairs. The ORC ECA Key Recovery System (KRS) provides the computer system hardware, software, staff and procedures to store the private keys securely and recover them when appropriate. Section 1.3.2 describes the ORC ECA KRS and its components.

Since the ORC ECA KRS has a significant impact on the confidentiality services provided by the ORC ECA, its design and operation engender a high degree of trust. In order to manage risk and provide trust ORC has developed and is implementing an operational policy as described in this Key Recovery Practice Statement (KRPS). This KRPS describes procedural and technical security controls that ORC implements in order to securely operate the ORC ECA KRS, in accordance with the US Government ECA Key Recovery Policy (KRP).

1.1 OVERVIEW

The ORC ECA key recovery capability is based on the principle that all encryption activities using the certificates are performed on behalf of the person or the organization that authorized the issuance of encryption certificates. Therefore, the person or the business has the right to identify the persons authorized to recover the decryption private key(s) in order to maintain continuity of business operations. In addition, there may be need to access the information for investigative and law enforcement purposes.

The ORC ECA KRPS requires the use of two Key Recovery Agents (KRAs) to recover decryption private key(s) from the ORC ECA Key Escrow Database (KED), when an authorized party requests recovery of a subscriber's private key. The US Government ECA Policy Management Authority (EPMA) is the compliance authority for this KRPS, in accordance with the US Government ECA KRP V1.0, dated June 4, 2003.

1.2 IDENTIFICATION

There is no stipulation for an object identifier for this KRPS.

1.3 COMMUNITY AND APPLICABILITY

This section describes the roles and systems involved in the ORC ECA key recovery process. The ORC ECA KRS supports non-DoD entities transacting electronic business with or for US

Government entities. ORC ECA Subscribers may include contractors, vendors, allied partners, North Atlantic Treaty Organization (NATO) allies, Foreign Nationals, members of other Government agencies and their trading partners.

1.3.1 Key Recovery System Roles

1.3.1.1 Certificate Authority Administrator (CAA)

An ORC ECA Certificate Authority Administrator (CAA), as defined in the ORC ECA CPS, administers the ORC KRS Application.

1.3.1.2 Key Recovery Agent (KRA)

A KRA is an appointed and trusted individual who, using a two party control procedure with a second KRA, is authorized to interact with the KED (refer to Section 1.3.2.1 for a description of the ORC ECA KED) in order to extract an escrowed decryption private key. KRAs have high-level sensitive access to the KED. Because ORC ECA KRAs will have the ability to recover large numbers of keys, ORC places a high level of trust in them. ORC ECA CAAs will closely control the number and location of KRAs. KRAs are ORC personnel performing trusted ORC ECA KRS roles, as defined in section 5.2.1, of the ORC ECA CPS and herein.

1.3.1.3 Key Recovery Official (KRO)

The ORC ECA KRS can use the services of a Key Recovery Official (KRO) to perform identity verification and authorization validation tasks. KROs may authenticate the requestor and provide the encrypted recovered keys to the requestor, at the request of an ORC KRA. KROs consist of personnel from a subscriber organization. KROs are only able to participate in the recovery of keys of subscribers from their organization. In the event that a particular subscriber organization does not employ the services of a KRO, all requirements outlined in this KRPS for KROs apply to an ORC KRA.

1.3.1.4 Requestor

A requestor is the person who requests the recovery of decryption private key(s). A requestor is generally the subscriber, a third party from the subscriber's organization (e.g., supervisor, corporate officer) or a law enforcement officer who is authorized to request recovery of a subscriber's escrowed key. Any individual who can demonstrate a reasonably verifiable authority in accordance with the subscriber's organization information access and release policy and need to obtain a recovered key can be considered a requestor.

Internal Requestor: An internal requestor is any requestor who is in the subscriber's organization and is authorized to obtain the subscriber's key on behalf of the organization. The intent of this KRPS is not to change the policy and procedures of the organization. The

subscribers' organization will appoint authorized requestors and ORC will implement this KRPS so that the existing organization's policy regarding access and release of sensitive information can be met.

External Requestor: An external requestor is an investigator or someone outside the subscriber's organization with an authorized court order to obtain the **decryption** private key of the subscriber. An external requestor must work with an internal requestor unless the law requires ORC to release the subscriber's private key without approval of the subscriber and subscriber's organization. Nothing in this document is intended to change the current procedures for obtaining information about individuals in connection with such requests. ORC and subscriber organizations will appoint authorized personnel and implement this KRPS so that the existing organization policy regarding release of sensitive information can be met.

1.3.1.5 Subscriber

An ORC ECA subscriber is a person or device that holds a private key that corresponds to a public key listed in that certificate. For the purposes of this KRPS a subscriber is a person or device that holds a decryption private key that is escrowed in the ORC KED.

1.3.2 OEC ECA Key Recovery System (KRS) Components

The ORC ECA KRS consists of an information system used to provide key escrow and key recovery services for ORC ECA issued key encipherment (or key exchange) public/private key pairs. The ORC ECA KRS consists of the KED and KRA workstation(s). KROs perform their function from desktop computers and securely communicate with the KRAs via signed and encrypted e-mail.

1.3.2.1 Key Escrow Database (KED)

The ORC ECA KED is the subsystem that maintains the escrowed private keys in an unusable encrypted form. The ORC KED is configured to store keys in an encrypted format. The keys can only be decrypted by two KRAs authenticating separately to the KED and requesting the key at one time, providing for protection of the keys. Section 5.2.1.3 contains the description of trusted roles required to operate the ORC ECA KED.

1.3.2.2 KRA Workstation

The ORC ECA KRAs perform the recovery process by directly accessing the KED or from an ORC ECA KRA workstation that securely communicates with the ORC ECA KED. During recovery one KRA is able to send recovered medium assurance keys in a PKCS 12 format to the requestor or a KRO, via signed and encrypted email. The second KRA is able to send the appropriate PKCS 12 password to the requestor via signed and encrypted email or via US mail.

In the case of medium hardware assurance certificates, private **decryption** keys are recovered at a KRA workstation and imported onto the subscribers token at a KRA workstation; where one KRA

provides the location of the PKCS 12 file and the second KRA provides the required password. If the subscriber's original token is not available the key is imported to a new token under the control of the requestor.

1.3.2.3 KRO Workstation

KROs supporting the ORC KRS perform their function from a desktop computer equipped with a cryptographic token reader. KROs communicate with ORC ECA KRAs via signed and encrypted e-mail. All KRO transactions will be performed using a medium hardware assurance certificate as defined in the ORC ECA CPS. KROs will perform the following functions:

- Authentication of the requestor
- Validation of the requestor's authorization
- Sending key recovery requests to a KRA
- Receiving encrypted recovered key from a KRA
- Providing encrypted recovered key to requestor

1.3.3 Applicability

This KRPS applies to the ORC ECA, ORC ECA subscribers and ORC ECA subscribers' organizations.

1.4 CONTACT DETAILS

1.4.1 Key Recovery Policy Administration Organization

The EPMA is responsible for the oversight and approval of this KRPS. The EPMA is the Office of the Assistant Secretary of Defense for Networks and Information Integration, and its designees.

1.4.2 Contact Office

The contact office for the ORC ECA KRPS is:

ORC ECA KRA
11250 Waples Mill
Suite 210, South Tower
Fairfax, Virginia 22030

1.4.3 Person Performing Policy/Practice Compatibility Analysis

The EPMA is responsible for assessing compliance of this KRPS with the US Government ECA KRP. Mr. Daniel E. Turissini, is responsible for registration, maintenance, and interpretation of this KRPS.

Daniel E. Turissini
President
11250 Waples Mill, South Tower, Ste 210
Fairfax, VA 22030

1.4.4 Contact Personnel

Ms. Denise Finnance, Operational Research Consultants, Inc., (703) 246-8530, e-mail finnanced@orc.com.

Mr. Richard Webb, Operational Research Consultants, Inc., (703) 246-8545, e-mail webbr@orc.com.

Mr. Ken Pillow, Operational Research Consultants, Inc., (703) 246-8561, e-mail pillowk@orc.com.

2 GENERAL PROVISIONS

2.1 OBLIGATIONS

When subscribers or subscriber organizations request key escrow, subscribers are notified that the private keys associated with their encryption certificates will be escrowed as part of the ORC ECA key escrow process. When subscribers (or requestor) request key recovery, the delivery of recovered keys is protected against disclosure to any party except the requestor. This KRPS describes the method for ensuring that each individual understands and complies with the obligations for any Key Recovery role they execute.

2.1.1 ORC ECA KRS Obligations

The ORC ECA KRS provides escrowed keys to requestors under the Policy defined in the US Government KRP and this KRPS and conforms to the stipulations of these documents. In particular, the following stipulations apply; the ORC ECA KRS:

- Has obtained the EPMA approval for this KRPS
- Provides a copy to and makes available this KRPS to KRAs
- Provides a copy to and makes available KRO obligations to KROs
- Operates the KED in accordance with the stipulations of this KRPS and the US Government ECA KRP
- Automatically requests permission for key archival and notifies the subscribers when their private keys have been escrowed with the KED via a dialog box on a subscriber's screen during the certificate request process or secure e-mail
- Monitors KRA and KRO (as stipulated in Section 5.2) activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiates inquiries or investigations as appropriate

Any ORC ECA KRA or authorized KROs not operating in accordance with this KRPS will have their KR privileges and ORC ECA certificates immediately revoked.

2.1.2 KRA Obligations

An ORC ECA KRA who executes requests as described in this KRPS will comply with the stipulations of this KRPS. In particular, the following stipulations apply to an ORC ECA KRA:

- Maintains a copy of this KRPS
- Operates in accordance with the stipulations of this KRPS
- Protects subscribers' escrowed keys from unauthorized disclosure, including the encrypted files, encryption password, and associated decryption keys
- Protects all information, including the KRA's own key(s) that could be used to recover subscribers' escrowed keys
- Releases subscribers' escrowed keys only to properly authenticated and authorized requests from requestors by validating the digital signature of the requester or verifying the identity of the requestor, in person, in accordance with the activities specified by ORC ECA CPS for authentication of individual identity during initial registration for at least the specified certificate assurance level of the key being recovered
- Authenticates and validates the authorization of a KRO by ensuring that the KRO is an authorized KRO for the subscriber whose key is being requested for recovery
- Protects all information regarding all occurrences of key recovery
- Communicates knowledge of a recovery process only to the KRO and requestor involved in the key recovery (KRAs will not communicate any information concerning a key recovery to the subscriber except when the subscriber is the requestor)
- Monitors KRO activity (as stipulated in Section 5.2) for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiates inquiries and/or investigations as appropriate

Requestor authentication and authorization verification may be delegated to a KRO with authorization from an ORC ECA CAA. When delegated to a KRO, the KRA will authenticate KRO correspondence via signed and encrypted email, using a medium hardware assurance certificates issued by the ORC ECA. KRAs may request additional information or verification from the KROs as deemed necessary to meet this obligation.

2.1.3 KRO Obligations

A KRO authorized by the subscriber's organization and accepted by ORC, is responsible to initiate a key recovery request for a requestor. The requestor is either a third party, or the subscriber. A KRO under this KRPS is obligated to:

- Protect subscribers' recovered keys from compromise (a KRO may receive the recovered keys in encrypted form from a KRA via signed and encrypted email, after providing the

- requestor with the encrypted key, the KRO will destroy any local copy of the key in their system)
- Request the subscriber's keys only upon receipt of a request from an authorized requestor:
 - As an intermediary for the KRA, the KRO will validate the identity of any requestor seeking a key recovery
 - The process for validating the identity will be the same as the one used for user registration as defined in ORC ECA CPS
 - In the case of persons other than the subscriber seeking a key recovery, the KRO will also ensure that the requestor has the authority to request the subscriber's key in accordance with the subscriber's organization policy
 - Protect all information; including the KRO's own key(s) that could be used to receive the subscriber's recovered key(s) in encrypted form
 - Protect all information regarding all occurrences of key recovery
 - Communicate knowledge of any recovery process only to the requestor (the KRO will not communicate any information concerning a key recovery to the subscriber except when the subscriber is the requestor)
 - Accurately represent themselves to all entities when requesting key recovery services
 - Maintain records of all recovery requests and disposition, including acknowledgement of receipt by the requestor (audit records will not contain subscribers' keys in any form; plaintext, split, encrypted, etc.)

2.1.4 Requestor Obligations

Prior to receiving a recovered key, the ORC ECA ensures that the requestor formally acknowledges and agrees to the following obligations, the "Requestor Recovery Agreement" requires the requestor to:

- Protect subscribers' recovered key(s) from compromise
- Use a combination of computer security, cryptographic, network security, physical security, personnel security, and procedural security controls to protect their keys and recovered subscribers' keys (when the requestor is not the subscriber, the requestor will destroy subscribers' keys when no longer required [i.e., when the data has been recovered])
- Request the subscriber's escrowed key(s) only to recover subscriber's data that they are authorized to access
- Use the subscriber's recovered keys only to recover subscriber's data they are authorized to access
- Accurately represent themselves to all entities during any key recovery service (when a request is made to a KRA or KRO, the requestor will provide accurate identification and authentication information):

- This will be accomplished by the requestor via a digitally signed e-mail using ORC ECA issued credential of the same or higher assurance level as the key being recovered (the KRA or KRO will use the signed email to electronically authenticate the requestor by validating the signature through establishing a trust chain to the ORC ECA and confirming that the certificate used in signing is not on the revocation list)
- In person identification and authentication information will be in accordance with the same level as that used for user registration at the level of the key being requested, as defined in ORC ECA CPS
- Protect information concerning each key recovery operation. The requestor will communicate information concerning the recovery to the subscriber when appropriate, as determined by the reason for the recovery:
 - Whether to notify the subscriber or not, will be based on the law, and subscriber organization's policies and procedures for third party information access
 - In the event that the requestor notifies the subscriber of a key recovery, the requestor will advise the subscriber to determine whether or not the recovery circumstances warrant revoking the associated public key certificate
- Upon receipt of the recovered key(s), the requestor (if not the subscriber) will sign a document prepared by the requestor, which includes the following statement (this statement is available at the ORC ECA website and by contacting the ORC ECA help desk):

“I hereby affirm that I have legitimate and official need to recover this key in order to obtain (recover) the encrypted data that I have authorization to access. I acknowledge receipt of a recovered ORC ECA decryption private key associated with the subscriber identified here. I certify that I have accurately identified myself to the KRO (or KRA), and truthfully described all reasons that I require access to data protected by the recovered key. I acknowledge my responsibility to use this recovered key only for the stated purposes, to protect it from further exposure, and to destroy all key materials or return them to the KRO/ KRA when no longer needed. I understand that I am bound by subscriber's organization policies, applicable laws and US Federal regulations concerning the protection of the recovered key and any data recovered using the key.”

As a condition of receiving recovered key(s), a requestor will sign this acknowledgement of agreement to follow the law and the subscriber's organization policies relating to protection and release of the recovered key(s).

2.1.5 Subscriber Obligations

ORC will ensure that all Subscribers comply with the following stipulations, Subscribers will:

- Provide accurate identification and authentication information during initial registration and subsequent key recovery requests

- Determine whether revocation of the public key certificate associated with the recovered key is necessary, when the subscriber is notified that their escrowed key has been recovered, and request the revocation, if necessary

2.2 LIABILITY

2.2.1 Warranties and Limitations on Warranties

ORC warrants that its procedures are implemented in accordance with this KRPS, and that any private encryption keys escrowed and or recovered by the ORC ECA KRS, are in accordance with the stipulations of this KRPS.

ORC warrants that any KRA or designated authority under this KRPS shall operate in accordance with the applicable sections of this KRPS.

Subscriber (applicant) organizations that authorize KROs under this KRPS warrant that:

- The KRO procedures are implemented in accordance with the US Government ECA KRP and this KRPS, as well as, the US Government ECA CP and the ORC ECA CPS, where applicable
- All ORC KRO key escrow and recovery actions are accomplished in accordance with this KRPS
- KROs operate in accordance with the applicable sections of this KRPS
- The subscriber (applicant) organization will cooperate and assist ORC in monitoring and auditing that authorized KROs are operating in accordance with the applicable sections of this KRPS
- Network security controls to KRO equipment are in accordance with the applicable sections of this KRPS

2.2.2 Damages Covered and Disclaimers

Other than the warranties included in section 2.2.1, ORC disclaims any warranties or obligations of any type concerning the accuracy of information provided by a Subscriber or Requestor to ORC ECA, provided the procedures stated in this ORC ECA KRPS were followed and the procedures were in compliance with the ORC ECA CPS and this KRPS. Furthermore, ORC disclaims any and all liability for negligence and lack of reasonable care on the parts of Subscribers, Requestors and Subscriber's Organization's KROs.

ORC warrants that KRS procedures are implemented in accordance with this KRPS, and that all keys are escrowed and/or recovered in accordance with the stipulations of this KRPS. ORC warrants that all ORC employed KRAs, KROs (if applicable), and KED operate in accordance with the applicable sections of this KRPS.

2.2.3 Loss Limitations

ORC disclaims any liability for loss due to use of private keys recovered via the ORC ECA KRS provided that the private key was recovered in accordance with this KRPS. ORC acknowledges professional liability with respect to the ORC KRS and/ or the ORC KRAs.

If ORC or any agent of ORC (including KRAs and ORC employed KROs) is negligent, reckless, or engages in fraudulent activity, ORC shall not be liable for more than \$1 million (U.S. Dollars) total liability. The limit for losses per transaction due to improper actions by ORC, or its agents is \$1,000 (U.S. Dollars).

2.2.4 Other Exclusions

Requestors and Subscribers signify and guarantee that their request for and use of recovered private keys from the ORC ECA KRS does not interfere with or infringe upon the rights of any others regarding their trademarks, trade names or any other intellectual property. Certificate applicants hold ORC harmless for any losses resulting from any such act.

2.2.5 US Federal Government Liability

Subscribers and Requestors will have no claim against the US Federal Government arising from use of the Subscriber's recovered private key or for the ORC ECA inability to recover a private key. In no event will the Government EPMA be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any key escrow or recovery operation, or non-performance of a key escrow or recovery operation, except in the event that a Government agent accepts the role of a KRO.

Subscribers and Requestors will have no claim against the US Federal Government arising from erroneous key escrow and key recovery operations by the ORC ECA KRS. ORC will have no claim for loss against the EPMA, except in the event that a Government agent accepts the role of a KRO.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification by Relying Parties and Subscribers

Neither ORC nor its agents (e.g., KRA, ORC employed KRO, etc.) assume financial responsibility for improper use of a recovered key by subscriber or by requestor.

2.3.2 Fiduciary Relationships

Escrow and recovery of private keys in accordance with this KRPS does not make the ORC, ORC personnel, or any personnel filling KRA or KRO roles, an agent, fiduciary, trustee, or other representative of Subscribers or Requestors.

2.3.2 Administrative Processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

As stipulated in the ORC ECA CPS.

2.4.2 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this KRPS is incorrect or invalid, the other sections will remain in effect until the KRPS is updated. Requirements for updating this KRPS are described in Section 7. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

2.4.3 Conflict Provision

In the event of any conflict between the ORC ECA KRPS and US Government ECA KRP, the US Government ECA KRP will take precedence over this ORC ECA KRPS.

2.4.4 Dispute Resolution Procedures

The EPMA shall be the sole arbiter of disputes over the interpretation or applicability of the ECA KRP.

With respect to Subscriber or Relying Party Agreements or Obligations made by an entity by purchasing the services associated with this KRPS an attempt shall be made to resolve any dispute through an independent mediator, mutually agreed to by all disputing parties. If mediation is unsuccessful in resolving such a dispute, it shall be resolved by arbitration in accordance with applicable statutes.

2.5 FEES

Fees for performing key recovery services will be established by ORC and provided to the Subscriber or the Subscriber's Organization upon request.

2.6 PUBLICATION AND REPOSITORY

A summary of this EPMA approved KRPS is publicly available on the ORC ECA website.

2.7 COMPLIANCE AUDIT

A nationally known firm audits ORC annually, in accordance with WebTrust. ORC is also audited aperiodically by: GSA, DoD and NSA. ORC has an independent internal department that performs weekly procedures in order to attest to ORC's compliance with this KRPS. Audit and inspection is accomplished in accordance with the American Institute of Certified Public Accountants (AICPA) WebTrust Program for Certification Authorities or other current industry accepted standards and practices.

2.7.1 Frequency of Entity Compliance Audit

ORC audits the KRS and KRS components with the following audit frequencies:

- KED(s) – Annually
- KRA/ KRO(s) – with the same frequency as the ORC ECA Registration Authorities (RAs) and Local Registration Authorities (LRAs), as specified in the ORC ECA CPS

To the greatest extent possible ORC will audit the KRS in conjunction with the audit of the other elements of the ORC PKI, including the ECA and the ECA Certificate Status Authority (CSA).

In the event that a KRA or KRO is relieved of that responsibility due to a failure to comply with this KRPS, ORC will comply with a special compliance audit, as directed by the EPMA. The purpose of that audit will be to determine whether any key recovery activities of the removed KRA or KRO may have been improper or may have affected the integrity of the KRS.

2.7.2 Identity/Qualifications of Compliance Auditor

ORC will engage the services of an auditor that is competent in the field of security compliance audits of Information Technology systems and is thoroughly familiar with this KRPS. Further, the selected auditor will have experience in information security, cryptography and PKI.

2.7.3 Compliance Auditor's Relationship to Audited Party

The auditor, as defined in Section 2.7.2, is an independent entity. ORC also performs internal audits of the KRS facility conducted by the Corporate Security Auditor, as defined in the ORC ECA CPS.

2.7.4 Topics Covered by Compliance Audit

All the topics identified in this KRPS document will be covered by the compliance audit. The purpose of a compliance audit will be to verify that the ORC KED, KRAs/ Workstations, and KROs have requisite procedures and control in place.

2.7.5 Actions Taken as a Result of Deficiency

Should the compliance auditor find a discrepancy between a KED, KRA or KRO operation and the stipulations of this KRPS, the following actions shall occur:

- The compliance auditor will note the discrepancy
- The compliance auditor will notify the parties identified in Section 2.7.6 of the discrepancy
- The audited entity will propose a remedy, including expected time for completion, to the EPMA

ORC will propose a remedy and will comply with the remedy determined appropriate by the EPMA, up to and including revocation or non-recognition of the audited entity's certificate. Upon correction of the deficiency, the ORC may request the EPMA to reinstate the audited entity.

ORC will note any discrepancies between ORC ECA KRS operations, and the stipulations of this KRPS and the US Government ECA KRP and immediately notified the EPMA of all discrepancies. ORC will comply with all EPMA remedies, including a time for completion. ORC acknowledges that remedy may include permanent or temporary ECA cessation or termination of ECA accreditation, and that several factors will be considered in this decision, including the severity of the discrepancy, the risks it imposes, and the disruption to the certificate using community.

2.7.6 Communication of Results

In the case of an ORC ECA KED compliance audit, the compliance auditor will submit a report of the compliance audit to the EPMA and to ORC. In the case of a KRA compliance audit, the compliance auditor will submit a report to ORC. In the case of a KRO compliance audits, the results will be submitted to ORC and to the designated representative of the subscribers' organization that the KRO serves.

A compliance audit summary outlining key results is posted on the ORC ECA web site in a medium hardware assurance certificate, authenticated, read only, access-controlled area protected by an ORC ECA server (SSL) certificate to protect against alteration of and unauthorized access to the result information. If an entity (i.e., KED, KRA, or KRO) is found not to be in compliance with this KRPS, or the policy identified in the US Government ECA KRP, ORC shall notify the EPMA immediately upon completion of the audit.

2.8 CONFIDENTIALITY

2.8.1 Type of Information to be Protected

ORC requires that the KED, KRA, KRO and requestor protect personal or sensitive information used to identify and authenticate participants in the recovery process, to the greatest extent possible. Such information includes Social Security Number (SSN), identification credential serial numbers, and

affiliation with investigative agencies when specified by the requestor as sensitive. Protections are described in Sections 4, 5, and 6 of this KRPS and in the ORC ECA CPS.

ORC will ensure that the KED, key escrow, and key recovery processes protect the subscriber private keys. ORC will ensure that, when key recovery is requested by a third party, information concerning the request will also be protected, to the greatest extent of the law.

2.8.2 Information Release Circumstances

ORC will release sensitive data to law enforcement officials only under a proper court order. ORC will not disclose non-public certificate or certificate-related information to any third party unless expressly authorized by the US Government ECA CP, the US Government ECA KRP or the EPMA, required by criminal law, government rule or regulation, or order of a criminal court with jurisdiction. External request must be made via the subscriber's organization KRO, unless under court order. ORC shall authenticate such requests prior to disclosure.

An ORC KRA will not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless authorized by ORC and the EPMA; required by the law, government rule, or regulation; by the subscriber's organization policy; or by order of a court of competent jurisdiction. The identity of the requestor of escrowed keys will be authenticated and the authorization validated per Section 3 of this KRPS.

2.9 INTELLECTUAL PROPERTY RIGHTS

Refer to ORC ECA CPS Section 2.9.

3 IDENTIFICATION AND AUTHENTICATION

The purpose of Identification and Authentication is to verify that requestors are whom they say they are and are authorized to access requested escrowed key. The user's authenticated identity will be used as the basis for determining the user's authorizations and providing user accountability.

3.1 IDENTITY AUTHENTICATION

Identity authentication will be commensurate with the assurance level of ORC ECA certificate associated with the key being recovered, as described in the ORC ECA CPS. Authentication of individual identity will be based on digital signatures that can be verified using public key certificates for at least the specified certificate assurance level of the key(s) being recovered. In the rare case where digital authentication is not possible, in person identity authentication or verification may be accommodated. It will comprise the activities specified by ORC ECA CPS for authentication of individual identity during initial registration for at least the specified certificate assurance level.

3.2 REQUESTOR

This section defines the requirements for authentication and authorization of a third party requestor, i.e., a requestor other than the subscriber itself. The requirements for authentication and authorization, when the requestor is the subscriber, are addressed in Section 3.3.

3.2.1 Requestor Authentication

ORC ensures that a requestor establishes his or her identity to a KRA (or a KRO, as an intermediary for the KRA), as specified in Section 3.1. In cases where an electronic request is made a KRA or KRO will verify the digital signature on the request and ensure that the request is signed using a certificate at least to the specified assurance level of the key being recovered, prior to initiating the key recovery request. In all cases where a digitally signed, electronic request is made (directly to a KRA or via a KRO), a KRA shall authenticate the identity of the requestor (and the KRO) by validating their digital signatures.

In cases where digital authentication is not possible, a KRA or KRO will perform in person identity authentication, as specified in Section 3.1. If performed by a KRO, the KRO will provide that information to the KRA, along with a recovery request for the requestor, via digitally signed email. The KRA receiving the KRO email shall authenticate the identity of the KRO by validating the digital signature of the KRO.

In all cases KRAs may request additional information or verification from a KRO if deemed necessary by the KRA to confirm the requestor's identity.

3.2.2 Requestor Authorization Verification

An ORC KRA (or a KRO as an intermediary for the KRA) will validate the authorization of the requestor in consultation with the subscriber's organization management and/or legal counsel, as appropriate.

3.3 SUBSCRIBER

3.3.1 Subscriber Authentication

ORC ensures that a subscriber establishes their identity to a KRA (or a KRO, as an intermediary for the KRA), as specified for a requestor in Section 3.2.1. In cases where an electronic request is made to a KRA or KRO will verify the digital signature on the request and ensure that the request is signed using a certificate at least to the specified assurance level of the key being recovered, prior to initiating the key recovery request. In all cases where a digitally signed, electronic request is made (directly to a KRA or via a KRO), a KRA shall authenticate the identity of the subscriber (and the KRO) by validating their digital signatures.

In cases where digital authentication is not possible, a KRA or KRO will perform in person identity authentication, as specified in Section 3.1. If performed by a KRO, the KRO will provide that information to the KRA, along with a recovery request for the subscriber, via digitally signed email. The KRA receiving the KRO email shall authenticate the identity of the KRO by validating the digital signature of the KRO.

In all cases KRAs may request additional information or verification from a KRO if deemed necessary by the KRA to confirm the requestor's identity.

3.3.2 Subscriber Authorization Verification

Only current/validated subscribers, in accordance with section 3.1, are authorized to request recovery of their own escrowed key material either medium assurance or medium assurance hardware. In the case of in person identity authentication a KRA will first query the ECA database to ensure that the subscriber has been issued a current/ valid certificate and ensure the identity of the subscriber matches that of the key to be recovered with an ORC ECA RA.

3.4 KRA AND KRO AUTHENTICATION

3.4.1 KRA

ORC KRAs are assigned by an ORC CAA and are issued medium hardware assurance level certificates, generated on cryptographic hardware tokens that have been certified at FIPS 140-1/2 Level 2, as listed on the NIST website. The identity proofing of an ORC KRA is accomplished in person with an ORC Registration Authority (RA), in accordance with the ORC ECA CPS. The medium hardware assurance level certificate is used to access the KED, sign correspondence to the KRO and requestor and accept encrypted email from a KRO or requestor.

3.4.2 KRO

KROs are assigned by the subscriber's organization, accepted by the ORC CAA and are issued medium hardware assurance level certificates, generated on cryptographic hardware tokens that have been certified at FIPS 140-1/2 Level 2, as listed on the NIST website. The identity proofing of an ORC KRO is accomplished in person with an ORC ECA RA, in accordance with the ORC ECA CPS. KROs authenticate to an ORC KRA via signed email using the medium hardware assurance certificate. In the signed email the KRO identifies the domain for which they have authority to make requests. The KRA will validate the KRO with a master KRO list maintained by the ORC CAA, which identifies each KRO's domain and status. In the event that the recovered PKCS 12 file cannot be sent to the requester via signed and encrypted email the KRO's may receive the recovered PKCS 12 file via signed and encrypted email.

4 OPERATIONAL REQUIREMENTS

4.1 ESCROWED KEY RECOVERY REQUESTS

4.1.1 Who Can Request Recovery of Escrowed Keys

Subscribers may request recovery of their own escrowed encryption keys as verified by the organization's KRO or in person at an ORC KRA workstation. Additionally, personnel permitted by the subscriber's organization policy as verified by the organization's KRO (such as the Subscribers supervisor or human resource manager) and authorized law enforcement personnel with a court order from a cognizant court (such as a DoD investigator who has authorization to access the subscriber communication, or a duly authorized law enforcement or court official who has court authorization to access subscriber communication) may also request recovery of escrowed keys from a subscribers KRO.

4.1.2 Requirements for Requesting Escrowed Key Recovery

Subscribers must use electronic means to request their own escrowed keys from the KRS. The subscriber may submit the request to a KRA or KRO. The subscriber will digitally sign the request using an ORC ECA issued signature certificate of assurance level equal to or greater than that of the escrowed key. Written requests signed by hand and notarized may be accepted on a case-by-case basis.

Third party requestors must use electronic means to request the subscribers' escrowed keys. The requestor will submit the request to a KRA or KRO, digitally signing the request using an ORC ECA issued signature certificate of assurance level equal to or greater than that of the escrowed key. Written requests signed by hand and notarized may be accepted on a case-by-case basis.

4.2 PROTECTION OF ESCROWED KEYS

Escrowed keys are stored in a protected KED, as stipulated in section 4.1 of the ORC ECA CPS. The KED consists of equipment dedicated to the key recovery and ECA archival functions. KED and KRA physical controls are specified in Section 5.1. The KED maintains the escrowed private keys in an unusable encrypted form. The KED private keys are protected as stipulated in Section 6.2.1. Archived subscriber keys can only be decrypted by two KRAs authenticating separately to the KED and requesting the key at one time, providing for protection of the keys.

4.2.1 Key Recovery through KRA

ORC KRAs are provided access to a copy of key(s) escrowed in the KED only in response to a properly authenticated and authorized key recovery request. Such access requires the actions of at least two KRAs. All copies of escrowed keys are protected using two person control procedures

during recovery and delivery to the authenticated and authorized third party requestor and during operation and maintenance of the ORC ECA KED.

The protection mechanisms during recovery and delivery will be by two party procedures. During recovery operations password procedures are used to maintain two person controls at the KED or KRA workstation consoles.

4.2.2 Automated Self-Recovery

The ORC KRS does not support automated self-recovery.

4.3 CERTIFICATE ISSUANCE

Certificate issuance is in accordance with the ORC ECA CPS.

4.4 CERTIFICATE ACCEPTANCE

Certificate acceptance is in accordance with the ORC ECA CPS.

4.5 SECURITY AUDIT PROCEDURES

Security auditing capabilities of ORC ECA KED and KRA workstation equipment operating systems are enabled upon installation and remain enabled during operation.

4.5.1 Types of events recorded

The ORC ECA KED equipment is configured to record the following event types and may be recorded in conjunction with the events recorded in Section 4.5.1 of the ORC ECA CPS:

- Installation
- Software modification
- Configuration modification
- KED application access
- Actions taken in response to requests for KED actions
- Physical access
- Receipt of keys for escrow and posting of these keys to the KED
- Retrieval, packaging
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages
- Any known or suspected violations of physical security, suspected or known attempts to attack the KED equipment via network attacks, equipment failures, power outages, network failures, or violations of this KRPS

All signed e-mail requests received by a KRO shall be maintained as electronic audit records. A KRO will archive their KRO inbox to a CDROM on a monthly basis. The KRO will also manually log/record the following information for audit:

- Transfer of recovered keys to requestors, if transmitted through the KRO
- Any security-relevant actions performed in support of delivery of recovered keys
- Requestor identity and authorization verification (including copies of authorizations such as court orders) supporting key recovery requests acted upon by the KRO
- Signed requestor acknowledgement forms

For each auditable event defined in this section, the audit record will include, at a minimum:

- Type of event
- Time the event occurred
- For messages from KRAs, KROs, or other entities requesting KRS actions, the message source, destination, and contents
- For requested KRS actions – a success or failure indication
- For operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action
- The KED, KRA and KRO audit logs are configured to not contain recovered keys (in plaintext or encrypted forms) and passwords used to protect the keys

4.5.2 Audit Log Processing

Automated audit logs are processed as required to prevent audit overflow, audit over-write or stoppage of system operation.

4.5.3 Audit Log Retention Period

All audit logs are archived in a protected off site facility and retained for a period as stipulated in Section 4.5.3 of the ORC ECA CPS.

4.5.4 Audit Log Protection

Audit logs are protected from unauthorized modification or unauthorized deletion. No person is authorized to modify the content of audit logs, except for appending new audit records without overwriting existing audit records. Two parties, as described in the ORC ECA CPS, Operating Procedures, and Roles Manual protect data access.

Electronic audit logs are deleted only after they have been backed up to archive media. Root access is required to delete KED logs. No person is authorized to delete or destroy audit data recorded on archive media.

4.5.5 Audit Log Back Up Procedures

ORC's Corporate Security Auditor and all audit log-processing personnel are required to use the procedures described in the ORC ECA Operator's Manual to perform regular back up of all audit logs.

4.5.6 Audit Log Collection System (Internal vs. External)

The automatic audit log processes are internal to the ORC ECA KED and KRA equipment. Audit processes are invoked at component system startup and cease only at component system shutdown. Audit processes run automatically without human intervention. Should it become apparent that an automated audit process has failed the KED will cease all operations until an audit capability can be restored.

KRO audit logs are manually collected. Signed e-mail requests received by a KRO shall be maintained as electronic audit records. A KRO will archive their KRO inbox to a CDROM on a monthly basis. The KRO will also log/ record the information stipulated in Section 4.5.1. These logs/ records will be archive by the KRO on a monthly basis.

4.5.7 Subscriber Audit Notification

There is no requirement to notify a subscriber of an audit event.

4.5.8 Vulnerability Assessments

KRAs, SAs, and other supporting personnel monitor for attempts to violate the integrity of the KRS, including the equipment, physical location, and personnel. Audit logs are reviewed by ORC's Corporate Security Auditor (or designated audit log-processing personnel) at least once per week for events such as repeated failed actions, requests for escrowed keys, attempted access of escrowed keys, unauthenticated requests, or other suspicious or unusual activity. ORC's audit log-processing personnel also checks for continuity of the audit logs. Anomalies must be reported to the Corporate Security Auditor to initiate investigations and report it to the EPMA if determine necessary.

4.6 RECORDS ARCHIVAL

The ORC KED maintains a trusted archive of information stored and of transactions carried out. The primary objective of the archive is to be able to reconstruct the key recovery activities, in case of dispute, such as:

- Validation of the identity of the recipient of a copy of the subscriber's escrowed key
- Verification of authorization and need of requestor to obtain the escrowed key copy
- Establishment of the circumstances under which a copy of the escrowed key was provided

4.6.1 Types of information recorded

The following information will be archived:

- The US Government ECA KRP and this KRPS
- Agreements with KRAs, KROs, subscribers, and/or subscribers' organization
- Audit logs identified in section 4.5.1
- Security Audit data
- Escrowed keys

The US Government ECA KRP is archived by the EPMA and a copy is archived by the ORC ECA. All other information will be archived by the ORC Corporate Security Officer. ORC also retains the necessary software and hardware, either as operational components or, after decommissioning, as archive retrieval components, to support interpretation of the information during the entire archive retention period.

4.6.2 Archive Retention Period

The archive retention period is in accordance with the requirements specified in ORC ECA CPS Section 4.6.2 for certificate assurance levels supported. Escrowed keys are maintained within the online ORC ECA KED for a minimum of one year after the expiration of the associated public key certificate.

4.6.3 Archive Protection

No person is able to modify or delete archived data written to CD ROM. Archived escrowed keys are protected as specified in Section 4.2. Archive media is stored in a separate, safe, secure storage facility, as described in the ORC ECA CPS, Section 5.1.2. Archive media is labeled with the ORC ECA distinguished name and date of archival.

4.6.4 Archive backup procedures

The ORC ECA KRS audit data shall be backed-up in accordance with the requirements of the ORC CPS, Section 4.6.4.

4.6.5 Requirements for time-stamping of records

The ORC ECA KRS archived records contain information necessary to determine when an event occurred. Audit records will be signed and time stamped. The time precision will be such that the sequence of events can be determined.

4.6.6 Archive Collection System (Internal vs. External)

Archive data will be collected monthly.

4.6.7 Procedures to obtain and verify archive information

The procedures used to verify the accuracy of the archived information are as stipulated in accordance with the ORC CPS, Section 4.6.6.

4.7 KRA KEY CHANGEOVER

KRA certificates will be issued for three years in accordance with the requirements of the ORC ECA CPS for medium hardware assurance identity and encryption certificates.

4.8 KED COMPROMISE AND DISASTER RECOVERY

Compromise or disaster notification and recovery procedures are employed by the ORC ECA KRS to ensure the KED remains in a secure state. The security provided by the KED is dependent on protection of the private keys associated with the KED certificates. The ORC KED keys are protected from compromise due to malicious attack or inadvertent loss of key/ activation data, as well as, from disasters cause by loss of essential equipment loss by employing controls such as:

- Two person control procedures of the KED hardware encryption module, which includes physical separation of its activation mechanism
- Two person control procedures of the KED key activation data
- Assignment of passwords only to authorized trusted users
- Periodic changing of KRA token passwords (not less then quarterly)

These measures minimize the risk of compromise due to use, storage, or knowledge of key activation mechanisms.

4.8.1 KED Compromise

The ORC KED uses component certificates as defined in Section A.5 of the ORC ECA CPS and Section A.5 of the US Government ECA CP for SSL, transport, and storage; however, key recovery may be required for Subscriber archived certificates beyond the life of the KED keys.

To minimize risk to the PKI through compromise, the ORC KED will be “re-keyed” every three (3) years. All previous KED instances will continue to be maintained, in accordance with this KRPS to enable recovery of previously escrowed keys beyond the life of the KED transport and storage certificates (up to four (4) years after a KED is no longer archiving keys). ORC will issue new SSL certificates used to configure the KED to support the recovery of valid escrowed keys.

In the case of a KED transport, storage, or SSL key compromise, all subscriber certificates associated with the keys protected by the compromised key will be revoked and each affected subscriber notified.

In the event that the ORC ECA KED is compromised, or compromise is suspected, ORC will notify the EPMA. The EPMA will be granted sufficient access to information to determine the extent of the compromise. ORC will comply with EPMA directed appropriate action. This may include revocation of certificates associated with the compromised private keys stored in the KED. In the case of any compromise ORC reserves the right to revoke all effected certificates.

4.8.2 Disaster Recovery

Disaster recovery is in accordance with the ORC ECA CPS, Section 4.8.2.

4.8.3 KRA or KRO Key Compromise

If an ORC ECA KRA or KRO certificate is revoked due to compromise, there is a potential for some subscriber's escrowed keys to have been exposed during the recovery process. ORCs Corporate Security Auditor (or designated audit personnel) will review the audit records to identify all potentially exposed escrowed keys. Each of the potentially exposed escrowed keys will be revoked, according to procedures specified in ORC ECA CPS Section 4.4.1, and the subscriber will be notified of the revocation.

4.8.4 KRA or KRO Certificate Revocation

If an ORC ECA KRA or KRO certificate is revoked for any reason other than compromise, and the KRA or KRO remains authorized to perform their duties, the KRA or KRO is required to request a new KRA or KRO certificate from the ORC ECA. The ORC ECA will report the old KRA or KRO certificate as revoked using the revocation notification procedures defined in the ORC ECA CPS. The ORC ECA procedures for certificate issuance will be used for the new KRA or KRO public key certificate.

4.9 KRA TERMINATION

Upon termination ORC will transfer all KRA archive records to the ORC Corporate Auditor. The medium and format in which the data is archive is described in section 4.6 of the ORC ECA CPS.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

The ORC KED consists of equipment dedicated to the key recovery and ECA archival functions. KED physical controls are those specified in ORC ECA CPS Section 5.1 for ECA equipment. KRA workstation physical controls are equivalent to those specified in ORC ECA CPS Section 5.1 for Issuing Authority (IA) equipment.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted roles

The primary trusted roles defined by this KRPS, over and above the roles defined in the ORC ECA CPS, are the KRA and the KRO. An SA, as defined in the ORC ECA CPS, is primarily responsible for administration of the ORC KED and KRA workstation host computers and operating systems. The CAA, as defined in the ORC ECA CPS, administers the KED application and keys.

5.2.1.1 Key Recovery Agent

ORC KRAs operating under this KRPS are subject to the stipulations of this KRPS and are required to maintain a copy of and operate in accordance with the stipulations of this KRPS. ORC KRA responsibilities are to ensure that the functions defined in Section 2.1.2 occur according to the stipulations of this KRPS. KRAs will also monitor KRO activity for patterns of potentially anomalous activity as indicators of possible problems in the infrastructure, and initiates inquiries and/or investigations as appropriate. On a monthly basis the KRA will report to the sponsoring activities PKI Sponsor the level of key recovery activity and note any concerns that may indicate potentially anomalous activity.

Each KRA shall report any anomaly occurring that is not in accordance with the stipulations of this KRPS to ORC's Corporate Security Auditor via signed email.

5.2.1.2 Key Recovery Official

All KROs operating under this KRPS are subject to the stipulations of this KRPS. A KRO is responsible to ensure that the following functions occur according to the stipulations of this KRPS:

- Verify requestor's identity and authorization as stated by this KRPS
- Build key recovery requests on behalf of authorized requestors
- Securely communicate key recovery requests to and responses from the KRA
- Participate in distribution of recovered keys to the requestor, as described by this KRPS

A KRO is a trusted person who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The functions performed in this role form the basis of trust in the entire KRS. ORC requires that subscriber organizations sponsoring persons to fill the KRO role shall ensure that the person(s) hold an active secret clearance or pass a thorough background check, including, but not limited to:

- Criminal history check that shows no misdemeanor or felony convictions
- Civil lawsuit history checks and a social security number trace to confirm valid number
- Personal, financial, and work/job reference checks, which show that the subject of the check is competent, reliable and trustworthy

- Financial status check showing that the subject of the check has not committed any fraud or is other wise financially trustworthy
- Education verification of highest or most relevant degree
- DMV records shall demonstrate no pattern of violations

ORC requires that subscriber organizations sponsoring persons that fill the KRO role shall ensure that the KRO:

- Be of unquestionable diligence, loyalty, trustworthiness, and integrity
- Have demonstrated security consciousness and awareness in all daily activities
- Have a technical understanding of the KRS system and the responsibilities of the KRO within that system
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties
- Be U.S. citizens
- KROs shall be trained in the authentication and verification policies and practices of the ORC ECA CPS and shall be trained in the performance of KRO duties
- KROs shall be trained in the third party requestor authorization validation in accordance with the subscribers' organization policy.

5.2.1.3 Other Trusted Roles

ORC SAs are responsible for administration of the ORC ECA, IA, CSA, KED and KRA workstation host computers and operating systems, as defined in the ORC ECA CPS Section 5.2.1.3.

A **Corporate Security Auditor** is responsible for reviewing the audit logs recorded by the ORC KED, KRA, and KRO. The Corporate Security Auditor backs up and archives all audit data and reviews the logs for events such as the following:

- Repeated failed actions
- Requests for privileged information
- Key Recovery Requests
- Attempted access of system files or databases
- Receipt of improper messages
- Suspicious modifications

A Corporate Security officer is also responsible for analyzing the key recovery requests to determine patterns of abuse by a KRA or a KRO. The Corporate Security Auditor is a distinct individual who is not in the direct reporting chain of the Information Technology or Operations Department and does not perform any additional trusted roles.

ORC will maintain lists, including names, organizations, and contact information, of those company individuals who act in trusted roles, and shall make them available during compliance audits.

5.2.2 Separation of Roles

At least two parties are necessary to do any key management or audit log operation. KED key-pair generation and initialization of KED tokens shall require the active participation of a CAA and the SA.

5.3 PERSONNEL CONTROLS

5.3.1 Background, qualifications, experience, and clearance requirements

Persons selected for KROs roles must meet the requirements of the subscriber's organization, but at a minimum meet minimum background, qualifications, experience, and clearance requirements. It is the responsibility of the sponsoring applicant organization to ensure that KROs employed by their organization meet the following requirements:

- Criminal history check that shows no misdemeanor or felony convictions
- Civil lawsuit history checks and a social security number trace to confirm valid number
- Personal, financial, and work/job reference checks which show that the subject of the check is competent, reliable and trustworthy
- Financial status check showing that the subject of the check has not committed any fraud or is other wise financially trustworthy
- Education verification of highest or most relevant degree
- DMV records shall demonstrate no pattern of violations
- A residence check to demonstrate that the person is a trustworthy neighbor

An active secret clearance shall be sufficient to meet these requirements. The results of these checks will not be released except as required by section 2.8 of the US Government ECA CP.

5.3.2 Background check procedures

Background check procedures are as specified in ORC ECA CPS Section 5.3.2.

5.3.3 Training requirements

All personnel involved in ORC ECA KRS operation will be appropriately trained in the following:

- Operation of the KRS software and hardware
- Operational and security procedures
- Stipulations of the US Government ECA KRP
- Stipulations of this ORC ECA KRPS

Training in the following areas is required for KROs:

- Security awareness and proper protection for cryptographic devices (when applicable)

- Training on KRO responsibilities

Note: It is the responsibility of the sponsoring applicant organization to ensure that LRAs, PKI Sponsors and CSAAs employed by their organization are properly trained.

5.3.4 Retraining frequency and requirements

Significant changes to the ORC KRS operation is accompanied by implementation of a training (awareness) plan that includes any retraining required for KRS operation staff, KRA or KRO personnel. The execution of such plan is documented in the ORC ECA Audit Notebook.

5.3.5 Job rotation frequency and sequence

Job rotation frequency and sequence will be as specified in ORC ECA CPS.

5.3.6 Sanctions for unauthorized actions

ORC will commence appropriate administrative and disciplinary actions against any person who violates this KRPS. Subscriber organizations will be required to commence appropriate administrative and disciplinary actions against personnel who violate the organization's policy relating to key recovery requests, to the greatest extent the law allows.

5.3.7 Contracting personnel requirements

Procedures to ensure that subcontractors perform in accordance with ORC ECA KRPS include appropriate administrative and disciplinary actions against subcontractor personnel who violate this KRPS.

5.3.8 Documentation supplied to personnel

Documentation sufficient to define duties and procedures for each role are provided to the personnel filling each role. This includes administrative and operations manuals for the host operating system, key escrow and recovery applications, and cryptographic modules, ORC Roles Manual; and this ORC ECA KRPS and the US Government ECA KRP.

6 TECHNICAL SECURITY CONTROLS

6.1 PROTOCOL SECURITY

All copies of the keys recovered by the KRAs will be protected continuously by two person controls during recovery and delivery to the authenticated and authorized requestor (or to the requestor's hardware token in the case of medium hardware assurance keys).

6.1.1 KED Protocol Security

Communications between the ORC ECA KED and KRAs is via credential authentication over client authenticated SSL, secure from protocol threats such as disclosure, modification, replay, and substitution on transactions between the KED and KRA.

During key escrow, the subscriber encrypts the private key using the KED transport public key. The KED key pair size is as high as the subscriber key pair or 1024 bits.

During medium hardware assurance key recovery, the key shall be exported from the KED to two KRAs at the KRA workstation, and then from the KRA workstation to the subscribers existing token or to a new token under the control of the subscriber or requestor. See section 4.2.1 for key recovery procedures through KRAs.

6.1.2 KRA - KRO Protocol Security

Communications between the ORC ECA KRA and KRO are secure from protocol threats such as disclosure, modification, replay, and substitution by using signed and encrypted email. The strength of all cryptographic protocols is medium assurance hardware.

6.1.3 Escrowed Key Distribution Security

The KED does not distribute the keys to the subscribers. All keys are recovered and distributed by the KRAs.

6.2 KED, KRA AND KRO PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Modules

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [current version of FIPS 140-1/2]. The ORC KRS only employs cryptographic modules validated to the FIPS 140-1/2, as identified in this section.

ORC KRAs and KROs private keys (for identity and encryption certificates) are protected by cryptographic hardware tokens that meet the criteria specified at FIPS 140-1/2 Level 2, as listed on the NIST website. The ORC KED private keys (for storage, transport, and SSL certificates) are protected by a hardware cryptographic module that meets the criteria specified at FIPS 140-1/2 Level 3 for key storage, as listed on the NIST website.

6.2.2 Private Key Control

The private components of KRA and KRO signature key pairs and encryption key pairs are under single person control. When not in use, KRA and KRO cryptographic hardware tokens must be

remove from the workstation/ computer and kept in the possession of the KRA and KRO or protected under lock and key.

The ORC KED private keys (for storage, transport, and SSL certificates) are controlled under a 'k of m' (two or more) person control.

6.2.3 KED Key Backup

The KED private keys (for storage, transport, and SSL certificates) are backed up and stored off site to provide secure continuity of key recovery operations. The backup keys are only created, stored, and restored under two-person control. The process of restoring the backup KED key is maintained by two party controls throughout.

6.2.4 Private Key Generation and Transport

The ORC KED keys pairs (for storage, transport, and SSL certificates) are generated by and stored in cryptographic modules.

6.2.5 Method of Activating Private Key

Passwords shall be used to activate the private keys associated with:

- ORC KED SSL, transport, and storage certificates
- KRA and KRO medium hardware assurance certificates/ tokens
- Subscriber's medium assurance and medium hardware assurance certificates/ tokens

6.2.6 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be left unattended or otherwise active to unauthorized access. The KED private key (associated with the SSL certificate) is deactivated upon completion of key archival, which ends the SSL session with the ORC ECA; or upon the completion of key recovery by the two KRAs ending the session. The KED is configured to time-out any SSL session inactive for over 30 seconds. The KED private key (associated with the transport) is deactivated immediately upon completion of key encryption or decryption activities. The KED is configured to deactivate any activated private key session after 60 seconds.

In order to deactivate the KRO and KRA private keys, KRO and KRA hardware tokens shall be removed from the token reader and protected by the KRO and KRA in accordance with the requirements stipulated in the ORC CPS Section 6.2.8.

6.2.7 Method of Deactivating Storage Key

Activated ORC KED hardware cryptographic modules are not left unattended or otherwise open to unauthorized access. If not in continuous use, they are deactivated via a manual logout procedure.

The ORC KED hardware token shall be stored in accordance with Section 5.1.2 of the ORC ECA CPS when not in use. The KED storage key is deactivated as soon as the key recovery operation is complete.

6.3 PRIVATE KEY ACTIVATION DATA

ORC ensures that generation, change, and management of private key activation data are in accordance with FIPS 140-1/2. KED SSL, transport, and storage keys are generated and managed directly on a hardware encryption module. The KED hardware encryption module activation mechanism is under two party controls.

6.4 COMPUTER SECURITY CONTROLS

6.4.1 KED

The KED server is dedicated to administrating the public key infrastructure and has only ORC CA related software installed. The KED server is behind a firewall provided by Checkpoint, installed on SUN hardware, that permits only https (in and out) and LDAPs (out) to and from the network. All upgrades will be from the original equipment manufacturers and software vendors.

6.4.2 KRA and KRO Workstation

ORC requires that KRA workstations use operating systems that:

- Require authenticated logins
- Provide discretionary access control
- Provide operating system self-protection
- Provide process isolation
- Provide a security audit capability

ORC KRA workstation equipment is hosted on Common Criteria evaluated platforms in support of computer security assurance requirements (hardware, software, operating system) operating in an evaluated configuration.

6.4.3 Anomaly Detection

The ORC key recovery infrastructure is capable of detecting anomalous key recovery activities and behavior and reporting them to appropriate ORC ECA authorities for further action as described in this KRPS.

6.5 LIFE CYCLE TECHNICAL CONTROLS

Individuals with trusted roles within the ORC KED facility use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

Security management controls include the execution of tools and procedures that ensure that the operational systems and network adhere to the security requirements of the ORC ECA CPS and this KRPS. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

6.6 NETWORK SECURITY CONTROLS

Access to the ORC KRS is protected by a firewall specifically allocated to protection of the ORC ECA suite. Only required accounts are present on the firewall. HTTPS shall be the only type of data access that is allowed in. HTTPS and LDAP are the only packet types allowed out. The firewall itself shall be secured in the locked ECA environment area and not accessible over the network. An approved trusted individual shall make all changes at the firewall station itself.

6.7 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are stipulated in Section 6.2.1.

7 POLICY ADMINISTRATION

7.1 POLICY CHANGE PROCEDURES

This KRPS is maintained under the specification change procedures identified in the ORC ECA CPS, Section 8.1.

7.2 PUBLICATION AND NOTIFICATION POLICIES

This KRPS will be published as specified in ORC ECA CPS, Section 8.2.

7.3 POLICY APPROVAL PROCEDURES

This KRPS will be approved based on the procedures specified in ORC ECA CPS, Section 8.3.

Appendix A: References

Certificate Policy for External Certification Authorities, Version 2.0, June 4, 2003; Internet; <http://iase.disa.mil/pki/ieca/Documents/ECA%20CP%20v2.0%206-4-2003%20signed.PDF>

Key Recovery Policy for External Certification Authorities, Version 1.0, June 4, 2003; Internet; <http://iase.disa.mil/pki/ieca/Documents/ECA%20KRP%20v1.0%206-4-2003%20signed.PDF>

ORC ECA Certificate Practice Statement, Version 2.1, February 11, 2004

The Common Criteria Evaluation and Validation Scheme, *Validated Products List*, November 6, 2003; Internet: <http://niap.nist.gov/cc-scheme/ValidatedProducts.html>

Appendix B: Acronyms and Abbreviations

CA	Certification Authority
CAA	Certificate Authority Administrator
CMA	Certificate Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSAA	Code Signing Attribute Authority
CSOR	Computer Security Objects Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECA	External Certification Authority
EPMA	ECA Policy Management Authority
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
FTP	File Transfer Protocol
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
IP	Internet Protocol
ISO	International Organization for Standards
IT	Information Technology
KEA	Key Exchange Algorithm
KED	Key Escrow Database
KRA	Key Recovery Agent
KRO	Key Recovery Official
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
KRS	Key Recovery System
MD	Maryland
NIST	National Institute of Standards and Technology

OCSF	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RD	Road
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SCVP	Simple Certificate Validation Protocol
SDN	Secure Data Network
SSL	Secure Socket Layer
US	United States
USC	United States Code
USD	United States Dollar
WWW	World Wide Web