.au Domain Administration Ltd

Registry Technical Specification

Prepared by Dr Greg Watson, Associate Professor Jim Breen and Dr Len Whitehouse of Monash University

Version 1.0

September 2001

1. INTRODUCTION

This document defines the technical requirements of the Registry Service to be undertaken by a Registry Operator. The Technical Specification forms part of the Request for Tender. auDA may choose to amend any or all of the Specification from time to time in order to address new or changing requirements. When amendments are made to the Specification, the version number of the document will be updated.

Each section provides details of the minimum requirements which must be met by prospective Registry Operators. Tenderers are free to nominate higher performance or service levels, or specify additional functionality in any or all aspects of the Specification. However this is not necessary in order to be considered to have met the technical requirements.

Tenderers must respond where they have been asked to supply additional information. Tenderers that do not have or do not intend to address a particular item should respond with 'Not applicable'.

In a number of locations in the Specification the phrase 'to be determined by auDA' or similar has been used. This indicates that the particular information is currently unknown or still under development. The correct information will be inserted into the Specification when it becomes available. It is not expected that this information will impact on the Tenderers ability to respond to these requirements.

2. FUNCTIONAL SPECIFICATIONS

2.1 Registry Database

A Registry Operator must develop and operate a Registry Database which conforms to the structure described in this section.

2.1.1 Structure

The Registry Database specification is deliberately abstract so that it provides prospective Registry Operators freedom to choose a particular database system which best suits their requirements.

The Registry Database consists of four sets of records. The definition of these records is as follows:

(a) Registrar Records. These hold administrative and contact information about each accredited Registrar. They also hold essential control information for the Interim Registrar-Registry Protocol, such as the PGP key information.

(b) Registrant Records. These hold administrative and contact information about each Registrant.

(c) Domain Records. These hold the name and nameserver IP address and hostname information about each registered domain name. One or more Domain Records are associated with each Registrant Record.

(d) Contact Records. These hold contact information about the technical and administrative contacts for a domain name. Two or more Contact Records are associated with each Domain Record.

2.1.2 Field Labelling

A set of short mnemonic field labels is specified for the data items in the database. Registry Operators are not required to use these labels internally, but they will be used to identify fields in the IRRP and for data escrow purposes.

2.1.3 Field Coding

Three types of field coding are used in the database definition:

(a) Numeric: a field representing an integer number.

(b) Date: a field representing a date.

(c) Variable-length character (vc): a text field where the number in parentheses after each field description is the minimum length in 8-bit bytes.

All text fields must be coded in UTF-8 (Unicode UCS Transformation Format, 8-bit), as defined in Section 3.8 of the Unicode Standard 3.0 (not modified in the current 3.1.1 Annexure). This means that 7-bit ASCII characters are recorded without change, and other characters from the Unicode set are coded in sequences of bytes with the most significant bit (MSB) set. (This effectively leaves options open for internationalisation, including the domain names themselves. In the case of domain names, other transformation formats may be used in zone files and DNS software, but a consistent coding must be used in the Registry Database.)

2.1.4 Database Format Details

Details of the Database Record formats are provided in Appendix A.

2.1.5 Predefined Code Fields

There are a number of fields in the Database Record specification which require the use of predefined codes. Registry Operators must enforce these codes when processing Registrar requests and when exporting data from the Database.

Field Name	Type	Code to Use
rar-code	vc(20)	Allocated by auDA
rar-type	vc(10)	To be determined by auDA
rar-bus-code-type	vc(10)	ACN, ABN, RBN and others as determined by auDA
rar-address-scode	vc(10)	ACT, NSW, NT, QLD, SA, TAS, VIC, WA or appropriate abbreviation for foreign addresses
rar-address-ccode	vc(2)	ISO-3166-1 2-digit country code
reg-code	vc(20)	REG-NNNNNNNNNN
reg-registrar	vc(20)	Same as rar-code
reg-type	vc(10)	Same as rar-type
reg-bus-code-type	vc(10)	Same as rar-bus-code-type
reg-address-scode	vc(10)	Same as rar-address-scode
reg-address-ccode	vc(2)	Same as rar-address-ccode
domain-reg-code	vc(20)	Same as reg-code
domain-code	vc(20)	DOM-NNNNNNNNNN
contact-reg-code	vc(20)	Same as rar-code
contact-code	vc(20)	CON-NNNNNNNNNN
contact-domain-code	vc(20)	Same as domain-code
contact-type	vc(5)	T or A
contact-address-scode	vc(10)	Same as rar-address-scode
contact-address-ccode	vc(2)	Same as rar-address-ccode

Codes used to identify Registrant Records, Domain Records and Contact Records will use a 10-digit number prefixed with ‘REG-‘, ‘DOM-‘ and ‘CON-‘ respectively. Registry Operators will allocate a

unique number to each record from a range of numbers supplied by auDA.

2.1.6 Database Service Performance and Availability

The following performance and availability criteria are to be met by the Registry Database. Definitions for performance criteria are provided in Appendix D:

(a) **Service availability**: At least 99.5% per calendar month;

(b) **Processing time**: At least 95% of enquiries serviced within 1.5 seconds. At least 95% of create/modify/delete requests serviced within 3 seconds;

(c) **Planned outage**: limited to a maximum of 8 hours per calendar month; between 0600 and 1400 AEST Sundays. 3 days notice to be given to Registrars;

(d) **Extended outage**: limited to a maximum of 18 hours per calendar month; between 0600 and 2400 AEST Sundays. 28 days notice to be given to Registrars.

2.2 Registry Access Protocol

The purpose of the Registry Access Protocol (RAP) is to allow Registrars to perform various operations which are necessary when creating, modifying and deleting domain name registrations. The RAP provides a remote interface into the Registry Database.

Traditionally domain name registries of ccTLD's have been developed on an ad hoc basis to suit domestic circumstances. These registries differ in most aspects, including data content and format, method of operation, access requirements and access protocols. However they almost universally employ a single 'thick' registry (i.e. one that contains both DNS and registrant information) for the domain and its sub-domains. An exception is AUNIC which contains Registrant information and some domain information, but zone file information is maintained separately.

At the gTLD level the situation is also diverse. For existing gTLD's (.com, .net and .org) a 'thin' registry (i.e. one that contains only DNS information) is used. The new gTLD's (.biz, etc.) will employ 'thick' registries.

RAPs used to access the registries also vary considerably. Most ccTLDs rely on a simple text based protocol using a variety of mechanisms for authentication and security. The more demanding requirements for gTLDs have resulted in the development of more

rigorous protocols. The table below shows this arrangement for various TLDs.

Who	Registry	Registrar	RAP	Transport	Security	Authentication
Nominet (.uk)	Thick	Open Tag Holder	Text	SMTP	None	PGP key
CIRA (.ca)	Thick	Accredited	Text XML	SMTP SSL Web form	PGP	Password
ISOCNZ (.nz)	Thick	Accredited	Text	Web form	SSL	Password
AUNIC (com.au)	Thinner	Single	Text	SMTP	None	Password
Verisign (.com, .net, .org)	Thin	Accredited	RRP	TCP	None SSL	Password
Newlevel (.biz)	Thick	Accredited	EPP	BEEP TCP	Transport dependent	Password

In determining the appropriate RAP for use in .au it is essential that consideration be given to minimising barriers to entry for Registrars while promoting a competitive environment. The following principles are fundamental to the selection of the .au RAP:

- the RAP should be mandated by auDA;
- the RAP should be placed in the public domain;
- all open 2LD's should be accessible using the same RAP;
- a minimum open-source implementation of the RAP should be available;
- the RAP should operate with a variety of transport mechanisms;
- the RAP should meet the technical requirements for access to the Registry; and
- no or minimum licence fees should apply to use of the RAP.

In the Competition Panel recommendations for Technical Requirements for Registry and Registrar, the panel notes in relation to the IETF Provisioning Registry Protocol (EPP) that:

'2.3 The registry-to-registrar protocol should be consistent with IETF standards. […] This protocol is based on using XML (extensible markup language) from the World Wide Web Consortium to provide an extensible protocol that supports the addition of new services. This is important in a multiple registry environment, where not all registries will provide the same features. It also allows support for the policy rich environment to be incorporated in the protocol (eg. incorporating sign-off procedures from an independent body to approve certain domain names), and will support the different requirements of the various 2LDs within .au.'

While this statement is supported in principle it should be noted that:

(a) there is considerable uncertainty as to the final arrangement of Registries operating in .au and no guarantee that it will be a multiple Registry environment;

(b) it is envisaged that any 'sign-off procedures' in a Registry will be fully automatic decisions and the application of policies for domain name approval will be the responsibility of Registrars only;

(c) there is no indication that different requirements of the 2LDs within .au will necessitate any intervention on the part of a Registry;

(d) EPP has not yet been adopted as an industry standard; and

(e) there is no public domain implementation of EPP currently available.

In view of these issues it is considered too early to mandate the use of EPP at this stage.

2.2.1 RAP Requirements

Registry Operators are required to support the IRRP as defined in 2.2.2. auDA will provide a reference implementation of IRRP for use by Registrars and Registry Operators.

auDA is continually monitoring developments of the IETF Provisioning Registry Protocol, and once the protocol is adopted as an IETF standard will undertake an analysis of the protocol. The objective of this analysis will be to ensure that the protocol will promote strong market development and is consistent with the principles outlined in 2.2. Provided that the protocol meets these objectives and the existing IRRP is found to be an inhibiting factor to this market development, auDA may then require that the Registry Operators support the EPP.

Registry Operators will be required to continue support the IRRP regardless of the outcome of this process. This will ensure that barriers to entry for future Registrars are minimised.

Because additional protocol support may be required in the future, it is suggested that Registry Operators design their Registry software in such a way so that is in not dependent on a particular RAP. For example, a common registry access protocol layer could be provided which allows different RAPs to be supported through separate modules.

2.2.2 Interim Registry Registrar Protocol (IRRP)

This section describes an Interim Registry-Registrar Protocol (IRRP) for use between Registrars and Registry Operators. The protocol is to be used until such time as standard IETF protocols such as the Extensible Provisioning Protocol are approved and implemented.

The IRRP should be considered a work in progress. Registry Operators and Registrars will have the opportunity to suggest modifications or improvements to the protocol during the testing period.

This interim protocol has been designed to be as simple as possible in its implementation and operation in order to minimize any duplication with the implementation of EPP or other standard protocols.

This section must be read in conjunction with the Registry Database specification (above), as the names of data items are aligned in the two sections.

2.2.2.1 Overview

The IRRP is message based, with all messages passing between Registry Operators and Registrars. The purpose of the messages is to enable the creation, update, deletion and recall of Registrant, contact and domain information from the Registry Operators' databases, and to make other essential enquiries such as the availability of specific domain names.

The message dialogue is in the form of action requests from the Registrar and responses from the Registry Operator. Every action request message from a Registrar will result in a response from the Registry Operator. There are no unsolicited messages from the Registry Operator.

Messages will be passed between Registry Operators and Registrars in the following ways. A response to a request message will always be sent using the same transport method:

(a) SMTP. The Registry must dedicate an SMTP service to this message stream and nominate a single email address to which requests will be sent. Responses will be sent to the email address identified by the “From: “ line in the incoming email message.

(b) SSL (Secure Socket Layer). The Registry must dedicate an SSL server to this message stream.

Registry Operators must maintain a log of all incoming and outgoing IRRP messages for audit trail and recovery purposes.

2.2.2.2 Security and Authentication

Data security of IRRP messages will be provided by one of two mechanisms depending on the transport method employed.

(a) For SMTP transactions, messages from the Registrar to the Registry Operator will be encrypted using the public PGP key

of the Registry Operator. Messages from the Registry Operator to the Registrar will be encrypted using the public PGP key of the Registrar.

(b) SSL transactions will rely on the security provided by the SSL protocol.

Both transport methods will provide authentication by signing the message with the private PGP key of the Registrar. Responses from the Registry Operator to the Registrar will be unsigned.

2.2.2.3 Message Structure

Each IRRP message will consist of multiple lines of text. The characters in the text will be in UTF-8 coding. Where this means that characters are outside the set of printable ASCII characters, messages using SMTP transport must be handled in appropriate MIME coding, e.g. quoted-printable or base64, **prior** to encryption.

Each line of message text will consist of a key/value pair separated by a colon character (':', octal 072) and a space character (octal 040). The line will be terminated by a newline character (octal 012). Where the last character of the line (prior to the newline) is a backslash character ('\', octal 134), the following line is a continuation of the value.

Key strings are one of the following:

(a) **irrp-sequence**: Provides a numeric sequence number for the message. Marks the beginning of each message. The value field consists of the sequence number;

(b) **irrp-action**: An action request submitted by a Registrar to a Registry Operator followed by zero or more additional parameters;

(c) **irrp-response**: A response from a Registry Operator following a request submitted by a Registrar. The value will consist of a response/error code followed by further parameters and human-readable information as appropriate. A list of response/error code is provided below;

(d) **irrp-inf**: Information associated with a request or response. One or more **irrp-inf** lines will typically follow an **irrp-response** line;

(e) database field name (any valid database field name appropriate to the request or response). The value consists of the initial, current or replacement contents for the database field ;

(f) **irrp-end:** Marks the end of each message.

Key strings will be case-insensitive.

Normally each message from a Registrar to a Registry Operator must deal with a single Registrant and associated domain and contact information. The only exception is messages containing the **domain-enquire** action. More than one of these can occur in the one message.

Each message between a Registrar and a Registry Operator must begin with an **irrp-sequence** line with a value of an integer sequence number one higher than the previous message. The maximum possible sequence number is 2^{31}-1. The Registrar is responsible for generating the sequence number. A Registry Operator will use the same sequence number in the associated response. A break or reset in the sequence will not invalidate enquiry messages, but it will be noted in the response by the Registry Operator. Messages which create or update records in the database **must** have a sequence number higher than that of the preceding message, or the request will be rejected.

The first line in an action request message will consist of the Registrar's unique identification code. This line **must** precede the other lines and must be sent in plain text as it will be used to identify the Registrar to the Registry, and enable decryption and/or authentication to take place. This line is not used in response messages.

Lines starting from the first **irrp-sequence** line to the last **irrp-end** line will then be first signed and then encrypted (for SMTP). Refer to RFC2014 and RFC2440 for details on the OpenPGP-MIME and OpenPGP standards.

2.2.2.4 Action Messages

Action messages and their corresponding responses are provided in Appendix B.

2.2.2.5 Actions Not Handled by IRRP

The IRRP is intended to cover the main interactions between Registry Operators and Registrars. Other interactions can be identified, however their handling is considered to be outside the scope of an interim system, and it is intended that they be covered by alternative procedures.

The primary interaction not handled by IRRP is the creation and update of Registrar Records in the database. It is expected this will be effected by the internal procedures of the Registry Operator.

2.2.2.6 Response and Error Codes

On successful completion of an action request, a response code in the form 'RNNN' will be issued using the **irrp-response** key. When an action has not been successful an error code in the form 'ENNN' will be issued. A short description of the error is also supplied.

In the case of **irrp-response** lines which indicate an error code, one or more **irrp-inf** lines will typically follow the **irrp-response** line providing a more detailed explanation of the cause of the failure.

IRRP response and error codes are listed in Appendix C.

2.3 Authoritative Nameserver Service

Each Registry Operator must provide an authoritative nameserver for the domain(s) it operates. The nameservers must comply with IETF standards for the Domain Name Service (RFC1035, RFC2181 and RFC2182). Registry Operators must also commit to the implementation and operation of DNS extensions in such areas as internationalisation, security, etc. when these have been adopted by the IETF and have achieved a satisfactory level of community support.

2.3.1 Nameserver Reliability

In compliance with the relevant RFCs, the authoritative nameserver service must be implemented using a number of nameservers to maintain high levels of availability. The Registry Operator must operate at least the primary nameserver, and may cooperate with other Registry Operators, carriers, or ISPs to host secondary nameservers. The Registry Operator will be responsible for achieving the levels of service specified below. It is expected that at least the primary nameserver will be located in a carrier-class data centre, with redundant network connections (through multiple telecommunication carriers) of at least 2 Mbps capacity each, redundant air-conditioning systems, redundant power supplies (including UPS and power backup), fire detection and control systems, and 24-hour manned security systems.

As geographical and carrier dispersion of nameservers is considered essential for reliability (see RFC2182) it is expected that Registry Operators will arrange for secondary nameservers to be operated in at least two Australian cities.

2.3.2 Zone File Maintenance

The Registry Operators will use the Registry Database as the authoritative source for creation of zone file information. Registry Database updates must be reflected in the zone file(s) within 15 minutes of completion.

2.3.3 Provision of Zone Files to auDA

A copy of the zone file(s) must be made available to auDA on request.

2.3.4 DNS Service Performance and Availability

The following performance and availability criteria are to be met by the authoritative nameservers. Definitions for performance criteria are provided in Appendix D:

(a) **Service availability**: At least 99.999% per calendar month;

(b) **Processing time - nameserver resolution**: At least 95% to be processed in less than 1.5 seconds;

(c) **Update delay time**: At least 95% of updates to the Registry Database available to the nameserver service within 15 minutes;

(d) **Cross-network nameserver performance**: Maximum RTT (Round Trip Time) of 300ms, and maximum packet loss of 10%;

(e) **Planned outages**: Nil.

2.4 Public WHOIS Service

It is intended that each Registry will offer a public WHOIS service for the 2LD(s) under its management. auDA will also offer a public WHOIS service for the entire .au domain.

2.4.1 Central Public WHOIS

For the purposes of enabling auDA to provide a central public WHOIS service, each Registry must provide auDA with a copy of the current database records associated with each 2LD at least once in each 24 hours. The database records are to consist of multiple lines of UTF-8 text in the 'key: value' format using the field labels in the Database Specification shown in Appendix A.

The database file(s) are to be transmitted to a host or hosts using an appropriate secure file transfer system as advised by auDA. Details of the transfer method and time of transfer will also be advised by auDA at a later time.

2.4.2 Registry-provided Public WHOIS

Each Registry must provide a reliable public WHOIS service for the 2LD(s) under its management. The WHOIS service must be fully

compliant with RFC954 and must conform to auDA's stated policies with regard to each 2LD. In particular, auDA will specify:

(a) the information which may be provided as a result of a WHOIS enquiry. This may vary between 2LDs;

(b) the nature of the queries that may be serviced, in particular the fields against which searches can be made, and the extent to which "wild-card" searches can be accepted;

(c) the performance and service levels of the WHOIS service.

Registry Operators should develop their WHOIS service in such a way that these factors are taken into consideration.

2.4.3 WHOIS Data Set

The following information is to be potentially available from the Registry Database as a result of a WHOIS enquiry. Fields within this set may be restricted by auDA policy for some 2LDs:

(a) the fully qualified domain name;

(b) the hostnames of the primary nameserver and at least one secondary;

(c) the corresponding IP addresses of those nameservers;

(d) the identity of the Registry;

(e) the identity of the Registrar;

(f) the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the domain name Registrant;

(g) the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the domain name;

(h) the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the domain name;

(i) the original creation date of the domain and term of the registration; and

(j) the date of the most recent update of any part of this set of information.

The WHOIS service may be provided either directly from the Registry Database or from a database dedicated to the service. If a dedicated database is used, it must be regularly updated from the Registry Database (see below for minimum update delays.) Registry Operators must be able to demonstrate that integrity will be maintained between the WHOIS files (if any) and the Registry Database.

2.4.4 WHOIS Enquiries

The public WHOIS service to be provided by Registry Operators is to be oriented towards providing information about specific domain names or constrained sets of domain names. Bulk access to WHOIS information will be managed by auDA.

The following search keys are to be accepted by the Registry-provided WHOIS services. Searches are to be case insensitive:

(a) the name of the domain;

(b) a string of five or more contiguous characters to be matched at the beginning of, or within the name, of the domain;

(c) the name of the Registrant;

(d) two or more words within the name of the Registrant;

(e) the hostname of a primary or secondary nameserver.

Where a key results in multiple matches, a short list containing the matched items (domain names or Registrant names) is to be returned to the user. Only when a user has identified a single domain name or a single Registrant is the full WHOIS information to be returned.

Repeated WHOIS enquiries from individual hosts are to be limited in number in a given time period. Hosts exceeding this limit are to be blacklisted for a set period.

2.4.5 Format of WHOIS Information

The information to be provided by WHOIS service will consist of multiple lines of UTF-8 text terminated by ASCII CRLF. Each item or group of items as listed above is to be preceded by a short description.

The following may be taken as an example of a suitable format:

```
Domain: foobar.com.au
Registry: Dominant Names Pty. Ltd.
Registrar: Acme Oz Registrations Pty. Ltd.
Primary Nameserver: dns1.foobar.com.au (123.234.1.1)
Secondary Nameserver: dns2.foobar.com.au (123.234.2.1)
Registrant: Foo Bar Pty. Ltd, 1 Swanston St, Melbourne VIC
```

```
3000; info@foobar.com.au; (ph) +61396991234; (fax) +61396992222
Admin Contact: Fred Smith, Foo Bar Pty. Ltd, 1 Swanston St,
Melbourne VIC 3000; fred@foobar.com.au; (ph) +61396991239;
(fax) +61396992222
Tech Contact: George Scott, Flybynight Sysadmins, Wellington
Rd, Clayton 3168; george@fbn.net.au; (ph) 0418123456
Created: 1998-2-15
Duration: 3 years
Modified: 2001-5-12
```

2.4.6 WHOIS Service Performance and Availability

The following performance and availability criteria are to be met by the WHOIS service. Definitions for performance criteria are provided in Appendix D:

(a) **Service availability**: At least 99.5% per calendar month;

(b) **Processing time**: At least 95% of enquiries serviced within 1.5 seconds;

(c) **Update delay time**: At least 95% of updates to the Registry Database available to the WHOIS service within 15 minutes;

(d) **Planned outage**: Limited to a maximum of 8 hours per calendar month; between 0600 and 1400 AEST Sundays. 3 days notice to be given to Registrars;

(e) **Extended outage**: Limited to a maximum of 18 hours per calendar month; between 0600 and 2400 AEST Sundays. 28 days notice to be given to Registrars;

(f) **WHOIS limits**. Maximum number of matches to be returned in response to a query: 10. Maximum number of queries to be accepted from a single host: 20 per hour and 100 in any 24-hour period. Blacklist period: 24 hours.

2.5 Legacy Data

Registry Operators will be required to pre-load their Registry Database, nameserver and WHOIS servers with existing domain name and Registrant information prior to commencing operation.

Legacy data will be supplied using the same formatting conventions as described in Section 5: Data Escrow Requirements. Field names will conform to those described in Appendix A. However, it is unlikely that the data will be supplied using the same structure as described in 2.1.1. It will be the responsibility of the Registry Operator to ensure that the legacy data is converted into an appropriate format suitable for the Registry Database.

Details of the record structure and transfer method will be advised by auDA at a later time.

2.6 Functional Specification Response

Tenderers must respond to the Functional Specification by indicating how they intend to meet the minimum requirements of the Specification. In particular, Tenderers should indicate how they intend to:

(a) implement the Registry Database as per the Specification, including providing details of the proposed hardware and network configuration;

(b) implement the Registry side of the Interim Registry-Registrar Protocol as per the Specification;

(c) provide a Public WHOIS service as per the Specification, including providing details of the proposed hardware and network configuration;

(d) provide an authoritative nameserver service as per the Specification, including providing details of the proposed hardware and network configuration;

(e) implement an additional RAP such as an IETF standard protocol once it has been approved, at a time to be set by auDA;

(f) meet the Performance Specifications and Service Levels for the Registry Database, WHOIS and nameserver services as set out in the Specification.

3. SECURITY ARCHITECTURE

This section of the tender specification relates to security aspects of the proposed Registry System. Due to the critical nature of the information and services to be provided by the Registry, adequate protection is required for all aspects of the system and the environment in which it is to operate.

It is a requirement of the Tender that proposed Registry Systems comply with the following Australian Security Standards:

(a) Information Technology – Code of practice for information security management (AS/NZS ISO/IEC 17799:2001, previously AS/NZS 4444.1:1999);

(b) Information Security Management, Part 2: Specification for information security management systems (AS/NZS 7799.2:2000, previously AS/NZS 4444.2:2000).

The above security standards are generic and not all areas addressed are relevant to this Tender. Tenderers should aim to provide a secure computing environment for reliable and continuous operation of the proposed Registry System. Data integrity is to be emphasized. Tenderers should aim to develop or use systems which ensure maximum protection of data against accidental or deliberate changes or corruption.

The security standards cover a variety of development platforms and run-time environments. It is recognized that Tenderers have a wide range of options when considering solutions for the proposed Registry System. Solutions may range from a single server to provide all facilities for a small Registry, to a cluster of servers for all Registries. Servers may be based on a variety of platforms (e.g. Unix, NT etc.). Tenderers may propose new purpose built systems, or may elect to incorporate the Registry System into existing environments. Application software may be entirely web based or may function as part web based and part client/server via a local area network.

With this variety of options, Tenderers should respond to security issues which are appropriate to their solutions. Where an item does not apply, Tenderers should respond with “Not applicable”.

In addition to a statement of general compliance with the above, Tenderers are requested to provide detailed responses to the following security issues.

3.1 Security Policy

A clear statement is required from senior management of the Tenderer’s commitment to and support of information security.

If an existing Information Security Policy Document is available, it should be included in the supporting documentation accompanying the Tender.

Details are also required of the Tenderer's on-going review of the security policy in response to changes affecting risk assessment, security incidents and technological change.

3.2 Organisational Security

This section relates to the management of information security within an organisation. Tenderers are requested to provide details of the management structure established to implement an information security policy within the organisation and the involvement of staff and users throughout the organisation. Commitment to the information security policy at a senior management level is considered essential.

Responses are required to the following items:

(a) State the name, ranking and other responsibilities of the Information Security Manager within the organisation;

(b) State the policy for allocating responsibility for information assets within the organisation and the authorisation process for information processing facilities;

(c) State the level of reliance the organisation places on external information security advice and list the level of use of external security advisors over the past two years;

(d) List membership of security groups and industry forums;

(e) Provide details of the most recent security audit undertaken by the organisation (internal or external);

(f) List identified risks from third party access to the organisation's sites or systems, e.g. cleaners, maintenance staff, software specialists, trading partners and joint ventures;

(g) Provide details of third party contracts which will impact on the current Tender;

(h) Provide details of outsourcing arrangements which may impact on the tender.

3.3 Asset Classification and Control

This section relates to the identification and protection of information assets within the proposed Registry System. Individuals within the

Tenderer's organisation should be assigned responsibility for information assets and be accountable for those assets and their use.

In this Tender, information assets include databases, data files, system documentation, user manuals, training material, operating instructions and procedures, archived material, application and system software, development tools and utilities. Physical assets include computers, peripherals, communications equipment, magnetic media, other technical equipment, furniture and accommodation. Service assets include computer and other equipment maintenance, and general utilities, e.g. heating, lighting, power, air-conditioning.

Responses are required to the following items:

(a) Provide an itemised list of information assets in the proposed Registry System;

(b) Describe the facilities within the organisation used to maintain an appropriate inventory of information assets;

(c) Describe the facilities within the asset inventory system to assign protection levels to tables of information and/or individual fields;

(d) Provide details of the classification of information within the proposed Registry System;

(e) Describe how the above classification of data will be used to protect data from illegal use or copying;

(f) Describe the handling procedures for each classification type in terms of the following types of information processing activities: copying, storing, transmission by post, fax, electronic mail, spoken word, mobile phone, voicemail, or answering machine;

(g) Describe the handling procedures for the destruction of information in each classification type;

(h) Describe the facilities provided for labeling outputs (reports, tapes, disks, CDs, cassettes) and electronic documents to identify sensitive or critical information.

3.4 Personnel Security

This section deals with security aspects of staffing within an organisation which are specifically designed to reduce the risks of human error, theft, fraud and misuse of facilities and information. Security responsibilities apply to all staff within an organisation, permanent, part-time, contract and service staff.

Responses are required to the following items:

(a) Provide examples of job specifications within the organisation detailing the information security policy as applied to individual positions;

(b) Describe the validation checks performed during the staff selection process to ensure an applicant's details (academic, professional, employment history) are complete and accurate;

(c) Describe additional checks undertaken when existing staff members are promoted to a higher level requiring access to financial or confidential information;

(d) Describe period review procedures established for monitoring the performance of staff with access to sensitive information;

(e) Describe or provide examples of confidentially and/or non-disclosure agreements employees are required to sign as part of the terms and conditions of employment;

(f) Describe the levels of training to be provided to staff and users of the proposed Registry System in the area of information security;

(g) Describe the procedures to be incorporated into the proposed Registry System for reporting, registering, investigating and resolving security incidents;

(h) Describe procedures for reporting software malfunctions in the proposed Registry System;

(i) Describe the disciplinary process to be applied to employees violating security policies and procedures.

3.5 Physical and Environmental Security

This section relates to physical aspects of security, namely, secure areas to house information systems, protection of equipment, provision of a secure power supply and cabling infrastructure, and a clear desk policy to prevent unauthorised access to information.

3.5.1 Secure Area

The proposed Registry System must be located in a secure environment with adequate protection from unauthorised access, damage to equipment and interruption of the Registry service. It is a requirement of the Tender that the site be equipped with 24-hour manned security systems.

Responses are required to the following items:

(a) State in which city or cities the proposed Registry System will be located;

(b) Describe the physical environment which will be used to house the Registry System and staff required to operate it. If available, provide plans and diagrams of the layout of the site;

(c) Describe security features of the proposed environment and methods for controlling access to the facility;

(d) Provide a risk assessment for the site at which the required 24-hour manned security systems will be located;

(e) Describe the construction and security aspects of the building to house the system and nominate secure areas within the site;

(f) Describe security access controls to restrict access to the site to authorised personnel only;

(g) Provide details of fire protection facilities incorporated into the security system;

(h) Describe the security mechanisms used to control access to secure areas by staff and visitors;

(i) Describe methods for securing offices and documents within the site and any special arrangements for access to computer rooms and equipment;

(j) Describe procedures for authorising and monitoring access of visitors to the site;

(k) Describe procedures for processing restricted access for third party personnel (e.g. maintenance engineers);

(l) Provide details of procedures and holding areas for deliveries (e.g. printer paper) to the site.

3.5.2 Equipment Security

Equipment within the secure area should be protected to prevent loss, damage or disruption of the Registry service.

Responses are required to the following items:

(a) Provide a layout diagram of all equipment associated with the proposed Registry System showing security boundaries;

(b) Provide the maintenance schedule for equipment in the proposed Registry and details of procedures to be followed when equipment is shipped off-site for maintenance;

(c) Describe controls to minimize the risks of theft, fire, explosives, smoke, water damage, dust, vibration, chemical effects, electricity supply interference, electromagnetic radiation;

(d) State the policy to be adopted regarding eating, drinking and smoking in equipment areas;

(e) Provide details of the monitoring of environmental conditions within equipment areas to ensure continuous operation of the proposed Registry System;

(f) Provide details of the environment surrounding the secure area together with a risk analysis of possible disaster situations, e.g. fire in a neighbouring building or water leaks from a higher floor.

(g) Describe measures taken to ensure that the site has a reliable power supply, including details of uninterruptible power supplies and back-up power generators;

(h) Provide details of emergency switches in secure areas to shut off power to equipment during emergencies. Also provide details of emergency lighting;

(i) Provide details of measures to prevent damage caused by lightning strikes.

3.5.3 Cabling Security

It is a requirement of this Tender that power and telecommunication lines be secured from interception and damage.

Responses are required to the following items:

(a) Describe the method of access of power and telecommunication cables (underground is preferred);

(b) Provide network wiring diagrams showing all network connections in the proposed Registry System;

(c) Provide electrical wiring diagrams for the proposed Registry System, specifically indicating areas (e.g. ducts) sharing both power and network or communication cables;

(d) Provide details of alternative cabling (e.g. optical fibre) to minimize possible interference or security breaches;

(e) Describe procedures to be adopted to ensure that unauthorised devices are not attached to cables.

3.5.4 Equipment Off-Premises

This section applies to any equipment associated with the proposed Registry System which is stored or used off-site. This includes mobile computers, organizers, mobile phones, manuals and documentation.

Responses are required to the following items:

(a) Provide a list of equipment which is to be stored or used off-site from the proposed Registry System;

(b) Describe procedures to be followed to register off-site equipment and to record access to and from the site;

(c) Describe procedures to ensure that off-site equipment and documentation are secure when off-site;

(d) Describe procedures to ensure that communication between off-site equipment and the Registry System does not compromise normal security requirements.

3.5.5 Disposal of Equipment

Disposal or re-use of equipment from the Registry System should be subjected to special checks to ensure that all information has been erased from the equipment.

Responses are required to the following items:

(a) Describe the procedures to be followed in the disposal or re-use of equipment from the Registry System;

(b) Describe the methods to be adopted for erasing information from magnetic storage devices;

(c) Describe procedures for destroying damaged storage devices to ensure no data can be copied from the devices.

3.5.6 Clear Desk Policy

The adoption of clear desk and clear screen policies by staff reduces the risk of unauthorised access to data. Papers and documentation are stored in secure cabinets and accessed only when they are required for use. System tasks should terminate to blank screens requiring re-entry of passwords if screens are not accessed for a specified period.

Responses are required to the following items:

(a) Describe the “clear desk” policy to be applied in the proposed Registry System;

(b) Describe systems to be incorporated in the Registry software to ensure “clear screen” operation.

3.6 Communications and Operational Management

This section considers factors affecting the correct and secure operation of the proposed Registry System.

3.6.1 Operational Procedures

All operational procedures must be fully documented with any changes subjected to formal management review and approval. Operational procedures are required for all information processing tasks, error handling, interaction with maintenance and support specialists, system input and output requests, and restart and recovery procedures in the event of system failure.

Responses are required to the following items:

(a) Provide examples of operational procedures developed by your organisation;

(b) Describe systems developed for operational change control in the above examples;

(c) Describe systems developed for recording and managing incidents (system failures, loss of service, etc.) which occur in the above examples;

(d) Describe facilities for maintaining error messages and audit trails in the above examples;

(e) Describe controls implemented in the above examples to minimize the effect of accidental or deliberate system misuse;

(f) Describe the strategy to be adopted for isolating such tasks as software development, system testing and production running;

(g) Describe controls which will be employed for managing external contractors and/or services.

3.6.2 System Planning and Acceptance

This section deals with the issues of system and capacity planning prior to the development of a system and acceptance testing undertaken prior to commissioning a system.

Responses are required to the following items:

(a) Describe your organisation's experience with system and capacity planning with a scope similar to that of the proposed Registry System;

(b) Describe your organisation's experience with acceptance testing in the following areas:

(i) Performance and computer capacity;

(ii) Error recovery, re-start and contingency planning;

(iii) Testing of routine operational procedures;

(iv) Testing of security controls;

(v) Testing of manual procedures;

(vi) Testing of business continuity plans;

(vii) Testing the effect of new systems on existing systems;

(viii) Testing user training.

(c) Describe your organisation's approach to determining acceptance criteria and ensuring that all acceptance criteria have been met.

3.6.3 Protection against Malicious Software

Computers systems are vulnerable to the introduction of malicious software, e.g. computer viruses, logic bombs. Facilities are required to prevent and detect such occurrences.

Responses are required to the following items:

(a) Describe software and procedures to be incorporated in the proposed Registry System to provide protection against malicious software;

(b) Describe controls to be used which prohibit the use of unauthorised software;

(c) Describe procedures for reviewing information and software on computers running the proposed Registry System;

(d) Describe facilities for checking electronic mail or Internet downloads for viruses.

3.6.4 Housekeeping

This section deals with the routine housekeeping activities required to maintain a well organised computer system.

Responses are required to the following items:

(a) Describe procedures for performing back-up and recovery operations of the proposed Registry System;

(b) Describe testing procedures to ensure the back-up and recovery procedures are performing correctly;

(c) Describe procedures for checking that all essential data is included in the back-up and recovery process;

(d) Describe the information recorded in the operation logs maintained in the proposed Registry System;

(e) Describe the information recorded in the fault logs maintained in the proposed Registry System;

(f) Describe procedures for reviewing the fault logs and recording the resolution of fault conditions.

3.6.5 Network Management

This section relates to security management of networks and information passing through public networks.

Responses are required to the following items:

(a) Describe your organisation's approach to network operations in the proposed Registry System;

(b) Describe procedures and controls to be incorporated in the proposed Registry System to maintain the availability of network services and connected computers;

(c) Describe facilities designed to ensure the security of data in networks and to protect connected services from unauthorised users.

3.6.6 Media Handling and Security

This section deals with the protection of documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorised access.

Responses are required to the following items:

(a) Describe procedures and controls in the proposed Registry System to ensure that data is totally erased from computer media no longer required;

(b) Describe procedures and controls in the proposed Registry System to ensure that the copying of system data to removable media is controlled and appropriate audit trails maintained;

(c) Provide details of operational procedures to ensure that information copied to secondary media is stored securely;

(d) Provide details of operational procedures to ensure printed information is handled and disposed of securely;

(e) Describe procedures and controls in the proposed Registry System to ensure that all communication facilities (e.g. e-mail, voice mail, post and fax) are subject to audit;

(f) Describe procedures and controls in the proposed Registry System to ensure that system documentation is secure and accessed only by authorised users.

3.6.7 Exchanges of Information and Software

This section deals with the exchange of information or software between organisations. Such exchange arrangements are subject to formal agreements which define what information is to be transferred and the level of security and controls required in the transfer

Responses are required to the following items:

(a) Describe the level of authentication and authorisation for information exchanges in the proposed Registry System;

(b) Provide details of the level of encryption of information exchanges in the proposed Registry System.

3.7 Access Control

This section relates to the control of access to information in the proposed Registry System.

3.7.1 Access Control Policy

The proposed Registry System requires relatively high levels of controls over the ability of individuals to access or change information in the system. In general, staff performing system and software development tasks will have different access rights from staff controlling the operation of the production system. It is envisaged that the development environment will be different from the production environment. These may take the form of different directories on one computer, or different computer systems. For example, web based software may be uploaded from the development environment to the production environment.

Responses are required to the following items:

(a) Describe the software development and support environment for the proposed Registry System;

(b) Describe the production environment for the proposed Registry System;

(c) Describe the procedures and controls for assigning access rights to staff (note that a hard rule based system is preferred in which access to a task is forbidden unless specifically assigned).

3.7.2 User Access Management

This section aims at preventing unauthorised access to the proposed Registry System. A formal user registration system is required which specifies a user's access rights to the system.

Responses are required to the following items:

(a) Describe the procedures and controls in the proposed Registry System for registering users in order to access system facilities;

(b) Describe the mechanism which controls user access to various classes of facilities in the Registry System;

(c) Provide samples of statements to be signed by users to indicate they understand their levels and conditions of access.

(d) Describe procedures and controls for the assignment of user access privileges to various system facilities, e.g. operating system, databases, application software modules;

(e) Describe procedures and controls for assigning and managing user passwords in the proposed Registry System;

(f) Describe other technologies which are recommended for incorporation in the proposed Registry System (e.g. finger prints, smart cards, etc).

3.7.3 User Responsibilities

This section defines the responsibilities of users accessing the proposed Registry System. The co-operation of authorised users is essential for effective security.

Responses are required to the following items:

(a) Describe procedures and controls in the proposed Registry System to allow users to change passwords (a minimum of six characters is recommended);

(b) Describe procedures and controls in the proposed Registry System for terminating user sessions after a workstation has been inactive for a set elapsed time (e.g. 2 minutes).

3.7.4 Network Access Control

This section relates to the protection of internal and external network services. The proposed Registry System is fundamental to the day-to-day operation of the Internet in Australia and its design must incorporate high levels of internal and external network security to ensure that the Internet operates correctly.

Responses are required to the following items:

(a) The proposed Registry System will be accessed by local users (staff of the successful Tenderer) and via the Internet (Registry Access Protocol, WHOIS and nameserver requests). Provide details of appropriate network controls for both areas;

(b) Provide details of enforced network path requirements in the proposed Registry System;

(c) Provide details of facilities for user authentication for external connections in the proposed Registry System;

(d) Provide details of facilities for node authentication in the proposed Registry System;

(e) Provide details of facilities for remote diagnostic port protection in the proposed Registry System;

(f) Provide details of facilities for segregation of networks in the proposed Registry System;

(g) Provide details of facilities for network connection control in the proposed Registry System, restricting access to electronic mail, file transfers and interactive access;

(h) Provide details of facilities for network routing control in the proposed Registry System;

(i) Provide details of facilities for restricting access to normal Internet browser services in the proposed Registry System.

3.7.5 Operating System Access Control

This section relates to security facilities at the operating system level used to restrict access to computer and operating system resources. Facilities are required to identify users when they log-in to the system, including an identification of remote computers or terminals being used. Users are authenticated by passwords or other mechanisms and appropriate audit logs are used to record both successful and failed log-ins.

Responses are required to the following items:

(a) Describe facilities to be incorporated in the proposed Registry System to identify user computers or terminals during log-in procedures;

(b) Describe the log-in procedure for users at computers or terminals attached to the proposed Registry System;

(c) Describe the methods adopted for user identification and authentication in the proposed Registry System;

(d) Describe the password management system to be incorporated in the proposed Registry System;

(e) Provide a list of system utility programs in the proposed Registry System capable of by-passing system and application access controls, and describe how the use of these utilities will be restricted and/or controlled;

(f) Describe facilities in the proposed Registry System for logging off users who have been in-active for a set period of time (e.g. 2-5 minutes);

(g) Describe facilities in the proposed Registry System for limiting connection time for user sessions, either the duration of the session or the time slot during which log-ins are accepted.

3.7.6 Application Access Control

This section relates to the prevention of unauthorised access to information in the proposed Registry System. Security facilities are used to restrict access to modules within the application software.

Responses are required to the following items:

(a) Provide details of the menu system to be incorporated in the proposed Registry System to permit tailoring of menus presented to users or classes of users according to their access requirements;

(b) Provide details of facilities in the proposed Registry System which restrict user access to system documentation according to their access requirements;

(c) Provide details of facilities in the proposed Registry System which controls the access rights of users, e.g. read, write, delete, execute;

(d) Provide details of facilities in the proposed Registry System which restrict access to facilities based on the identity or location of the computer or terminal being used.

3.7.7 Monitoring System Access and Use

The proposed Registry System should be monitored to detect unauthorised activities. Audit logs recording exceptions and other security sensitive events should be generated and retained for agreed periods to assist in future investigations and access-control monitoring.

Responses are required to the following items:

(a) Describe facilities in the proposed Registry System for event logging and provide details of the information contained in event logs;

(b) Provide details of facilities in the proposed Registry System for monitoring the use of system modules, e.g. authorising user log-ins, use of supervisor facilities, system start/stop, unauthorised access attempts;

(c) Describe facilities to be incorporated in the proposed Registry System for analysing or searching event log information, e.g. log-ins by user “X”;

(d) Describe facilities in the proposed Registry System for clock synchronization, e.g. to Universal Coordinated Time or local time.

3.7.8 Mobile Computing and Teleworking

This section relates to the use of mobile computing and teleworking facilities with the proposed Registry System. This section is particularly relevant to systems which are completely web based.

Organisations should provide details of any use to be made of mobile equipment or teleworking in the proposed Registry System, and special security controls for users of these devices.

Responses are required to the following items:

(a) Describe facilities for access controls, cryptographic methods, back-ups and virus protection for mobile computer users and teleworkers accessing the proposed Registry System;

(b) Provide details of the environment in which mobile computers and teleworking equipment will be operating when users are interacting with the proposed Registry System, for either or both development or production;

(c) Describe facilities to prevent unauthorised access the proposed Registry System by illegal users of mobile computers or teleworking equipment;

(d) Describe the type of work to be undertaken on the proposed Registry System by mobile computer users or teleworkers.

3.8 System Development and Maintenance

This section defines the security levels required in the development and maintenance of the proposed Registry System.

3.8.1 Security Requirements of Systems

The proposed Registry System is fundamental to the day-to-day operation of the Internet in Australia and its design must incorporate high levels of security to ensure that the system operates correctly.

3.8.2 Security in Application Systems

Individual program modules within the proposed Registry System must be designed to prevent loss, modification or misuse of information. Appropriate controls, audit trails and activity logs must be incorporated in the system, and facilities included to validate input data, internal processing and output data.

Responses are required to the following items:

(a) Describe the level of input data validation to be incorporated in the proposed Registry System;

(b) Describe the internal processing controls to be incorporated into the proposed Registry System;

(c) Describe the use to be made of message authentication techniques in the proposed Registry System;

(d) Describe the level of output data validation to be incorporated in the proposed Registry System.

3.8.3 Cryptographic Controls

Cryptographic controls protect the confidentially, authenticity and integrity of information. In the proposed Registry System, cryptographic controls are required when transferring Registry data to other sites but are not necessarily required for in-house database operations.

Responses are required to the following items:

(a) Describe the cryptographic controls to be used with the proposed Registry System;

(b) Describe procedures and controls for managing cryptographic controls and protecting cryptographic keys;

(c) Describe facilities to be provided in the proposed Registry System for registering and processing digital signatures.

3.8.4 Security of System Files

This section relates to the maintenance of a secure operational environment by controlling access to system software and information files.

Responses are required to the following items:

(a) Describe procedures and controls for updating operational program libraries upon receipt of appropriate management authorisation;

(b) Describe procedures and controls for ensuring that software is not implemented on an operational system without appropriate testing and user acceptance;

(c) Describe the contents of the audit log maintained for recording changes to the operating environment;

(d) Describe procedures and controls for retaining old versions of software modules for contingency purposes;

(e) Describe procedures and controls for generating or maintaining test data used for testing software changes;

(f) Describe procedures and controls for maintaining program source libraries.

3.8.5 Security in Development and Support Processes

This section relates to the maintenance of the security of application software and information in the proposed Registry System. Project and support environments should be strictly controlled.

Responses are required to the following items:

(a) Describe the change control procedures that will apply during design, implementation and support of the proposed Registry System;

(b) Describe the system of authorisation or approval of changes to the proposed Registry System;

(c) Describe the level of integration between the change control procedures and corresponding changes to system documentation;

(d) Describe the version control system for software releases in the proposed Registry System;

(e) Describe the information contained in the audit trail of changes that are introduced into the proposed Registry System;

(f) Describe the procedure for ensuring that changes to the proposed Registry System are introduced at the correct time without disturbing the normal operation of the Registry;

(g) Describe the environment for testing changes to the Registry System prior to their release to the production environment;

(h) Describe the procedures established to test the valid operation of developed application software in a changed operating system environment;

(i) Describe procedures and controls to identify covert channels, trojan code or logic bombs included in application software by careless or disgruntled employees;

(j) Describe procedures and controls for testing and accepting software modules developed by external organisations.

3.9 Business Continuity Management

This section deals with the security aspects of business continuity management which itself is discussed in detail in Section 4 of this document. Business continuity management involves the analysis of the consequences of disasters, security failures and loss of service, and the formulation of plans to allow business activities to be restored within an accepted time frame.

Responses are required to the following items:

(a) Provide details of your organisation's experience in developing and implementing business continuity plans;

(b) State how many existing sites are running with established business continuity plans.

3.10 Compliance

Tenderers should note that the design, operation, use and management of the proposed Registry System will be subject to statutory, regulatory and contractual security requirements which may vary from country to country, particularly for information created in one country that is transmitted to another country.

Responses are required to the following items:

(a) The successful Tenderer will be required to document all statutory and regulatory requirements of the proposed Registry System, together with specific controls and individual responsibilities to meet these requirements;

(b) The successful Tenderer will be licensed to provide Registry services to auDA. Intellectual property rights of the information contained in the Registry will be vested in auDA;

(c) The successful Tenderer must ensure that appropriate procedures are implemented to ensure that copyright is not infringed;

(d) The successful Tenderer will retain copyright in computer software developed specifically for the proposed Registry System;

(e) The successful Tenderer will be required to maintain a list of proprietary software used in the proposed Registry System and

perform any necessary checks and audits to ensure that only authorised software is used in the Registry;

(f) Tenderers should include a copy of their software copyright compliance policy as part of the tender documentation;

(g) Describe methods which will be employed to ensure that essential data contained in the Registry System is protected from loss, destruction and falsification;

(h) Describe methods which will be employed to ensure the protection and privacy of personal information in the Registry System;

(i) Describe audit controls which will be implemented to safeguard the integrity of the proposed Registry System and the information contained in system databases;

(j) Describe how audit tools will be protected to ensure that the audit process in performed without interference.

4. BUSINESS CONTINUITY PLAN

This section of the tender specification relates to the on-going operation of the proposed Registry System. Business continuity and disaster recovery are established methodologies which have evolved to provide a planned approach for the re-establishment of services following failures or disasters.

The successful Tenderer will be required to develop and implement a full business continuity plan for the proposed Registry System. The plan will detail the processes to be undertaken to ensure the continued operation of the Registry in the event of a disaster.

Business continuity planning is considered an addition to the normal operation of a well designed computer system. The latter includes regular system maintenance and routine back-up and recovery procedures for information files within the system, software maintenance and documentation. Off-site data escrow requirements are described in Section 5.

The following provides an overview of the level of continuity planning considered necessary for the proposed Registry System. The first stage of the process is the preparation of the business continuity plan. The second stage is the implementation of the systems and infrastructure required to ensure that the plan executes successfully.

The functions within the proposed Registry System are considered to be at two levels: production and maintenance. The production items include the real-time components of the proposed Registry System, e.g. the nameserver and WHOIS services. The maintenance items include the remainder of the system, e.g. maintenance of data records, reporting and enquiries.

Continuity planning should aim to re-establish operation of the primary or production level of the proposed Registry System by the end of the next business day – e.g. a disaster on Wednesday is recovered by midnight on Thursday, a disaster on Friday is recovered by midnight on Monday. The Registry System should be fully operational within three business days.

Continuity planning is usually a compromise between what can be achieved and the cost of achieving it. In this case, optimum continuity would be achieved with a solution based on fully duplicated sites at multiple locations (e.g. one in Melbourne, one in Sydney). The need for continuous operation of the proposed Registry System justifies the cost.

Business continuity planning is an established management approach to the recovery of business operations and procedures following a disaster. Disasters can be brought about by nature (e.g. floods,

cyclones, heat-waves, flu epidemics), can be accidental (e.g. fire, building collapse), can be man-made (e.g. bombs, sabotage, viruses, activation of sprinkler systems) or due to industrial disputes (e.g. power strikes). While the variations are numerous, disasters can be categorized as loss of information, loss of access or loss of personnel.

The aim of business continuity planning is to minimize interruptions to operations or services provided by the business, and to resume critical operations or services within a specified time after a disaster. Continuity planning also aims to minimize financial loss within an organisation and to assure clients and the community that their interests are protected. It ensures that management and staff within an organisation understand the implications of disasters on services and provides a positive public image of the organisation.

Business continuity planning requires a study of the operations of a business, identification of areas and facilities which are likely to be affected by disasters, and providing back-up equipment and procedures for re-establishing services in the event of a disaster. For the proposed Registry System, the continuity planning stages could be defined as follows.

(a) Business Impact Analysis

This stage involves an analysis of all aspects of the proposed Registry System, including housing, personnel, equipment, communications, procedures and business requirements. The resulting report should include the following:

(i) An audit of business sites, the personnel and equipment located at each site, and the impact of the loss of the sites, personnel and equipment.

(ii) A security assessment of computer and communications equipment within the organisation (as discussed in Section 3) including:

- Physical security, including access control;
- Tasks performed by personnel;
- Operating procedures;
- Back-up and recovery procedures;
- System development and maintenance;
- Database security;
- Personal computers.

(iii) An audit of possible disaster situations likely to impact on the proposed Registry System, in particular:

- Loss of power (e.g. failure or prolonged strike);

- Loss of environmental controls (e.g. air-conditioning);
- Breaches of security (e.g. physical, electronic – virus or hack attack);
- Loss of internal/external communications;
- System failure (e.g. computer or disk malfunction);
- Internet communication failure or interruption;
- Degraded performance;
- File corruption or lost files;
- Unreliable or incorrect results.

(iv) Determination of critical resource requirements for disaster recovery;

(v) Recovery strategies and methods to be applied in the event of disasters, and timelines for partial and full recovery;

(vi) Cost/benefit analysis for the various recovery alternatives;

(vii) Staffing requirements for the various recovery alternatives;

(viii) Recommended recovery strategy.

The business impact analysis is usually performed once, and subjected to a relatively minor annual review to assess changes introduced during the year.

(b) Business Continuity Plan

The business continuity plan is an extension of the business impact analysis and effectively documents the procedures to be followed to recover from a disaster situation. Copies of the documents should be kept off-site with appropriate back-up and software files in the event that the primary site is destroyed. The business continuity plan should be written to allow an external organisation or qualified individual to undertake the recovery process. The major components of the business continuity plan are as follows:

(i) Organisational details

This includes details of alternate office locations, contact details and staff trained in the execution of the recovery procedures;

(ii) Disaster declaration procedures for instigating disaster recovery operations

This should define the procedure for commencing the disaster recovery process, including a list of organisations and individuals to be notified;

(iii) Procedures for activating alternate work-sites

Arrangements must be made for alternate work sites in the event that the primary work site cannot continue to be used (e.g. destroyed by fire). This may take the form of an initial temporary arrangement at another site until a new site is found, or it may be part of a multi-site plan within the organisation;

(iv) Procedures for recovering vital records and files

Vital records and files must be stored off-site to as part of the disaster recovery procedure. This section should provide a list of such items and where they are located. Procedures should be established to ensure that the required files are stored off-site as part of the site's normal operational procedures, and for checking that they are correctly stored and updated. Procedures should be documented for the recovery of off-site information (software and data);

(v) Definition of recovery teams and responsibilities

Provide a list of individuals assigned to recovery teams and the tasks to be performed by the teams. This documentation should take the form of a "flowchart" for recovery in any situation. Arrangements could be made with external organisations or qualified individuals to be used as alternatives to in-house staff in the event of a disaster. External staff should be trained in recovery procedures as in (c) below.

(vi) Recovery procedures

This defines the steps involved in the recovery process. The steps should be clearly defined and reviewed during staff training in (c) below and testing in (d) below. This is the key area of the continuity plan.

(vii) Relocation procedures

This section relates to the relocation of the proposed Registry System either temporarily or permanently as the result of a disaster situation.

(viii) Resource requirements and procurement

This provides a list of vendors and suppliers who may be required to provide equipment and/or services to assist with the recovery process. The section should also document any arrangements or contracts with vendors to supply equipment at short notice, e.g. immediate supply of a replacement computer.

(c) Staff Training

Training is required for both in-house staff and external contractors in the execution of the business recovery plan. This section documents the level of training and provides procedures for documenting staff training levels. Training should include a review of the business continuity plan and participation in testing as described in (d) below.

(d) Testing of the Continuity Plan

This section documents procedures for testing the business continuity plan to ensure that recovery operations function correctly and that staff are adequately trained. Procedures should be included to evaluate the progress of general staff in following recovery procedures. Tests should be performed periodically and should be used to refine the recovery process.

(e) Effectiveness Evaluation and Monitoring

An annual review of the entire business continuity process should be conducted and reviewed by senior management.

Using the above as a guide, Tenderers should respond with an overview of a business continuity plan appropriate for their proposed Registry System, specifying very clearly the level of disaster recovery incorporated into the plan. Tenderers may also propose alternate business continuity plans.

5. DATA ESCROW REQUIREMENTS

This section of the specification defines the data escrow requirements of the proposed Registry System. Data escrow requires the transfer of data from the proposed Registry System to a site nominated at the time of contract by auDA, and to be accessed by auDA under strictly limited circumstances.

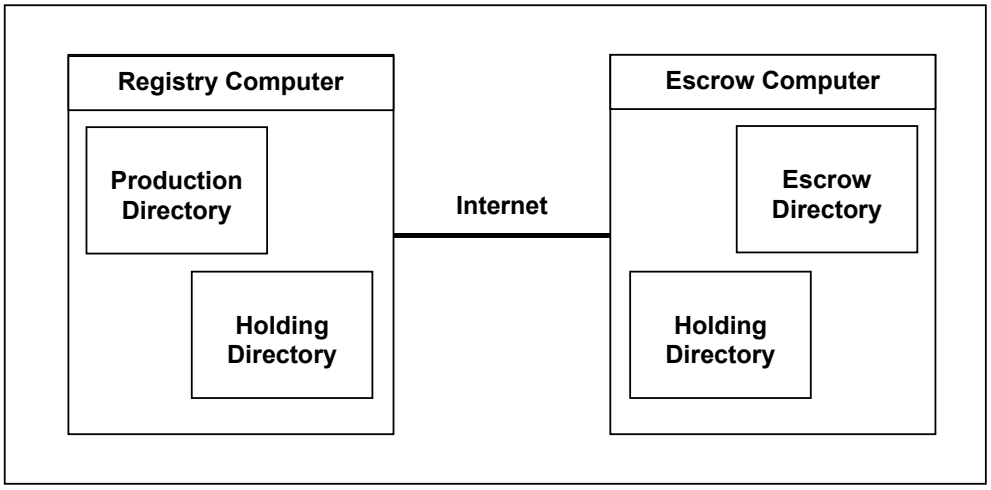
Data escrow operations will be undertake once within each 24 hour period.

5.1 Data Escrow Operation

In general terms data escrow needs to be performed on a regular basis and will require the transfer of all data, programs and documentation from the proposed Registry System to the nominated site. The data escrow process should be as fully automated as possible.

For example, a job could be scheduled to run at a convenient time (e.g. midnight) to extract the required data from the Registry's database and generate the required text files in a nominated directory, together with all required software and documentation files. The contents of the directory would then be transferred via the Internet to the escrow site and validated.

The following diagram provides a diagrammatic view of such a data escrow operation.



In the above diagram, the holding directories are accessible only to the escrow programs. The data escrow job executes the following tasks:

(a) Lock out database entry, update and delete operations for the duration of the job;

(b) Scan the nominated database tables in the Production Directory and generate text files of escrow data in the Holding Directory;

(c) Copy nominated software and documentation files from the Production Directory to the Holding Directory;

(d) All of the files in the holding directory are encrypted and signed, using best current practices, prior to transmission;

(e) Transfer the files in the Holding Directory of the Registry Computer via the Internet to the Holding Directory of the Escrow Computer;

(f) After a file has been transmitted it is verified to ensure that the transfer operation executed correctly. Verification is effected by reading the transferred file from the Escrow Computer and comparing it with the original file. The comparison may be made with the encrypted files, or the files may be decrypted and then compared. Files that fail verification are re-transmitted;

(g) A report of the data escrow operation is printed;

(h) Copy the encrypted files from the Holding Directory in the Escrow Computer to the Escrow Directory in the Escrow Computer, replacing the previous day's files;

(i) Files in the Production Computer's Holding Directory are then deleted;

(j) Files in the Escrow Computer's Holding Directory are then deleted;

(k) Re-instate normal database operations.

While this model is somewhat simplistic, it demonstrated the facilities required in the data escrow process.

Many variations are possible. One option could be to separate the escrow process for program and documentation files so that it is activated on demand (when software or documentation is updated) rather than being part of the routine escrow process.

Another alternative could be to replace the use of the Internet as the transfer medium with magnetic media (e.g. DAT tapes).

5.2 Data Escrow Contents

The purpose of the escrow process is to allow auDA to replicate the original Registry environment if necessary. This means that that the Registry Operator will be required to include everything necessary to reinstate a fully functioning Registry System. Normally this will include the following:

(a) Complete source code of Registry, nameserver and WHOIS software;

(b) Database definitions and contents of the database;

(c) Operational and configuration files and information;

(d) Documentation covering the installation, configuration and operation of the system;

(e) Help files, operation and user manuals.

In addition the escrow process should include the computer operating system, compilers and utilities if these are specifically required for Registry operation. As an alternative, the Registry Operator must provide full documentation of the computer hardware, system and database software and utilities to be used in the proposed Registry System.

The Registry Operator is to be responsible for the maintenance of paper records (e.g. manuals, printed reports) in accordance with the requirements of the Australian Record Management Standard AS4390.

In addition, the Registry Operator is required to provide auDA with a licence to run the Registry software in the event that auDA is obliged to establish a new Registry.

At Registry rollover, there must be a seamless transition between an incumbent Registry Operator and the designate Registry Operator. The Registry Operator is required to co-operate in the handover process to ensure continuous service to Registrars.

5.3 Data Escrow Format

As part of the data escrow process, information from each Registry table is to be extracted into one or more text files. Text fields in the Registry Database are coded in UTF-8 (Unicode UCS Transformation Format, 8-bit) and escrow data will also be coded in UTF-8. The following format will be adopted to represent fields of information:

<tag>: <data in UTF-8>[<cont>]<nl>

where

<tag> is the name of the field, followed by a colon and a space;
<cont> is an optional continuation character (octal 134);
<nl> is the new line character (octal 012).

The end of a record is indicated by two <nl> characters. The end of a file is indicated by the conventional EOF condition. Sample output is as follows:

Records containing Surname and Given Name fields:

```
Surname: Smith<nl>
Given Name: John<nl>
<nl>
Surname: Jones<nl>
Given Name: Henry<nl>
Address: PO Box 2434 <cont><nl>
VIC 3067<nl>
<nl>
```

Null or empty fields are omitted from the above. Non-text fields (e.g. date and numeric fields) are translated to text as part of the conversion process. Dates are to be converted to ISO 8601:1988 (E) format (YYYY-MM-DD).

Data escrow files are required for each of the tables contained in the Registry Database, namely:

(a) Registrar Record;

(b) Registrant Record;

(c) Domain Record;

(d) Contact Record.

The information content of the data escrow records will be as defined for the Registry Database Records in Section 2.1 Tag names will be those specified in Appendix A.

In the event that the Registry Database is expanded to include additional tables or fields, then the additional tables and fields must be included in the data escrow process.

5.4 Data Escrow Proposal

Using the above as a guide, Tenderers should respond with an overview of a data escrow plan appropriate for their proposed Registry. Tenderers may also propose alternate data escrow plans.

Tenderers will be required to develop or supply the software required for the data escrow process. Tenderers must also develop or supply any special software that is required in the Escrow Computer during data escrow operations. The data escrow facilities should allow transfer of files to and from the data escrow computer.

6. DOMAIN NAME EXPIRY AND DELETION

This section of the tender specification relates to the expiry and deletion of domain names in the proposed Registry.

When domain names are registered the expiry date of the domain name is entered into the Registry Database, usually as the date registered plus two years. Domain names may be deleted at the request of the Registrant or expire at the end of the registration period unless the Registrant pays the required renewal fee. Registrants are given a standard grace period in which to reverse the expiry or deletion.

It is a requirement of the Tender that deleted items become available for re-use as soon as possible after the period of grace. The proposed Registry must be provided with facilities to search for and delete these domain names.

It is also a requirement of the Tender that the proposed Registry contains no facilities (accidental or otherwise) which allows the Registry Operator or a Registrar to retain a deleted, expired or unregistered domain name. There should be no facilities for reserving domain names in the proposed Registry apart from under the strictly controlled conditions of the IRRP.

A dispute resolution process has been established by auDA to determine ownership of domain names which are shown to be held in bad faith. Registry Operators and Registrars are prohibited from using domain availability information to speculate in any manner on domain names.

Undesirable practices include, but are not limited to:

(a) A Registrar or Registry Operator squatting on domain names pending an increased fee, auction or other market-distorting activity;

(b) A Registrar or Registry Operator who removes a domain name from the market in response to a WHOIS query from a prospective Registrant, and attempts to obtain additional fees from the Registrant;

(c) A Registrar or Registry Operator who uses business registration information to squat on related domain names to obtain additional fees from the relevant prospective Registrant.

Tenderers are requested to acknowledge the above and describe the facilities to be incorporated in the proposed Registry to control these undesirable practices.

7. REPORTING REQUIREMENTS

This section describes the information to be provided to auDA in the form of a monthly report of the operation of the proposed Registry. The monthly report must be presented to auDA in the first week of the following month. The monthly report is to consist of the following information:

(a) Registrants

Report the total number of Registrants by Registrar in the Registry System at the end of the month, together with the numbers of Registrants in the current month.

(b) Domain Names

Report the total number of domain names registered by the Registry Operator at the end of the month, together with the numbers of domain names registered in the current month.

Provide a breakdown of the above domain name registrations by Registrar.

Report the number of domain name reservations where a reservation expires and the subsequent reservation of the same domain name is made by the same Registrar. This information should be reported on a per-Registrar basis.

(c) WHOIS Service Activity

Report the total number of WHOIS queries for the Registry in the current month and a breakdown of queries by 2LD.

Report any unusual or suspicious WHOIS activity, including the blacklisting of any hosts.

(d) Nameserver Activity

Report the total number of nameserver queries for the Registry at the end of the current month. Provide a breakdown of the number of nameserver queries for each 2LD.

(e) Service Level Performance

Report service levels for the Registry under the headings of Register, nameserver and WHOIS for the following items (where applicable):

- Service Availability
- Planned Outage

- Extended Planned Outage
- Average Add Time
- Average Modify Time
- Average Delete Time
- Average Time to Query Domain
- Average Time for WHOIS Query
- Average Time for Nameserver Resolution
- Update Frequency

The above should be displayed/printed with contracted service levels followed by the actual levels. The unit of measurement (e.g. %) should follow the value. Instances where performance requirements have not been met should be highlighted.

(f) Database Transactions

Provide a table of daily database transactions for each day of the current month together with the average daily transaction rate for the month.

(g) Database Size

Provide a report of the current size of the Registry Database relative to the capacity of the hardware, and the increase in size during the current month.

(h) Hardware, Software, Network and Security Issues

Provide a report of any hardware, software, network or security issues encountered during the month and the steps taken to resolve the issues and ensure that the issues do not reoccur.

In circumstances where a security breach occurs, auDA is to be provided with a report detailing the nature, extent of the breach and action taken, at the earliest available opportunity.

(i) Enquiries

Provide a report of the number and type of telephone and email support enquiries made to the Registry.

The monthly report should be available for viewing or printing. Specific details on the format and transmission of the report will be provided by auDA at a later time.

The Registry Operator will also be required to provide Registrars with reports relating to their customer base and other operational information that Registrars require to conduct their businesses.

8. REGISTRAR SUPPORT SERVICES

This section of the tender specification describes the Registrar support services to be provided as part of the proposed Registry operation.

The following services are regarded as a minimum:

(a) 7 day, 24 hour support in the form of a Registry help desk;

(b) E-mail address and telephone number for service requests and enquiries;

(c) Assistance with billing and account management;

(d) Provision of a test and evaluation environment to enable the testing of new software;

(e) Provision of a high quality domain name service to end users.

Tenderers are requested to comment on the above and describe any additional Registrar support services to be incorporated in the proposed service.

APPENDIX A: DATABASE RECORD FORMAT

A.1 Registrar Record

Field Name	Type	Mand/Opt	Comment
rar-code	vc(20)	mand	Unique identifier for Registrar
rar-name	vc(200)	mand	Name of the Registrar
rar-type	vc(10)	mand	Coded Category of Registrar (e.g. company, individual, educational institution)
rar-alt-name	vc(200)	opt	Alternative name of Registrar (e.g. "trading as ...")
rar-bus-code-type	vc(10)	mand	The type of Business registration code, if the Registrar is a company. E.g. ACN, ABN, etc.
rar-bus-code	vc(50)	mand	The Business registration code, if the Registrar is a company.
rar-address-street	vc(50)	mand	The street address of the Registrar
rar-address-other	vc(50)	opt	Additional address information, e.g. building, floor, etc.
rar-address-city	vc(50)	mand	City or suburb
rar-address-state	vc(50)	mand	State or territory
rar-address-scode	vc(10)	mand	Code for state or territory
rar-address-postcode	vc(20)	mand	Postal code
rar-address-ccode	vc(2)	mand	2-digit country code, from ISO-3166-1
rar-address-country	vc(50)	opt	Country name in English
rar-pgp-pub	vc(2000)	mand	The Registrar's public PGP key with which all database query/update messages will be verified.
rar-create-date	date	mand	Date of creation of the Registrar record
rar-update-date	date	mand	Date of the most recent update of the Registrar record

A.2 Registrant Record

Field Name	Type	Mand/Opt	Comment
reg-code	vc(20)	mand	Unique Registrant identifier for registration
reg-registrar	vc(20)	mand	Identification code of the associated Registrar
reg-name	vc(200)	mand	Name of the Registrant
reg-type	vc(10)	mand	Coded Category of Registrant (e.g. company, individual, educational institution)
reg-alt-name	vc(200)	opt	Alternative name of Registrant (e.g. "trading as ...")
reg-bus-code-type	vc(10)	mand	The type of Business registration code, if the Registrant is a company. E.g. ACN, ABN, etc.
reg-bus-code	vc(50)	mand	The Business registration code, if the Registrant is a company.
reg-address-street	vc(50)	mand	The street address of the Registrant
reg-address-other	vc(50)	opt	Additional address information, e.g. building, floor, etc.
reg-address-city	vc(50)	mand	City or suburb
reg-address-state	vc(50)	mand	State or territory
reg-address-scode	vc(10)	mand	Code for state or territory
reg-address-postcode	vc(20)	mand	Postal code
reg-address-ccode	vc(2)	mand	2-digit country code, from ISO-3166-1
reg-address-country	vc(50)	opt	Country name in English
reg-create-date	date	mand	Date of creation of the registration
reg-update-date	date	mand	Date of the most recent update of the registration details

A.3 Domain Record

Field Name	Type	Mand/Opt	Comment
domain-reg-code	vc(20)	mand	Registrant identification code
domain-code	vc(20)	mand	Unique identifier for the domain record
domain-name	vc(255)	mand	The fully qualified domain name
domain-refinf	vc(2000)	opt	Reference information about the domain. Free form text for Registrar use
domain-create-date	date	mand	Date of creation of the domain
domain-length	number	mand	Length of registration (in years)
domain-nmsv1-host	vc(255)	mand	Hostname of the primary nameserver
domain-nmsv1-ip	vc(16)	mand	IP address of the primary nameserver
domain-nmsv2a-host	vc(255)	mand	Hostname of secondary nameserver-1
domain-nmsv2a-ip	vc(16)	mand	IP address of secondary nameserver-1
domain-nmsv2b-host	vc(255)	mand	Hostname of secondary nameserver-2
domain-nmsv2b-ip	vc(16)	mand	IP address of secondary nameserver-2
domain-nmsv2c-host	vc(255)	opt	Hostname of secondary nameserver-3
domain-nmsv2c-ip	vc(16)	opt	IP address of secondary nameserver-3
domain-nmsv2d-host	vc(255)	opt	Hostname of secondary nameserver-4
domain-nmsv2d-ip	vc(16)	opt	IP address of secondary nameserver-4
domain-nmsv2e-host	vc(255)	opt	Hostname of secondary nameserver-5
domain-nmsv2e-ip	vc(16)	opt	IP address of secondary nameserver-5
domain-nmsv2f-host	vc(255)	opt	Hostname of secondary nameserver-6
domain-nmsv2f-ip	vc(16)	opt	IP address of secondary nameserver-6
domain-nmsv2g-host	vc(255)	opt	Hostname of secondary nameserver-7
domain-nmsv2g-ip	vc(16)	opt	IP address of secondary nameserver-7
domain-rec-create-date	date	mand	Date of creation of the domain record
domain-rec-update-date	date	mand	Date of the most recent update of the domain record

A.4 Contact Record

Field Name	Type	Mand/Opt	Comment
contact-reg-code	vc(20)	mand	Registrant identification code
contact-code	vc(20)	mand	Unique identifier for the contact
contact-domain-code	vc(20)	mand	Unique identifier for the domain record for this contact
contact-type	vc(5)	mand	Contact Type, e.g. T for technical, A for administrative
contact-name-given	vc(50)	mand	Given name of Contact
contact-name-other	vc(50)	opt	Middle name or initial of Contact
contact-name-surname	vc(50)	mand	Surname of Contact
contact-org	vc(50)	mand	Organization name for contact
contact-address-street	vc(50)	mand	The street address of the Registrant
contact-address-other	vc(50)	opt	Additional address information, e.g. building, floor, etc.
contact-address-city	vc(50)	mand	City or suburb
contact-address-state	vc(50)	mand	State or territory
contact-address-scode	vc(10)	mand	Code for state or territory
contact-address-postcode	vc(20)	mand	Postal code
contact-address-ccode	vc(2)	mand	2-digit country code, from ISO-3166-1
contact-address-country	vc(50)	opt	Country name in English
contact-email	vc(50)	mand	Email address for contact
contact-phone	vc(20)	mand	Contact telephone number (international format)
contact-fax	vc(20)	mand	Contact facsimile number
contact-create-date	date	mand	Date of creation of the contact record
contact-update-date	date	mand	Date of the most recent update of the contact details

APPENDIX B: IRRP ACTION REQUESTS

B.1 domain-enquire

Purpose: To enquire whether a domain name is available for issue and to reserve the name for subsequent registration.

Format: **irrp-action: domain-enquire** <domain-name>

Response: An **irrp-response** message indicating the status of that domain name.

Discussion: When an enquiry is made concerning an unallocated domain name, that name must be reserved by the Registry Operator for a maximum of 30 minutes (or other time to be advised by auDA) pending the receipt of a request to create a domain record for the name. If a record is not created in that time, the reservation is to be removed. Multiple **domain-enquire** actions may be included in the one message.

Example request:

irrp-sequence: 00001
irrp-action: domain-enquire foobar.com.au
irrp-end

Example responses:

irrp-sequence: 00001
irrp-response: R011 foobar.com.au available
irrp-end

or

irrp-sequence: 00001
irrp-response: R012 foobar.com.au unavailable
irrp-end

or

irrp-sequence: 00001
irrp-response: R013 foobar.com.au pending
irrp-end

B.2 add-reg

Format: **irrp-action: add-reg**

Followed by lines containing the mandatory and optional fields of the Registrant Record. All mandatory fields **must** be present or the message will be rejected. One or more **add-domain** actions and one or more **add-contact** actions for the Registrant may follow. In each case the

Registrant code and the domain code must be left blank as they will be supplied automatically.

Response: An **irrp-response** message indicating the success or failure of the creation of the Registrant Record.

Discussion: The lines making up the Registrant Record information may be in any order. Domain Records may only be created for domain names previously reserved via a **domain-enquire** action.

Example request:

irrp-sequence: 00002
irrp-action: add-reg
reg-registrar: XXXXXX
reg-name: Foo Bar Pty. Ltd
.....
irrp-action: add-domain
domain-reg-code
domain-code:
domain-name: foobar.com.au
domain-refinf: The Foo Bar company is Australia's oldest company in the obfuscation industry.
.....
irrp-action: add-contact
contact-reg-code
contact-code:
contact-type: T
contact-name-given: Fred
.....
irrp-end

Example responses:

irrp-sequence: 00002
irrp-response: R021 add-reg successful reg-code: XXXXXXX
irrp-end

or

irrp-sequence: 00002
irrp-response: E021 add-reg unsuccessful
irrp-inf: Mandatory field reg-name missing
irrp-end

B.3 add-contact

Format: **irrp-action: add-contact**

Followed by lines containing the mandatory and optional fields of the contact record. All mandatory fields **must** be present, or the action will be rejected.

Response: An **irrp-response** message indicating the success or failure of the creation of the contact record.

Discussion: The lines making up the contact record information may be in any order.

Example request:

```
irrp-sequence: 00003
irrp-action: add-contact
contact-reg-code: XXXXXXX
contact-type: A
.....
irrp-end
```

Example responses:

```
irrp-sequence: 00003
irrp-response: R031 add-contact successful contact-code: XXXXXXX
irrp-end
```

or

```
irrp-sequence: 00003
irrp-response: E031 add-contact unsuccessful
irrp-inf: Mandatory field contact-name-surname missing
irrp-end
```

B.4 add-domain

Format: **irrp-action: add-domain**

Followed by lines containing the mandatory and optional fields of the domain record. All mandatory fields **must** be present, or the action will be rejected.

Response: An **irrp-response** message indicating the success or failure of the creation of the domain record.

Discussion: The lines making up the domain record information may be in any order. Domain Records may only be created for domain names previously reserved via a **domain-enquire** action.

Example request:

```
irrp-sequence: 00004
irrp-action: add-domain
domain-reg-code: XXXXXXX
domain-name: foobarbletch.com.au
.....
irrp-end
```

Example responses:

irrp-sequence: 00004
irrp-response: R014 add-domain successful domain-code: XXXXXXX
irrp-end

or

irrp-sequence: 00004
irrp-response: E014 add-domain unsuccessful
irrp-inf: Mandatory field domain-name missing
irrp-end

B.5 update-reg

Format: **irrp-action: update-reg**

Followed by a **reg-code** line which contains the identifier of the Registrant Record being updated, followed by one or more lines which add or amend fields in the Registrant Record.

Response: An **irrp-response** message indicating the success or failure of the update of the Registrant Record.

Discussion: Apart from the **reg-code** line, which must be the first line following the **irrp-action** line, other lines may be in any order. Lines where no content follows the field identifier indicate that the field is to be deleted (optional fields only).

Example request:

irrp-sequence: 00005
irrp-action: update-reg
reg-code: YYYYYYY
reg-alt-name: Our New Trading Name
.....
irrp-end

Example responses:

irrp-sequence: 00005
irrp-response: R022 update-reg successful
irrp-end

or

irrp-sequence: 00005
irrp-response: E022 update-reg unsuccessful
irrp-inf: Mandatory field reg-name blank
irrp-end

B.6 update-contact

Format: **irrp-action: update-contact**

Followed by a **contact-reg-code** line and a **contact-code** line which contain the identifiers of the Registrant and contact records, followed by one or more lines which add or amend fields in the contact record.

Response: An **irrp-response** message indicating the success or failure of the update of the contact record.

Discussion: Apart from the **contact-reg-code** and **contact-code** lines, which must be the first lines following the irrp-action line, other lines may be in any order. Lines where no content follows the field identifier indicate that the field is to be deleted (optional fields only).

Example request:

irrp-sequence: 00006
irrp-action: update-contact
contact-reg-code: XXXXXXX
contact-code: YYYYYYY
contact-email: newemail@foobar.com.au
.....
irrp-end

Example responses:

irrp-sequence: 00006
irrp-response: R032 update-contact successful
irrp-end

or

irrp-sequence: 00006
irrp-response: E032 update-contact unsuccessful
irrp-inf: Mandatory field contact-name-surname blank
irrp-end

B.7 update-domain

Format: **irrp-action: update-domain**

Followed by a **domain-reg-code** line and a **domain-code** line which contain the identifiers of the Registrant and domain records, followed by one or more lines which add or amend fields in the domain record.

Response: An **irrp-response** message indicating the success or failure of the update of the domain record.

Discussion: Apart from the **domain-reg-code** and **domain-code** lines, which must be the first lines following the **irrp-action** line, other lines may be in any order. Lines where no content follows the field identifier indicate that the field is to be deleted (optional fields only). The **domain-name** field may **not** be modified in this action. The only mechanism for changing domain names is to delete the domain record and create a replacement.

Example request:

irrp-sequence: 00007
irrp-action: update-domain
domain-reg-code: XXXXXXX
domain-code: YYYYYYY
domain-nmsv1-host: newnameserver.foobar.com.au
....
irrp-end

Example responses:

irrp-sequence: 00007
irrp-response: R015 update-domain successful
irrp-end

or

irrp-sequence: 00007
irrp-response: E015 update-domain unsuccessful
irrp-inf: Invalid domain-code
irrp-end

B.8 delete-reg

Format: **irrp-action: delete-reg**

Followed by a **reg-code** line containing the identifier of the Registrant to be deleted. This action causes the Registrant Record and associated domain and contact records to be deleted from the database.

Response: An **irrp-response** message indicating the success or failure of the Registrant deletion.

Discussion: All deletion actions are final, and any re-instatement of deleted Registrants, etc. will necessitate the creation of new records. Deletion of a domain record releases the domain name for immediate re-issue.

Example request:

irrp-sequence: 00008
irrp-action: delete-reg

reg-code: XXXXXXXX
irrp-end

Example responses:

irrp-sequence: 00008
irrp-response: R023 delete-reg successful
irrp-end

or

irrp-sequence: 00008
irrp-response: E023 delete-reg unsuccessful
irrp-inf: registrant XXXXXXXX not valid for this registrar
irrp-end

B.9 delete-contact

Format: **irrp-action: delete-contact**

Followed by a **contact-code** line containing the identifier of the contact to be deleted. This action causes the domain record to be deleted from the database.

Response: An **irrp-response** message indicating the success or failure of the contact deletion.

Example request:

irrp-sequence: 00009
irrp-action: delete-contact
contact-code: XXXXXXXX
irrp-end

Example responses:

irrp-sequence: 00009
irrp-response: R033 delete-contact successful
irrp-end

or

irrp-sequence: 00009
irrp-response: E033 delete-contact unsuccessful
irrp-inf: contact XXXXXXXX non-existent
irrp-end

B.10 delete-domain

Format: **irrp-action: delete-domain**

Followed by a **domain-code** line containing the identifier of the domain to be deleted. This action causes the

domain record and any associated contact records to be deleted from the database.

Response: An **irrp-response** message indicating the success or failure of the domain deletion.

Discussion: Deletion of a domain record releases the domain name for immediate re-issue.

Example request:

irrp-sequence: 00010
irrp-action: delete-domain
domain-code: XXXXXXXX
irrp-end

Example responses:

irrp-sequence: 00010
irrp-response: R016 delete-domain successful
irrp-end

or

irrp-sequence: 00010
irrp-response: E016 delete-domain unsuccessful
irrp-inf: domain XXXXXXXX not valid for this registrar
irrp-end

B.11 enquire-reg

Purpose: To retrieve a copy of all the information in a Registrant Record and associated contact and domain records.

Format: **irrp-action: enquire-reg** <registrant-identifier>

Response: An **irrp-response** line indicating success or failure of the request, followed by either a sequence of lines containing the Registrant details or an **irrp-inf** line indicating the reason for the action failing.

Example request:

irrp-sequence: 00011
irrp-action: enquire-reg XXXXXXX (where XXXXXXX is the reg-code value of a registration)
irrp-end

Example responses:

irrp-sequence: 00011
irrp-response: R024 enquire-reg successful
reg-code: XXXXXXX
.....
irrp-end

or

irrp-sequence: 00011
irrp-response: E024 enquire-reg unsuccessful
irrp-inf: reg-code XXXXXXX invalid
irrp-end

B.12 recall-mesg

Purpose: To request a repetition of a previous response message.

Format: **irrp-action: recall-mesg** [<sequence-number>]

If no sequence number is specified, the previous response from the Registry Operator will be repeated.

Response: An **irrp-response** line indicating whether the requested response is available, followed by the requested message, if available.

Discussion: The **recall-mesg** may be used by Registrars to recover from situations where a previous request did not result in a response, either through loss of the command or response messages, or a processing failure.

Example request:

irrp-sequence: 00012
irrp-action: recall-mesg XXXXXXX
irrp-end

Example responses:

irrp-sequence: 00012
irrp-response: R041 recall-mesg XXXXXXX available
.....
irrp-end

or

irrp-sequence: 00012
irrp-response: E041 recall-mesg unsuccessful XXXXXXX unavailable
irrp-end

B.13 transf-reg

Purpose: To request the transfer of a Registrant to another Registrar.

Format: **irrp-action: transf-reg** <destination-registrar-code>

Followed by the **reg-code** line of the Registrant Record to be transferred.

Response: An **irrp-response** line indicating whether the requested transfer was successful.

Discussion: The transfer of Registrants will be actioned by the originating Registrar and must have the prior consent of the destination Registrar as per auDA policy.

Example request:

irrp-sequence: 00013
irrp-action: transf-reg XXXXXXX
reg-code: YYYYYYYYY
irrp-end

Example responses:

irrp-sequence: 00013
irrp-response: R042 transfer successful
irrp-end

or

irrp-sequence: 00013
irrp-response: E042 transfer unsuccessful
irrp-inf: invalid destination registrar code
irrp-end

B.14 transf-domain

Purpose: To request the transfer of a domain name to another Registrant.

Format: **irrp-action: transf-domain** <destination-reg-identifier>

Followed by the **domain-code** line of the domain record to be transferred.

Response: An **irrp-response** line indicating whether the requested transfer was successful.

Discussion: The transfer of domain names will be actioned by the originating Registrar. Where the new Registrant is being handled by another Registrar, the transfer must have the

prior consent of the destination Registrar as per auDA policy.

Example request:

irrp-sequence: 00014
irrp-action: transf-domain XXXXXXX
domain-code: YYYYYYYYY
irrp-end

Example responses:

irrp-sequence: 00014
irrp-response: R042 transfer successful
irrp-end

or

irrp-sequence: 00014
irrp-response: E042 transfer unsuccessful
irrp-inf: invalid destination registrant identifier
irrp-end

APPENDIX C: IRRP RESPONSE AND ERROR CODES

C.1 Response Codes

R011 <domain-name> available
R012 <domain-name> unavailable
R013 <domain-name> pending
R014 add-domain successful domain-code: <value>
R015 update-domain successful
R016 delete-domain successful
R021 add-reg successful reg-code: <value>
R022 update-reg successful
R023 delete-reg successful
R024 enquire-reg successful
R031 add-contact successful contact-code: <value>
R032 update-contact successful
R033 delete-contact successful
R041 recall-mesg <sequence-number> available
R042 transfer successful

C.2 Error Codes

E001 authentication failure
E002 message could not be decrypted
E011 badly formed domain name
E014 add-domain unsuccessful
E015 update-domain unsuccessful
E016 delete-domain unsuccessful
E021 add-reg unsuccessful
E022 update-reg unsuccessful
E023 delete-reg unsuccessful
E024 enquire-reg unsuccessful
E031 add-contact unsuccessful
E032 update-contact unsuccessful
E033 delete-contact unsuccessful
E041 recall-mesg unsuccessful <sequence-number> unavailable
E042 transfer unsuccessful

APPENDIX D: DEFINITION OF TERMS

Service Availability. Service availability is defined as the time, in minutes, that the Registry is responding to its users. Service is unavailable when a service listed is unavailable to all users, that is, when no user can initiate a session with or receive a response from the Registry ("Unavailability").

Service Availability is measured as follows:

Service Availability % = {[(TM - POM) - UOM] / (TM - POM)}*100 where:

TM = Total Minutes in the Service Level Measurement Period (#days*24 hours*60 minutes)

POM = Planned Outage Minutes (sum of (i) Planned Outages and (ii) Extended Planned Outages during the Service Level Measurement Period)

UOM = Unplanned Outage Minutes (Difference between the total number of minutes of Unavailability during the Service Level Measurement Period minus POM).

Planned Outage. Downtime to allow for regular maintenance.

Planned Outage Duration. The Planned Outage Duration defines the maximum allowable time, in hours and minutes, that the Registry Operator is allowed to take the Registry out of service for regular maintenance.

Extended Planned Outage. In some cases such as software upgrades and platform replacements an extended maintenance timeframe is required.

Extended Planned Outage Duration. The Extended Planned Outage Duration defines the maximum allowable time, in hours and minutes, that the Registry Operator is allowed to take the Registry out of service for extended maintenance.

Processing Time. Processing Time refers to the time that the Registry Operator receives a request and sends a response to that request. For example a processing time of 3 seconds for 95% means that 95% of the transactions will take 3 seconds or less from the time the Registry Operator receives the request to the time it provides a response.

Update Delay Time. This is delay measured from the time that the Registry confirms an update to the Registrar to the time the update appears in the nameserver and WHOIS server. For example an update delay time of 15 minutes for 95% means that 95% of the updates will be available in the nameserver and WHOIS server within 15 minutes.

Cross-Network Nameserver Performance. Cross-Network Nameserver Performance is the measured round-trip time and packet loss from arbitrary locations on the Internet to the Registry.