Final Report ccNSO
Contact Repository Implementation Working Group

Executive Summary

There is still a strong desire to create and subscribe to an incident response/ contact repository to enhance the security and stability of the DNS, in particular for ccTLDs, and to which a vast majority of the ccTLD community could subscribe. Based on this core finding, the WG recommends the following:

- Start very simple with a secure mailing list.
- Iteratively expand based on user experience, funding model per iteration.
- Consider the alternative of having the Repository hosted by an established specialized organization like the Secure Domain Foundation.
- Consider initiatives such as DNS-OARC to avoid duplicate efforts.
- Extend the scope of the Repository to all critical infrastructure with direct relation to DNS stability.

The ccNSO Council is advised to set-up a small working group , which members are trusted by the community, to develop and implement a secure mailing list.

Introduction and Scope of Activities

The Contact Repository Implementation (CRI) Working Group was launched in April 2011[1][2], following the recommendations of the Incident Response Working Group[3]. The purpose of the CRI WG was to explore in detail costs, and other relevant factors to implement, maintain and operate an incident repository as proposed by the Incident Response Working Group. In exploring models and modalities for the implementation of a Contact Repository, the CRIWG is guided by and has to take into account:

- The non-binding relationship between ccTLDs and other entities
- Diversity: language, time zones, resources, expertise
- Policies and practices guiding ccTLDs
- Technical requirements, such as 24/7 availability

The activities of the CRI WG are limited to and shall into consideration the outcome and results of the work of the Incident Response Planning Working Group as proposed in their Final Report [4]. In particular the CRI WG has to take into account and was limited by:

- The definition of incident for the purpose of incident response

---

[1] The names of the WG members are included in Annex A of this report

[2] http://ccnso.icann.org/workinggroups/charter-iriwg-18apr11-en.pdf

[3] The Incident Response Working group was launched and established in response to the Conficker Incident. *It purpose was: to develop sustainable mechanisms for the engagement of and interaction with ccTLD registries during incidents that may impact the DNS.*

[4] http://cartagena39.icann.org/meetings/cartagena2010/presentation-ccnso-members-irwg-07dec10-en.pdf

- The description of use cases of contact repository i.e. for what purposes can the repository be used:
    - Information exchange
    - Counter action
- The definition of contact repository data attributes
- The general criteria for implementation and maintenance of repository:
    - Support the envisioned use cases
    - High availability (24/7)
    - Alternative communication channels (not using the internet)
    - Actively maintain and keep data up-to-date

Activities to date

Since the WG became active (June 2011), the CRI WG focused on further detailing the requirement and set-up of a contact repository as required by and in accordance with its mandate. The work of the WG members have resulted in:

- A model describing the interactions between the actors for a centralized set-up of the repository,
- A document with a detailed set of requirements for a centralized repository based on the model
- A document on possible governance and funding models for a centralized repository.

The model and the documentation that has been developed are works in progress and are included in Annex B of this Report .

The WG, though its chairperson also presented progress reports to the community on a regular basis. As indicated in its latest Progress Report, the value of the contact repository system, and therefore its successful implementation, depends largely on the value of the system for individual ccTLD operators. In turn the value of the system depends, among others, on the following factors:

- Number of subscribed ccTLDs
- Capacity of ccTLDs to appoint dedicated point of contact(s) (24X7)
- Capacity of individual ccTLD operators to take mitigating actions
- Cost of subscription

Until August 2013 the WG worked on the basic presumption that a vast majority of the ccTLD community, in terms of absolute number of ccTLDs and/or in terms of total number of domain names under management, would subscribe to the service and maintain their contact details up-to-date. In other words: if the service is only provided to a limited number of ccTLDs or a fraction of domain names under management, the value of the system as a whole for individual ccTLD operators who subscribed, is limited.

Further, in the view of the WG, the costs for implementation and maintenance of the system is a key factor for subscription. As such, the critical factor here is

maintenance of the system. This is not limited to maintenance of the database as such. The main costs will be associated with maintaining the organization that operates the incident response and the need to keep the data attributes in the database accurate, confidential and available.

Based on these considerations the CRI WG needed to understand if a critical mass of the ccTLD operators would be interested in subscribing to an Incident Repository service, in particular in light of the potential expenditures associated with the subscription and maintenance of such a system. To this end the CRI WG conducted a survey and the results were presented to the community at the Singapore meeting[5] and are also available online[6].

Recommendations of the WG: Iterative Approach

The results of the survey strongly suggest that the community considers a global ccTLD Contact Repository a valuable service (81%), however a limited willingness to pay for its development and operational costs (55%). Taking into account the results of the earlier work, the WG therefore recommends to:

- Start very simple with a secure mailing list
- Iteratively expand based on user experience, and review the funding model per iteration
- Consider alternatives such as having the Repository hosted by an established specialized nonprofit organization like Secure Domain Foundation to provide the service.
- Consider initiatives such as DNS-OARC and avoid duplicate efforts.
- Extent the scope of the Repository to all critical infrastructure with direct relation with DNS stability.

Such an approach would allow trust to be build over time and align the costs with the added value.

The ccNSO Council advised to set-up a small working group, which members are trusted by the community, to work on the details to develop and implement a secure mailing list .

If the ccNSO Council is inclined to create such an implementation WG for a secure mailing list, it is suggested this WG should take at a minimum the following parameters into consideration:

- The Mailman service should be hosted by a neutral party such as ISOC, ICANN or established specialized nonprofit organization(s).

---

[5] http://singapore49.icann.org/en/schedule/wed-ccnso-members/presentation-cri-26mar14-en.pdf

[6] https://www.surveymonkey.com/sr.aspx?sm=DkkO70qW0Ks5Cw6M1Dq1vAzvdjUN6C0_2fm36SVyP5nAg_3d

- Only subscription for and accessible to representatives of a ccTLD who are responsible for the security and stability of their ccTLD, and at most two people per ccTLD on the list.
- The CEO or admin contact (to be determined) decides who should be on the list for their ccTLD.
- The use cases should initially be limited to those by the Incident Response WG.

Such a secure email list combines a rudimentary Contact Repository (subscribers of the mailing list) and a communications channel (email). These two elements might evolve into separate components in the future to allow for multi-channel communications between ccTLDs during an incident.

The WG also recommends that such a follow-up working group studies the coordination and collaboration with other Contact Repositories Initiatives, such as DNS-OARC's contact repository for DNS operators and regional repositories such as the one currently under development by CENTR. To avoid reduction of the potential incident response capacity of the global internet community, different non-interoperable contact repositories should be avoided.

Draft planning

To assist the ccNSO Council and a future WG, if established, the CRI WG has developed a high-level iterative planning for the Contact Repository (see Figure 1). The first cycle consists of bringing the secure email service online, which we consider V1.0 of the eventual Contact Repository. The second cycle involves developing or buying the Contact Repository as a service (V2.0).

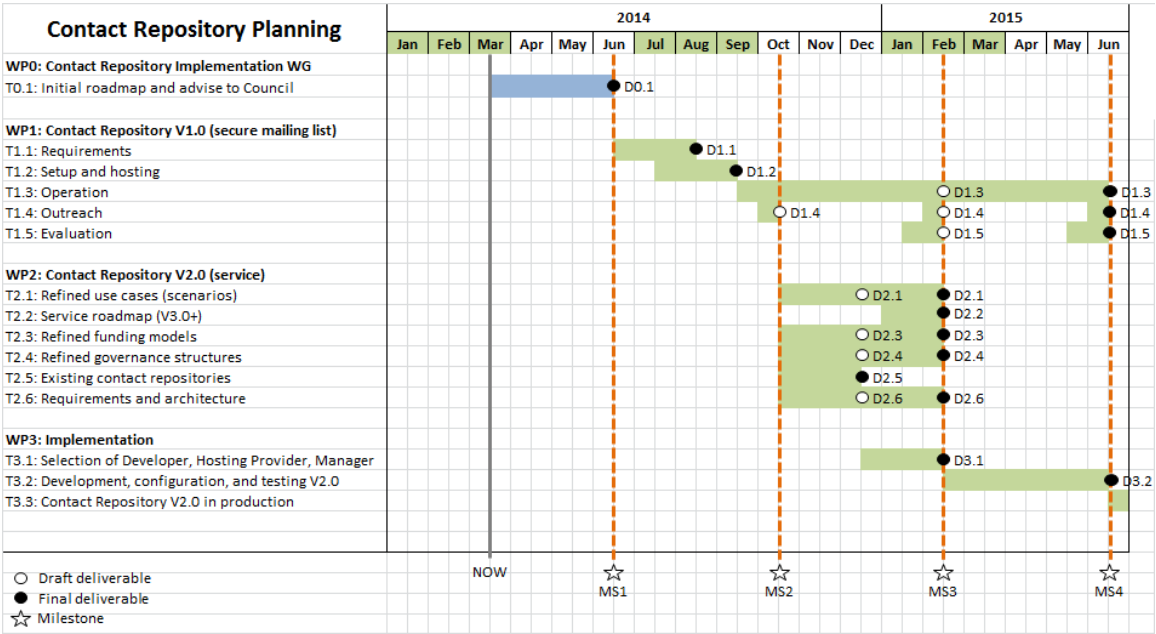


Figure 1. High-level planning.

Table 1 provides an overview of the milestones in Figure 1.

Table 1. List of deliverables.

No.	Title
MS1	ccNSO Council go/no go on proposed approach, establishment of new WG (ICANN50)
MS2	Contact Repository V1.0 (secure mailing list) available, start of work on V2.0 (ICANN51)
MS3	First round of evaluation results available (V1.0), go/no go to implement V2.0 (ICANN52)
MS4	Second round of evaluation results available (V1.0), V2.0. to production (ICANN53)

Table 2 provides an overview of the deliverables in Figure 1. We suggest aiming for 2 to 4 page deliverables that captures the essence of the corresponding work that has been carried out.

Table 2. List of deliverables.

No.	Title
D0.1	Initial roadmap and advise to Council
D1.1	Requirements document
D1.2	Description of setup
D1.3	Operational experiences
D1.4	Bundling of outreach results
D1.5	Evaluation report Contact Repository V1.0
D2.1	Refined use cases
D2.2	Refined service roadmap (V3.0+)
D2.3	Overview of funding models
D2.4	Overview of governance models
D2.5	Overview of existing repositories
D2.6	Requirements and architecture
D3.1	Implementers selection report
D3.2	Mailing Contact Repository V2.0

Annex A: list of membership CRI WG

Working Group Members

- Luis Diego Espinoza (Chair)
- Wim Degezelle, CENTR (observer)
- Cristian Hesselman, .nl
- Mohamed Ibrahim, .so
- Isak Jacobsen, .fo
- Antoinette Johnson, .vi
- Hitoshi Saito, .jp

Support Staff

- Bart Boswinkel
- Kristina Nordström
- Gabriella Schittek

Annex B: Model and documented requirements centralized repository (work in progress)

Draft Report for ccNSO

Contact Repository Implementation

Luis Espinoza, Chair

Antoinette Johnson

Isak Jacobsen

Hitoshi Saito

ccNSO CRI-WG – ICANN

July 2013

Abstract

The objectives of the Contact Repository Working Group (CRWG) formerly referred to as the Incident Repository Working Group (IRWG) is to propose a model of management, governance and funding in order to implement, operate and maintain documented procedures in response to one or more incidents.

The CRWG proposes the following list of suggested actions in order to accomplish the above mentioned objectives.

- Identify systems and services related to the Contact Repository of ccTLD and channels of communication for incident response. The two major components of the contact repository identified to accomplish the purpose of the interaction in case of incidents are:

    1. Directory Service (DS): the software system that stores, organizes and provides access to information in a directory or map between names and values.
    2. Contact Service Center (s) (CSC): the entity that operates processes to query the DS and manage all the contact information through different channels of communications such as telephone, fax, letter, e-mail, etc. This information should be stored and organized in the Directory Service.

- Implement sustainable mechanisms for the engagement of and interaction with ccTLD registries during security incidents that may impact the DNS.

1. Establish the baseline to determine cost estimates [or actual costs] and other relevant factors for implementation, maintenance and operation of the Contact Repository.

.

Table of Contents

Table of Contents 9
Section 1 10
Section 2. Contact repository functional description 11
Section 3. Governance model of the Contact Repository 18
Section 4. Funding model of the Contact Repository Implementation 21
Appendix 1. Contact Repository Relationship Diagram 22

Section 1

The CRWG defines an incident as a large scale, unintended malfunction of the Domain Name Service (DNS) or a systematic, rigorous preparation of an actual attack on:

1. The availability of the DNS or registration systems;
2. The data integrity or privacy of the DNS or registration systems;
3. The stability or security of the Internet at large;

where a coordinated international response by ccTLD operators and supporting organizations is advised.

Contact Repository Roles

1. Information Exchange: The Security Information Manager, the point of contact under any circumstance is authorized to access the DNS and when warranted issues early warnings.

2. Facilitate counter action: Inform the "participating community" about "an incident". Facilitate/enable community support for a community member.

Policy [Statement]Requirements of the Contact Repository

Policy for use of the resources of the Contact Repository should be limited to member organizations. The use cases included in this document should ensure but not be limited to preserve the confidentiality, integrity, and availability of information of the repository.

Section 2. Contact Repository Functional description

<BEGIN feedback Cristian Hesselman>

Based on what I gathered from the Beijing meeting, I think there are three major issues that we need to solve before we can really dig into the details of the requirements (see below). Once we have done that, we'll have a more detailed overall concept of the contact repository, from which I expect the requirements will follow in a natural way.

Issue #1: accommodate for the heterogeneity of the ccTLD community

- We somehow need to be able to accommodate the ccTLD community's wide range of views on who should manage the contact repository and who should finance it.
- One possible approach might be to cut out the central authority (the CSC) and fully distribute the system and its processes across the ccTLD community. This takes away the discussion on who should operate the system and it also reduces costs.
- One possible way of doing this would be by (1) requiring an X number of existing users to vouch for each new user that wants to include his contact info in the repository and (2) by putting the responsibility for keeping contact info up to date with the ccTLD (which is where it belongs, IMO).
- I think tackling the heterogeneity of the ccTLD community will be much more difficult in the centralized approach we're following now

Issue #2: We need to come up with a few (3?) realistic use cases/scenarios

- The scenarios need to show what kind of early warning messages need to be conveyed between ccTLD operators, in what format, and what the internet will gain from having such a sytem.
- The examples should largely drive the requirements for the repository so that it's clear *why* we need the set of requirements in Section 2.
- The example scenarios should preferably cover (or be based on) real-world incidents, for instance in terms of the information that was exchanged and how the incident was handled. I suggest to check with ICANN, I'm sure they're aware of a few.

Issue #3: We need to be able to indicate what the added value or novelty of the contact repository is compared to similar repositories, such as the one at DNS-OARC (see Figure 1 and Figure 2 below).

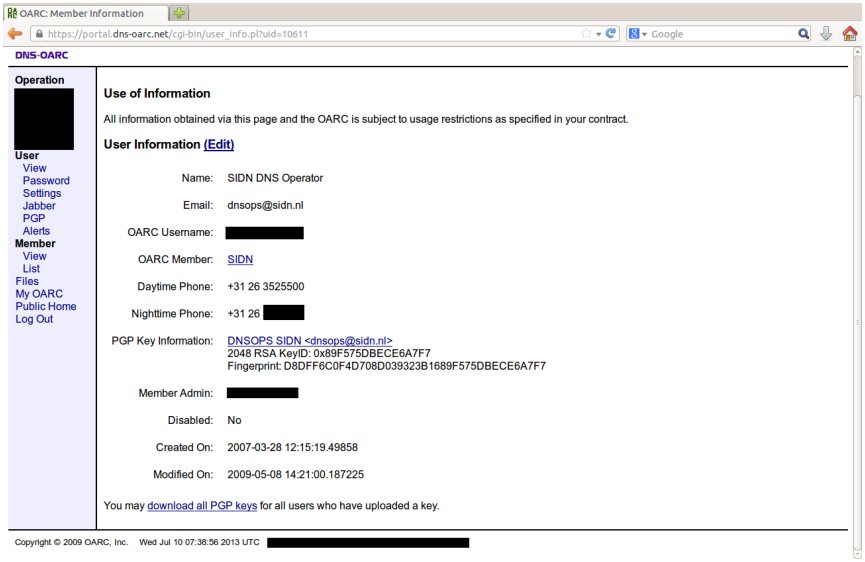


Figure 1. SIDN's contact information in the DNS-OARC repository,

Note that DNS OARC uses a vetting process for adding people to their contact repository, but that this is unlikely to scale to large numbers of users.

<END feedback Cristian Hesselman>

General Requirements

- The repository MUST support the real-life and envisioned uses cases defined in Section 1
- The repository MUST be available 24/7 and MUST be able to survive large-scale DNS or internet outages and security incidents..
- The repository MUST provide redundancy and fail over, which should be an integral part of the system.
- The access to the repository should be defined by a Policy of the Repository. The entities that can access the repository could include ICANN, ccTLDs, Regional Organizations, Incident Response Teams (FIRST, CERT, CSIRT, etc).
- Protect against unauthorized access and modification of repository contents. The repository must use at least 3 levels access control mechanisms (e.g. user, pass, token, etc)
- Primary and Alternative communication channels (not only internet)
- Provide Interfaces for different services (automated)
- The repository is able to store/search/deliver/delete Contact Information
- In a best effort manner, the data is kept accurate and complete.
- The repository is able to manage data at many levels of granularity.
- Access privileges to data in the repository can be managed at many levels of granularity.
- External search systems can be easily connected to the repository, in order to deal with specialized search fields.
- Administer the Database or Databases, Perform Queries.

- Provide comprehensive, readable, understandable documentation and on-line help thereby making it more precise to the external user who interacts with the system.

<BEGIN feedback Cristian Hesselman>

As for the requirement, I think we should more specific requirement categories, such as these 6:

1. Confidentiality, integrity, and availability. Examples:
    - It must be possible to obtain contact information from the repository without the availability of the DNS or the internet
    - The repository mustpush (a copy of) the contact information to end-user devices where possible in order to maximize availability
    - The repository must be accessible from a cell phone, for instance through an app
2. Registration and deregistration (creating/deleting an account)
3. Updating contact information
2. Obtaining contact information
3. Dealing with existing repositories, such as the one at DNS-OARC
4. Optional requirements on specific technologies to be used

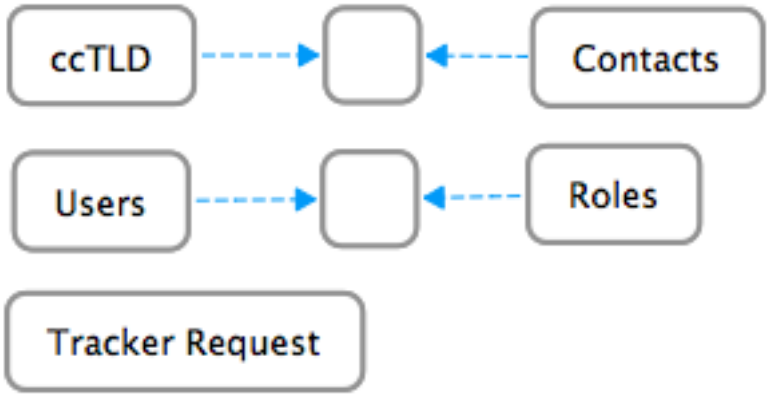
<END feedbackCristian Hesselman>

Main processes:

1. Respond to data requests of Contact Information
2. Contact management
    a. Browser/Search contacts.
    b. Add New Contact Information
    c. Update Contact Information
    d. Delete Contact Information
3. Periodically probe the information (Keep up to date).
4. User Management
    a. Assign roles according to the Policy of Information of the Repository.

1 **Process #1: Respond to Data Request of Contact Information.**

Preliminary data entities



Actors:

IRE = Incident Response Entity (IR Team or IR TaskForce) [example of IRE CERTS, FIRST, etc]

CRO = Contact Repository Operator, the person working in the Contact Center.

Process Flow

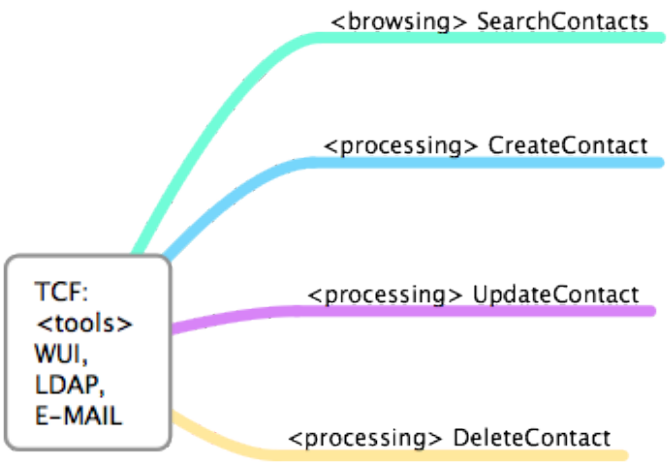
1. The IRE makes a data request to the CRO (query with specific contact information for specific ccTLD)
2. The CRO makes an entry in the tracker requests
3. The CRO run/execute the query of the data request to the CR
4. The CRO sends the response to data request
5. The IRE confirms that received the response
6. The CRO update the tracker request.
7. Result = obtained contact info

2 **Process #2: Contact management.**

The system should provide a web user interface (WUI) for the front end, and for the other systems access should provide lightweight directory access

protocol with SSL (LDAPS). Optional can implement CardDAV. The system must implement the following specifications. Why?

Preliminary data entities



Actors:

TCF = TLD Contact Information Facilitator (this is a role for the collecting information and not necessary).
DS = Directory Service System

Process Flow for WUI.

1. TCF prepare contact information according to the process to commit.
2. Create Contacts:
    a. TCF Login to the system with the credentials previously provided by DS User Management.
    b. TCF input contact data to the interface provided
    c. TCF commit the Contact profile.
    d. DS receive and validate the information according with the format and content allowed by DS policy.
    e. DS return an answer: Confirmation of creation of the contact or Rejection with an explanation.

f TCF take actions according to the returned answer: In case of confirmation, keep the ID of transaction, in case of rejection correct the transaction and start over step (b.)
g If there more contacts to include, TCF goes to step (b.)
h TCF logout from DS system.

3 Search Contacts:
a TCF Login to the system with the credentials previously provided by DS User Management. If no valid credentials is supplied, the DS can show only public information.
b TCF input the key criteria for the search into DS.
c DS returns an answer according with the authorization of the logged in: Positive results or empty results.
d TCF evaluate answer from DS and obtain the information requested or change the criteria and goes to step (b.)
e TCF can keep searching information providing search criteria in the step (b.)
f TCF logout from DS System (not necessary if no login was provided in step a.)

4 Update Contacts:
a TCF Login to the system with the credentials previously provided by DS User Management.
b TCF input the contact key criteria to search.
c DS returns an answer according with the authorization of the logged in, prefilling editable fields, according with the DS policy.
d TCF update contact data to the interface provided.
e TCF commit the updated Contact.
f DS receive and validate the information according with the format and content allowed by DS policy.
g DS return an answer: Confirmation of creation of the contact or Rejection with an explanation.
h TCF take actions according to the returned answer: In case of confirmation, keep the ID of transaction, in case of rejection correct the transaction and start over step (b.)
i If there more contacts to update, TCF goes to step (b.)
j TCF logout from DS system.

5 Delete Contact:
a TCF Login to the system with the credentials previously provided by DS User Management.
b TCF input the contact key criteria to search.
c DS returns an answer according with the authorization of the logged in, showing the contact to delete, according with the DS security policy.
d TCF delete Contact data to the interface provided.

e TCF confirm deletion of the Contact.
f DS return a confirmation of deletion.
g If there more contacts to delete, TCF goes to step (b.)
h TCF logout from DS system.

NOTE: The process flow for LDAPS and CardDAV should be according with the protocol specifications itself, but implementing at least the basic functions in this section: Create Contacts, Update Contacts, Delete Contacts, Search Contacts

5 **Process #3: Periodically probe the information (Keep up to date).**
The process of probe the information in the Contact Repository should be delivered with the following recommendations:

5.1 Capable of operating 24/7/365 and includes the following tools:

- E-mail response management
- Web Chat
- Session recording and transcript mailing
- Self-service Knowledge-base
- Analytics and Quality System
- Telephony infrastructure.
- Interactive Voice Response (IVR) technology

5.2 Frequency and rotation of communication methods.

- Probe 1 emergency contact each 3 months using 1 of the possible way of contact.
- Rotate the ways of contact in a year cycle for the same TLD.
- Alternate the set of contacts for each TLD in a year cycle.

5.3 Ability to support multi-lingual communications with customers.
5.4 Allows remote access with appropriate permission and security.

Estimated Monthly outbound contacts volume				
Number of TLDs		200	1000	5000
Number of contacts in the repository		400	2000	10000
Criteria of frequency				
1/15 monthly	Voice	13	67	333
1/15 monthly	Email	13	67	333

1/15 monthly	Fax	13	67	333
1/15 monthly	Chat	13	67	333
1/15 monthly	Letter/telegram	13	67	333

Note: Criteria of frequency is based on distribute all the TLD during 3 months and each month distribute the media of contact by equals. 1/5 of 1/3 of the total number of TLD.
Note2: The table assumes rotation of contacts within each TLD.

Section 3. Governance model of the Contact Repository

Standing Committee

1. Items to be governed
   a) Policy and review of Use cases in Section 1.
   b) Relation with Service Provider. Follow contractual and legal oversight of the procurement of the Service Provider.
   c) Policy for users.
   d) Relation with Subscribers.

2. Service is initially limited to ccTLD operators, members and non-members of the ccNSO.

3. WG organizes its activities through WG/Committee's which are open to members and non-members with ICANN staff support and/or providing substance matter expertise.

4. WG reports to ccNSO Council. Council oversees WG/ committees

Proposed governance structure:

ccNSO Council establishes standing committee's to manage relation with:
- Service provider (agreement compliance)
- Relation with subscribers. Subscribers apply through committee to ensure subscriber is ccTLD.
- Maintain register of subscribed ccTLD's.

WG or standing committee also maintains USE cases and reviews use of service. If change of use cases is indicated, new WG (temporary) consults with community of users and others,

WG comprises of members and non-members of the ccNSO, appointed by the Council with additional requirement that members of WG should be using the service.

WG report to the ccNSO Council and users (at Regional meetings and ccNSO meeting, and by email).

WG is supported by ccNSO secretariat and with expert assistance of SSR department

It is proposed that the Contact Repository have a Standing Committee whose specific role shall be to review the performance of the Contact Repository, make recommendations for change and or expansion; make decisions on membership and certification issues and provide input to goals and /or accomplishments of programs.

Standing Committee Composition

The Steering Committee shall consist of _____( ) members. The members of the Steering Committee shall be elected by majority vote of Contact Repository Full Body of Members. The Steering Committee will designate individuals to serve in the capacity of: [eg.] Steering Committee Chair; Steering Committee Vice-Chair and Steering Committee Secretary.

Standing Committee Term

The ____ ( ) members shall each serve for a term of ___ ( ) years [subject to Section §] with their terms being staggered so that every year the terms of ___ ( ) of these members expire. Elections shall normally be held during the annual Contact Repository meeting of the year, and terms of office shall coincide with the annual year meeting period in which they expire.

Standing Committee Term Limitation

An individual may only serve on the Steering Committee in any capacity for a maximum of ___ ( ) terms, except under Section §_____. Upon completion of these ___ ( ) terms of office, they are not eligible to serve on the Steering Committee in any capacity including [as] Steering Committee Chair; Steering Committee Vice-Chair and Steering Committee Secretary until at least ____ ( ) year (s) has passed.

Standing Committee Term Limitation Exception

1. In the event an elected Steering Committee member resigns, is dismissed, or is no longer capable of performing their duties, then a new member will be elected by the Full Body of Members at the next scheduled Contact Repository meeting for a term that will expire when the term of the original member would have expired. If this term is one year or less, it will *not* count for purposes of calculating consecutive terms.

2. Any member of the Contact Repository Full Body may request the dismissal of a Standing Committee member on the basis that the individual is no longer performing their duties as ethically required. Such a request must be submitted to the Chair of the Contact Repository, by verifiable digitally signed e-mail for possible further consideration of the Contact Repository Full Body of Members.

Standing Committee Meetings

The Standing Committee in general will conduct their meetings in conjunction with meeting of the Contact Repository, but at their discretion may also meet at other times as necessary either via audio or video conference.

Responsibilities

Standing Committee Secretary

The Steering Committee Secretary (Secretary) shall be responsible for ensuring that all committee meetings are documented either via notes or audio recordings. The Secretary is responsible for transmitting copies of the meeting notes to all Steering Committee members, as these documents are based upon discussions that are sensitive in nature they are classified as confidential. The Secretary shall be responsible for developing an Executive Summary of each Steering Committee meeting and transmitting the Executive Summary to the Chair of the Contact Repository.

The Secretary is responsible for scheduling and issuance of meeting notifications to the Steering Committee members in addition to inviting other persons. The Secretary shall circulate a copy of the meeting agenda to all Steering Committee members at least ____ ( ) day(s) before the scheduled meeting.
The Secretary shall develop Standing Committee proxy forms and disseminate said documents when necessary and appropriate.

Standing Committee Chair

The Standing Committee Chair shall chair all committee meetings. In the event the Chair is unavailable, then the meeting can be chaired by the Standing Committee Vice –Chair. In the absence of the Standing Committee Vice-Chair, the order of precedence shall be determined by whoever has served for the longest continuous period, and in the event of two (2) or more members having served the same amount of time, the member elected first (as Standing Committee Chair) will take precedence.

Standing Committee General Members

Decisions of the Standing Committee shall be through a simple majority consensus. In the event of a tie the Standing Committee Chair, having a casting vote in the event of a tie. The quorum required for valid decisions shall be a total number of ___ ( ) votes, not including any casting vote. Each Standing Committee member has one (1) vote. A member may authorize another Standing Committee member to enter a proxy vote on their behalf. The Standing Committee member must notify the

Standing Committee Secretary in advance via verifiable digitally signed e-mail ____ ( ) days prior to the meeting of their intent to authorize another Standing Committee to cast a proxy on their behalf. No Standing Committee member may vote on behalf of more than one (1) Standing Committee Member.
Any Standing Committee member may at a meeting request a poll. In the event of an e-mail poll, votes must be submitted by verifiable digitally signed e-mail _____ ( ) days of the poll be called on the mailing list.

Section 4. Funding model of the Contact Repository Implementation

Outline Funding model

Incident Response repository
The costs categories that need to be covered are:

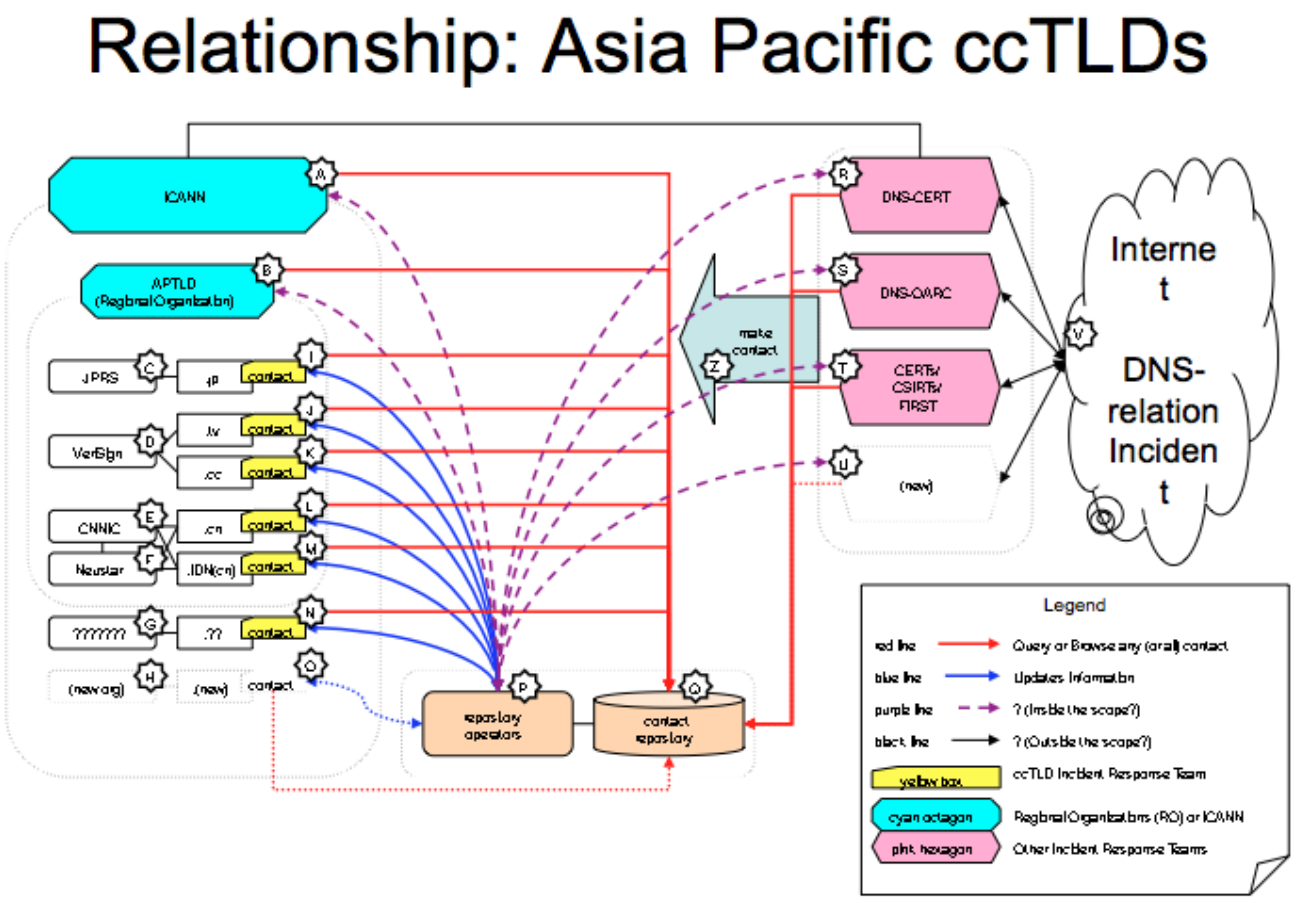
- Set-up fee (once off), either to build a new repository or to adjust existing system to the requirements defined. This depends on the preferred method of implementation (buy, make or use and adjust an existing system)
- Maintenance fee (Annual Subscription). Depending on the adopted requirements (maintenance of contact details)

Requirements for funding models
An incident repository only adds value to the community if a critical mass of ccTLD's are and remain to be subscribed for using it. In order to be sustainable, the critical mass has to be a very large proportion of the ccTLD's. From a funding perspective the costs for setting-up and maintaining subscriptions should therefore not be prohibitively high for the vast majority. The funding needs to be sustainable and predictable over a long period of time i.e. the model needs to ensure that a critical mass remains to be subscribed.

Funding Models
1. Uniform subscription and set-up fee applied to all ccTLD's .
Depending on the implementation model, the risk of prohibitive high annual subscription fees is eminent.

2. Cross-ccTLD funding
The more affluent ccTLD's will partially cover the costs for the less affluent. The issues here will be to determine the distribution model applied across the ccTLD's to ensure the continuity of funding. With regard to distribution model, the model of the ccNSO Finance WG could be used, with the caveat that that model will be based on voluntary contributions, and in this case it needs to be committed and sustainable.

3. ICANN funding (ICANN, other)
The annual subscription fees are funded by ICANN, and will be directly attributable to the ccTLD's. Part of the financial contribution is used for this purpose. In effect, the result is that ICANN collects and ensures payment. The more affluent ccTLD will bear the brunt as under the previous model, unless this is partly funded by ICANN from other resources.

4. Mixed funding
Direct contribution by the ccTLD's, support by the more affluent ccTLD's and ICANN.

Appendix 1. Contact Repository Relationship Diagram