SECIR Final Report

Deliverable D4, Version 1.0 (draft)
June 30, 2015

SECIR Working Group
http://ccnso.icann.org/workinggroups/secir.htm

Cristian Hesselman (.nl), Erwin Lansing (.dk), Jacques Latour (.ca), Frederico Neves (.br), Abibu Ntahigiye (.tz), Geng-Da Tsai (.tw), Gabi Schittek (ICANN)

Summary

The main result of the ccNSO working group "Secure Email Communication for ccTLD Incident Response" (SECIR) is the TLD-OPS mailing list, a basic incident response facility that serves as a Contact Repository for ccTLDs worldwide. It enables ccTLD operators to easily and quickly look up each other's contact information (name, email address, and phone number), thus allowing them to better handle security and stability-related incidents that require a coordinated response of ccTLDs at the global level. Examples of these incidents include targeted attacks on or malfunctions of registration systems, the DNS, or the Internet at large.

The TLD-OPS list is only accessible to people who are responsible for the overall security and stability of a ccTLD and in particular for the authoritative name servers and registration system of the registry. The list is explicitly open to both ccNSO members and non-ccNSO members and is set up in such a way that every ccTLD will be able to join.

The main conclusion that we draw from our work is that our approach has been relatively successful because we managed to get 134 (54%) of all ASCII ccTLDs and 20 (44%) of all IDN ccTLDs to subscribe to the TLD-OPS list within four months (mid February until mid June, 2015). Of these subscribers, 44 (30%) are non-ccNSO members. We also conclude that the ccTLD community continues to consider a Contact Repository to be useful incident response facility, which is in line with the results of the survey on this topic that the CRI WG carried out in late 2013.

Our main recommendations are to (1) establish a TLD-OPS Standing Committee that governs the daily operations and further development of the TLD-OPS list and the TLD-OPS "ecosystem", (2) to focus on further growing the number of TLD-OPS subscribers and the actual use of the list until ICANN56 (June 2016), and (3) to add the contact information of a ccTLD's security and stability contacts to the IANA database and have the TLD-OPS list interface with it.

This document is the final report of the SECIR WG and concludes its work.

Document History

No.	Date	Authors	Changes
V0.0	2014-08-01	Cristian Hesselman	First initial draft
V0.1	2014-08-11	Cristian Hesselman	Update based on first conference call (sections 1 and 3)
V0.2	2014-08-21	Cristian Hesselman	Update based on second conference call
V0.3	2014-09-23	Jacques Latour	Added OPS-T and requirements
V0.4	2014-09-24	Cristian Hesselman	Updated Figure 1, updated Chapter 3, added Section 5.1 and Chapter 6 (Similar Services)
V0.5	2014-10-15	Cristian Hesselman	Updated Chapter 7, now that we'll almost certainly use OPS Trust, inserted new overview picture (Fig. 1)
V0.6	2014-11-10	Jacques Latour	Major revision based on using DNS-OARC and OPS-T.
V0.7	2014-12-29	Cristian Hesselman	Addition of implementation based on OPS-TLD list (Section 6), revision of Section 7, integrated Section 8 into Section 7
V0.8	2015-05-24	Cristian Hesselman	Major update, focusing on (1) an overview of the TLD-OPS roles and services, (2) the approach of the SECIR WG, and (3) conclusions and recommendations. Removed all other chapters because they became part of the TLD-OPS overview document.
V0.9	2015-05-29	Cristian Hesselman	Refined document summary, conclusions, and recommendations. Plus various textual improvements.
V0.10	2015-05-31	Cristian Hesselman	Added IDN statistics to Section 1.
V0.11	2015-06-17	Cristian Hesselman Erwin Lansing Jacques Latour Gabi Schittek	Updated statistics in Section 1, added non-subscribed ccTLDs to Appendix A, processed feedback of WG members and the feedback of Patrik Fältström (SSAC)
V0.12	2015-06-20	Cristian Hesselman	Processed feedback of Kim Davies (IANA).
V1.0	2015-06-30	Cristian Hesselman Erwin Lansing Jacques Latour Frederico Neves Abibu Ntahigiye Geng-Da Tsai Gabi Schittek	Final version approved by all WG members and submitted to ccNSO Council.

Table of Contents

1 Introduction

The ccNSO working group "Secure Email Communication for ccTLD Incident Response" (SECIR) [1] started its work in July of 2014, using the deliverables of the working group "Contact Repository Implementation" (CRI) [3] as a starting point.

The two main objectives of the SECIR WG were to [9]:

- Implement version 1.0 of the ccTLD Contact Repository, which consists of a secure mailing list that enables ccTLD operators to (1) obtain each other's contact details and (2) exchange rudimentary incident messages; and
- Actively highlight and promote the added value of the SECIR mailing list to invite as many ccTLD operators as possible to join the list.

The SECIR WG's implementation of the Contact Repository is the TLD-OPS mailing list [6], which enables ccTLD operators to easily and quickly look up each other's names, email addresses, and phone numbers, even in offline situations. This enables them to better handle security and stability-related incidents that require a coordinated response of ccTLDs at the global level (e.g., [4]). Examples of these incidents include targeted attacks on or malfunctions of registration systems, the DNS, or the Internet at large.

We did not add encryption facilities to the list (e.g., PGP), because we felt their set up might form too big a threshold for some ccTLDs to join the list. We discussed this with the chairs of SSAC and ICANN's Security Stability Resiliency (SSR) team [10] at ICANN52 and they concurred. Since the TLD-OPS list is unencrypted, subscribers should exchange actual incident information through a different channel, such as telephone or instant messaging.

Table 1 shows an overview of the number of ccTLDs that have joined the list since ICANN52 (Feb 2015), which is when we started to invite ccTLDs to subscribe [2]. Of the ccTLDs on the list, 44 (30%) are non-ccNSO members.

Table 1. TLD-OPS subscribers per region, ASCII ccTLDs (June 17, 2015).

Region**	Subscribed		Non-subscribed		Total*
Total	***134***	***54%***	***112***	***46%***	***246***
Africa	21	41%	30	59%	51
Asia-Pacific	43	49%	44	51%	87
Europe	47	87%	7	13%	54
North America	4	67%	2	33%	6
Latin America and Caribbean	19	40%	29	60%	48

* On June 17, 2015, there were a total of 255 ccTLDs in the root zone (http://www.iana.org/domains/root/db). The status of six ccTLDs was "not assigned" (.bl, .bq, .eh, .mf, .ss, .um), one was "reserved" (.gb), and one was set to "retired" (.tp), thus leaving 247 (we have one ccTLD unaccounted for in our stats).

** We divided ccTLDs into geographic regions based on https://www.countries-ofthe-world.com

Table 2 shows the subscription statistics for IDN ccTLDs over the same period. We only considered delegated IDNs.

Table 2. TLD-OPS subscribers per region, IDN ccTLDs (June 17, 2015).

Region**	Subscribed		Non-subscribed		Total*
Total	***20***	***44%***	***25***	***56%***	***45***
Africa	2	40%	3	60%	5
Asia-Pacific	14	45%	17	55%	31
Europe	4	44%	5	56%	9
North America	0		0		0
Latin America and Caribbean	0		0		0

* On June 17, 2015, there were a total of 46 IDN ccTLDs in the root zone (http://www.iana.org/domains/root/db). 45 of them were active, which is the number we used in this table.
** We divided ccTLDs into geographic regions based on https://www.countries-ofthe-world.com

The full list of TLD-OPS subscribers is available at the TLD-OPS homepage [6]. Appendix A contains the list of ccTLDs still missing at the moment of writing, grouped by geographical region.

We refer to the TLD-OPS Overview document [8] for examples of communication scenarios that illustrate how TLD-OPS subscribers can use the list and how they get subscribed to it.

The rest of this final report provides an overview of the TLD-OPS "ecosystem" (Section 2), the approach we took that led to this result (Section 3), the conclusions that we draw from our work (Section 4), and the WG's recommendations (Section 5). The appendices contain more information on ccTLDs that have not subscribed yet (Appendix A), an overview of TLD-OPS-like initiatives at Regional Organizations (Appendix B), the list of deliverables of the SECIR WG (Appendix C), and our outreach results (Appendix D).

2 Overview

Figure 1 provides an overview of the TLD-OPS "ecosystem" in terms of its roles (Section 2.1), services (Section 2.2), and governance (Section 2.3). The central facility is the TLD-OPS server, which host the TLD-OPS mailing list and the TLD-OPS Script that we developed in the WG. We used mailman [5] for the TLD-OPS mailing list, which is a widely used mailing list software.

The SECIR WG developed the components with a green checkmark. The orange checkmark indicates that we managed to get 134 (54%) of all ASCII ccTLDs and 20 (44%) of all IDN ccTLDs on the list (see Table 1), but that we're not there yet.

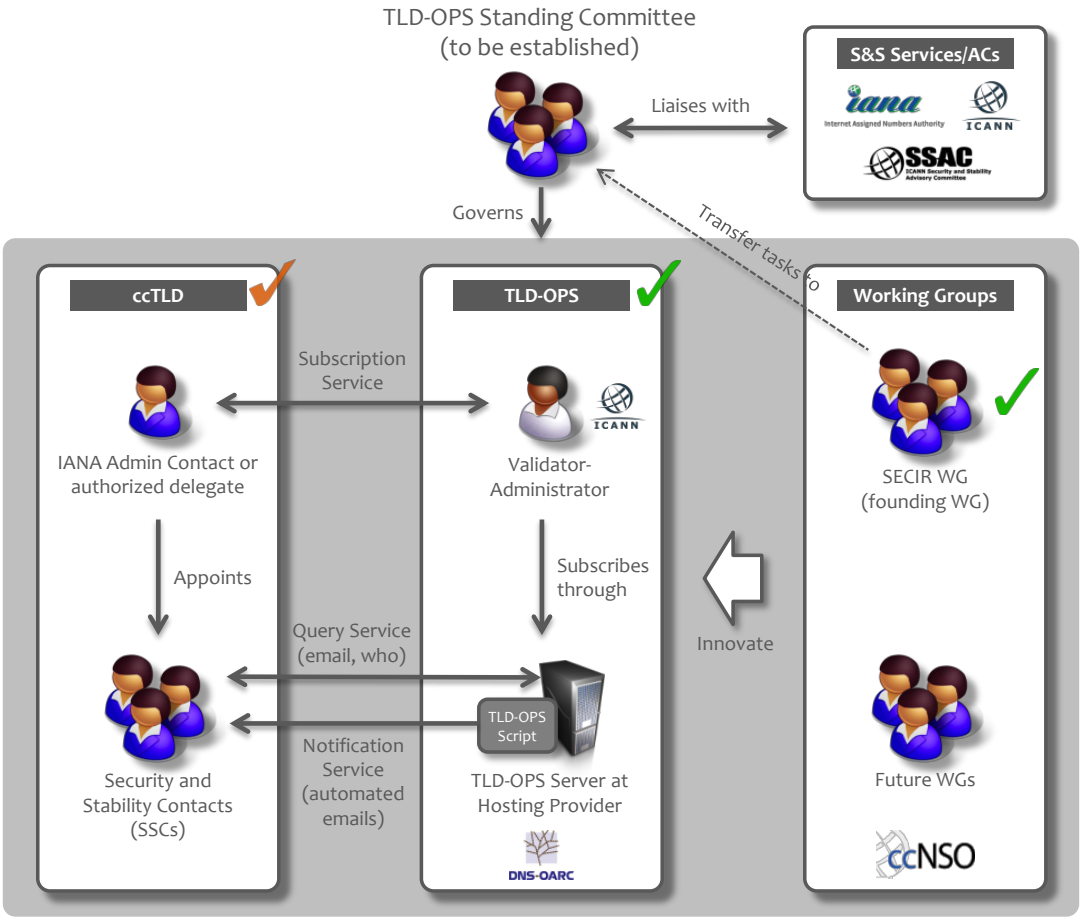

Figure 1. TLD-OPS overview.

2.1 Roles

Table 3 shows the TLD-OPS roles, their responsibilities, and the parties playing these roles. The roles we distinguish are the Security and Stability Contact (SSC) of a ccTLD, the IANA Admin Contact, TLD-OPS Validator, TLD-OPS Administrator, and TLD-OPS Hosting Provider.

Table 3. TLD-OPS operational roles.

Role	Responsibilities	Party
Security and Stability Contact (SSC)	A person who is responsible for the overall security and stability of a ccTLD, in particular for the ccTLD's authoritative name servers and its registration system. Every ccTLD must have at least two SSCs, one primary and one secondary. An SSC may be responsible for multiple ccTLDs. We currently allow at most three SSCs per ccTLD to subscribe to the TLD-OPS list.	Employee of a ccTLD operator or a third party contracted by that ccTLD
IANA Admin Contact	A person in the IANA database who is the administrative contact for a particular ccTLD. The Validator uses the IANA Admin Contact as a "trust anchor" to obtain the identity and contact information of the SSCs of a ccTLD.	Employee of a ccTLD operator
Validator	A person, group of persons, or organization that is responsible for authenticating SSCs. The Validator contacts the ccTLD's IANA Admin Contact in the IANA database to check if the SSC is responsible for that ccTLD's security and stability.	ccNSO Secretariat
Administrator	A person, group of persons, or organization that is responsible for administering the TLD-OPS mailing list. This for instance includes adding and removing SSCs to and from the list based on the authentication decisions that the Validator makes.	ccNSO Secretariat
Hosting Provider	The organization that hosts the TLD-OPS list server and the TLD-OPS Script. The TLD-OPS Script automatically sends out the full list of subscribed SSCs and their contact info on the list on a regular basis so SSCs may also access the contact info of their peers in offline situations through their inbox. The hosting provider supplies network connectivity, server hardware, and (virtualized) operating systems.	DNS-OARC

The ccNSO Secretariat currently plays the roles of both Validator and Administrator. We believe the ccNSO Secretariat is a suitable entity because the ccTLD community trusts them and because they already manage a number of mailing lists in their day-to-day business. The WG foresees that the ccTLD's IANA Admin Contact or an

appointed contact might become the Administrator for a particular ccTLD in the future (see Section 5.3).

The Hosting Provider for the TLD-OPS mailing list is DNS-OARC, as approved by the ccNSO community at ICANN51 in Los Angeles.

2.2 Services

Table 4 shows the services that the Validator, Administrator, and TLD-OPS List Server provide and a high-level description of the interactions involved. We distinguish five services: SSC subscription, SSC notification, SSC query, SSC update, and SSC removal. More details on the subscription, notification, and query services are available from [8].

IANA Admin Contacts need to make sure that their emails come from the address they have registered in the IANA database for their ccTLD's Administrative Contact. If this is not possible, they *must* copy the IANA admin email address in their email to enable the IANA Admin Contact to "track and trace" the interaction.

Table 4. TLD-OPS services.

Service	Roles involved	Interactions
SSC Subscription	IANA Admin Contact Validator Administrator TLD-OPS List Server	The IANA Admin Contact of a ccTLD informs the Validator-Administrator of the contact details of the SSCs of that ccTLD. The Validator-Administrator subscribes the SSCs to the TLD-OPS mailing list through the list server.
SSC Notification	SSCs TLD-OPS List Server TLD-OPS Script	The TLD-OPS script regularly sends out automated SSC Notifications on the TLD-OPS list. These messages contain the *full* list of subscribed SSCs and their contact information (ccTLD, first name, last name, phone number, and email address), thus enabling SSCs to also lookup this type of information in offline situations via their inbox. The scripts sends out SSC Notifications once a month as well as every week if the list of subscribed SSCs has changed.
SSC Query	SSCs TLD-OPS List Server	Subscribed SSCs query for contact information of their peers by sending an email asking them for this type of info. Subscribed SSCs can also get this information by sending a mailman "who" command to the List Server.
SSC Update	SSC	The IANA Admin Contact of a ccTLD

	IANA Admin Contact Validator Administrator TLD-OPS List Server	informs the Validator-Administrator of the contact details of the new SSCs of that ccTLD and which of the old SSCs they replace. SSCs modify their contact details themselves through the TLD-OPS list server without involvement of the Validator-Administrator.
SSC Removal	IANA Admin Contact Validator Administrator TLD-OPS List Server	The IANA Admin Contact of a ccTLD requests the Validator-Administrator to remove the SSCs of that ccTLD from the list. The Validator-Administrator unsubscribes the SSCs from the TLD-OPS mailing list through the list server.

2.3 Governance

The governance part of the TLD-OPS ecosystem consists of the TLD-OPS Standing Committee, which governs the daily operation and further development of the TLD-OPS ecosystem (see Figure 1). The Standing Committee works with the ccNSO Council to start new WGs that will further develop the TLD-OPS ecosystem and the underlying technical system.

The SECIR WG has effectively carried out the responsibilities of the Standing Committee during the initial development of the TLD-OPS ecosystem and we therefore recommend transferring these responsibilities to the Standing Committee right after the SECIR WG concludes its work (see Section 5.1). The ccNSO Council will initiate the establishment of the TLD-OPS Standing Committee, if they concur with our recommendations.

The TLD-OPS Standing Committee's responsibilities include:

- Developing and implementing new TLD-OPS policies and technical features in collaboration with the ccTLD community and other stakeholders such as IANA, SSAC, and ICANN's Security Stability Resiliency (SSR) team [10].
- Working with the Validator, IANA, SSAC, and SSR to "detect" ccTLDs that have gone through a redelegation and invoke the corresponding procedures.
- Regularly reviewing TLD-OPS processes, system performance, and agreements with contracted service providers, such as the TLD-OPS Hosting Provider (see Section 2.1). The latter includes the renegotiating of these contracts and if necessary contracting other parties.
- Deciding on which ccTLDs to subscribe to or unsubscribe from the TLD-OPS list in cases where the TLD-OPS Validator believes this requires a decision from the Standing Committee.
- Reporting to the ccNSO Council, SSCs as well as to the ccTLD community at large on the status and expected development of the TLD-OPS ecosystem.
- Requesting and managing a budget for the TLD-OPS list should this be required to manage and innovate TLD-OPS.

The TLD-OPS Standing Committee should represent the global ccTLD community and should for instance consist of:

- SSCs that are members of the TLD-OPS list
- At least one member from each region (AF, AP, EUR, NA, LAC)
- A mix of ccNSO and non-ccNSO members
- A member of SSAC, IANA, and ICANN's SSR team
- One or more members of other stakeholders, such as DNS operators and ISPs
- A chair, vice-chair, and a secretary

3 Approach

The approach we took to develop the TLD-OPS ecosystem of Figure 1 is based on a set of key requirements for the TLD-OPS list (Section 3.1) and two principal design decisions: (1) that the TLD-OPS list would need to be unencrypted (Section 3.2) and (2) that it would need to use a model of personal trust (Section 3.3).

3.1 Key Requirements

Table 5 provides an overview of the key requirements for the TLD-OPS list. We did not yet fully address the requirement that the list should be able to interact with similar facilities at Regional Organizations because they use different systems of different levels of maturity (see Appendix A).

Table 5. Key requirements.

Requirement	Description	Rationale
1. Further increase trust	The TLD-OPS list must facilitate a further enhanced level of trust within the ccTLD community.	A further increased level of trust is crucial for ccTLDs to collaboratively handle large-scale security and stability-related incidents and to further improve the collective incident response capabilities of the ccTLD community.
2. Easy to use	The TLD-OPS list must enable any SSC of any ccTLD to obtain the contact information of his peers in an easy way irrespective of the SSC's technical skills.	The global ccTLD community is diverse in terms of languages and technical expertise.
3. Always accessible	Any SSC of any ccTLD must be able to use the TLD-OPS list using widely used applications and operating systems, including in offline situations.	The global ccTLD community is diverse in terms of available technical resources (applications, devices, network capacity), so a "lowest common denominator" is important for adoption. Large-scale security and stability-related incidents may involve (partial) internet outages.
4. Near-zero costs	The costs of developing and operating the TLD-OPS list must be near zero.	The global ccTLD community is diverse in terms of available financial resources, plus that this is a key requirement that came out of the questionnaire

of the CRI WG [3].

3.2 Unencrypted List

Our first major design decision was to use the TLD-OPS list as is and not to encrypt it. The underlying rationale is that this keeps the list easy to use, available across devices and operating systems, and cheap (requirements 2, 3, and 4 in Table 5). Requiring SSCs to set up encryption facilities such as PGP often requires detailed technical expertise, which might not be readily available at every ccTLD (requirements 2 and 3). The same holds for dedicated incident response facilities such as OPS-Trust [7]. We developed and added the TLD-OPS Script to make the contact information of SSCs available in offline situations (requirement 3).

Since the TLD-OPS list is unencrypted, we recommend that subscribed SSCs exchange actual incident information through a different channel, such a telephone call or secure instant messaging.

If SSCs nonetheless decide to exchange such type of information through the TLD-OPS list, then we urge them to use the color codes and guidelines in Table 6 and clearly mark each message accordingly, for instance by including "[TLP-AMBER]" in the subject line. All responses to such a message inherit the same TLP code, unless the respondent indicated otherwise. If SSCs do not provide a TLP level, the default TLP level is RED.

Table 6. TLP color codes for sharing actual incident information.

TLP Color*	TLD-OPS Definition**	Sharing of Incident Info
RED: for named recipients only	TLD-OPS subscribers may not share RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed. This applies both to message content as well as sender identity (person or organization).	TLD-OPS subscribers explicitly flag message as RED. Incident info is relevant for one or a few ccTLDs. Subscribers must use a different communications channel to exchange the info and must not use TLD-OPS as the list is unencrypted.
AMBER: limited distribution	TLD-OPS subscribers may only share AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.	TLD-OPS subscribers explicitly flag message as AMBER. Incident info is relevant for a relatively large number of subscribed ccTLDs. Subscribers should consider sharing this information through a different channel if possible as the list is unencrypted.

GREEN: community-wide distribution	TLD-OPS subscribers may share GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.	TLD-OPS subscribers explicitly flag message as GREEN.
WHITE: unlimited distribution	TLD-OPS subscribers may distribute WHITE information without restriction, subject to copyright controls.	TLD-OPS subscribers explicitly flag message as WHITE.

* Traffic Light Protocol: http://en.wikipedia.org/wiki/Traffic_Light_Protocol
** Based on the definition of US-CERT: https://www.us-cert.gov/tlp
List members must not share automatically generated information on the list

3.3 Personal Trust

Our second main design decision was to use a personal trust model for TLD-OPS, which means that SSCs can only subscribe to the list with their personal email address and phone number. The underlying rationale is that we believe that a personal trust model will contribute to further increasing trust within the ccTLD community (requirement 1 in Table 5), for instance because people start recognizing each others names. The consequence is that role-based email addresses are not allowed on the TLD-OPS list, because they typically do not provide insight in who is behind them.

The vouching model that is typically used in the incident response community (e.g., in the OPS-Trust system [7]) is unsuitable for the TLD-OPS list. This is because the ccTLD community is a large group, which means that it will be hard to get relatively unknown people on the list using the vouching model.

4 Conclusions

Our main conclusion is that our approach (see Section 3) was relatively successful because we managed to get 134 (54%) of all ASCII ccTLDs and 20 (44%) of all IDN ccTLDs to subscribe to the TLD-OPS list within four months (from mid February until mid June, 2015). Of these subscribers, 44 (30%) are non-ccNSO members. We are confident that this number will increase over the next few months because we appear to have reached a critical mass of subscribers and because the Validator-Administrator (the ccNSO Secretariat) is getting more and more successful in getting ccTLDs on the list who are difficult to reach.

Based on the current number of TLD-OPS subscribers, we also conclude that the ccTLD community continues to consider a Contact Repository to be useful incident response facility, which is in line with the results of the questionnaire on this topic that the CRI WG carried out in late 2013 [3]. The true added value of the list will obviously be its use to handle an actual large-scale incident, which (fortunately) has not occurred yet at the time of writing.

We furthermore conclude that the main challenge of our work consisted of devising an approach that would work for every ccTLD on the planet. We learned that a plain mailing list extended with a TLD-OPS-specific script (see Figure 1) was an appropriate technical approach, which also enabled offline use of the Contact Repository through the TLD-OPS Script. We believe a more technologically advanced facility such as an encrypted mailing list or a dedicated incident response platform (e.g., OPS-Trust [7]) would have worked less well because it would have raised the bar for joining the system too much for some ccTLDs. We also learned that simplicity is key on the procedural side and that even the lightweight subscription procedure we developed for TLD-OPS frequently required follow-up from the Validator-Administrator.

Our final conclusion is that our outreach efforts were a crucial component to get folks on the TLD-OPS list and for the continued support of the ccTLD community. We believe that the TLD-OPS flyer, the TLD-OPS homepage, the summaries of the WG's conference calls, and our regular status updates at ccNSO meetings were instrumental to our level of success. Finally, we learned that it is of paramount importance to explain the key design decisions we made in setting up the TLD-OPS list, such as why we decided to opt for a personal trust model.

5 Recommendations

Our main recommendations are to put the TLD-OPS Standing Committee of Figure 1 in place (Section 5.1), to focus on further growing the number of TLD-OPS subscribers (Section 5.2), and to add the contact information SSCs to the IANA database (Section 5.3).

5.1 Establish Standing Committee

We recommend setting up a TLD-OPS Standing Committee (see Section 2.3) that governs the daily operations and further development of the TLD-OPS list and the TLD-OPS ecosystem.

We also recommend that the first Standing Committee fleshes out its responsibilities and way of working based on Section 2.3 and Chapter 3 of the CRI Final Report [3]. These responsibilities should explicitly include actively keeping the community up to date on the developments of the TLD-OPS list and its ecosystem. In terms of timing, we recommend setting up the TLD-OPS Standing Committee right after the SECIR WG finishes its work to ensure operational continuity.

We also advice to organize the Committee such that it is representative of the ccTLDs subscribed to the TLD-OPS list. This for instance means that its members should be subscribed SSCs, that the Committee contains representatives of all geographical regions (AF, AP, EUR, NA, LAC) as well as ccNSO and non-ccNSO members, and perhaps members of SSAC, IANA, and ICANN's SSR team.

We also recommend that the Standing Committee develops and implements a roadmap for the further development of the TLD-OPS ecosystem, procedures, and the underlying technical systems. Examples include the addition of encryption facilities to the TLD-OPS ecosystem based on a customized version of the OPS-Trust system, improvements of the validation process (e.g., based on nonces), and the addition of other types of stakeholders to the ecosystem (e.g., CERTs and gTLDs).

5.2 Further Grow Number of Subscribers

We advise that the first TLD-OPS Standing Committee focuses on growing the number of TLD-OPS subscribers and the actual use of the list until ICANN56 (June 2016) before starting any new WGs that aim to further develop the TLD-OPS technical components or the ecosystem around it.

At a later stage, we also recommend extending the TLD-OPS ecosystem with other types of players. This is important because in many the ccTLD community will probably also want to liaise with the CERT community, such as national CERTs, CERTs of ISPs and large enterprises. This was beyond the scope of the SECIR WG [9].

5.3 Add SSCs to IANA Database

For the longer term, we recommend adding the contact information of SSCs to the IANA database. This is a timely recommendation because IANA is currently exploring what new types of information the community would like to be included in the IANA database [12].

With a ccTLD's SSCs in the IANA database, IANA would become the TLD-OPS Validator (see Section 2.1) and the ccTLDs would become the Administrator of their own information. IANA would need to provide an additional service to ccTLDs to manage this type of information, which would have both a technical impact and an impact on the processes at ccTLDs. The TLD-OPS list would interface with the IANA database at a technical level and would become the mechanism to automatically distribute SSC contact information to subscribers so it would be available in SSCs' inboxes for offline situations.

We also recommend that the Standing Committee work with IANA to detail the compatibility of the SECIR contact model and that of IANA. For example, the SECIR WG assumed that the IANA Admin Contact is an employee of the ccTLD, but this is not necessarily true in the IANA contact model.

References

1. SECIR Homepage, http://ccnso.icann.org/workinggroups/secir.htm
2. "SECIR Working Group Update", ccNSO Members Day at ICANN52, Singapore, Feb 2015, http://singapore52.icann.org/en/schedule/tue-ccnso-members/presentation-secir-10feb15-en
3. Final Report ccNSO Contact Repository Implementation Working Group, June 2014, http://ccnso.icann.org/node/45566
4. Sandoche Balakrichenan, "Disturbance in the DNS", Tech Day, ICANN 51, Los Angeles, USA, Oct 2014, http://la51.icann.org/en/schedule/mon-tech/presentation-dafa888-dos-attack-13oct14-en.pdf
5. Mailman homepage, http://www.gnu.org/software/mailman/
6. TLD-OPS Homepage, http://ccnso.icann.org/resources/tld-ops-secure-communication.htm
7. OPS Trust homepage, https://portal.ops-trust.net/
8. "TLD-OPS Overview", version 1.2, March 2015, http://ccnso.icann.org/workinggroups/secir-tld-ops-overview-02mar15-en.pdf
9. SECIR WG Charter, http://ccnso.icann.org/workinggroups/charter-secir-21jul14-en.pdf
10. "ICANN's Security Stability Resiliency Team", ICANN50, London, June 2014, http://london50.icann.org/en/schedule/wed-ssr/presentation-ssr-25jun14-en
11. IDN ccTLD Fast Track String Evaluation Completion, https://www.icann.org/resources/pages/string-evaluation-completion-2014-02-19-en
12. Kim Davies, "IANA Update", ccNSO Members Day, ICANN52, Singapore, http://singapore52.icann.org/en/schedule/tue-ccnso-members/presentation-iana-10feb15-en
13. TLD-OPS leaflet, April 2015, http://ccnso.icann.org/workinggroups/ccnso-tld-ops-mailing-list-en.pdf

A Appendix: List of Non-subscribed ccTLDs

Table 7 shows the list of ccTLDs that received an invitation to join the TLD-OPS list, but that have not been able to subscribe yet. The list of ccTLDs that have joined the TLD-OPS list is available on the TLD-OPS homepage [6]. We divided ccTLDs into geographic regions based on https://www.countries-ofthe-world.com.

Table 7. ccTLDs not yet subscribed per region (June 17, 2015).

Region	ccTLDs	Country
Africa (AF)	1) .ac	Ascension Islands
	2) .ao	Angola
	3) .bj	Benin
	4) .cd	Congo, the Democratic Republic of the
	5) .cf	Central African Republic
	6) .cg	Congo, Republic of
	7) .ci	Cote d'Ivorie
	8) .cm	Cameroon
	9) .dz	Algeria
	10) .eg	Egypt
	11) .er	Eritrea
	12) .et	Ethiopia
	13) .ga	Gabon
	14) .gn	Guinea
	15) .gq	Equatorial Guinea
	16) .gw	Guinea-Bissau
	17) .lr	Liberia
	18) .ls	Lesotho
	19) .ml	Mali
	20) .mr	Mauritania
	21) .na	Namibia
	22) .ne	Niger
	23) .sd	Sudan
	24) .sl	Sierra Leone
	25) .so	Somalia
	26) .st	Sao Tome and Principe
	27) .sz	Swaziland
	28) .td	Chad
	28) .tg	Togo
	29) .zw	Zimbabwe
Asia-Pacific (AP)	1) .as	American Samoa
	2) .az	Azerbaijan
	3) .bd	Bangladesh
	4) .bn	Brunei Darussalam
	5) .bt	Bhutan

	6) .cc	Cocos (Keeling) Islands
	7) .ck	Cook Islands
	8) .cx	Christmas Islands
	9) .dj	Djibouti
	10) .fj	Fiji
	11) .gu	Guam
	12) .hm	Heard and McDonald Islands
	13) .in	India
	14) .io	British Indian Ocean Territory
	15) .iq	Iraq
	16) .ir	Iran
	17) .kg	Kyrgystan
	18) .ki	Kiribati
	19) .kp	Korea, Democratic People's Republic
	20) .kz	Kazakhstan
	21) .la	Laos
	22) .lb	Lebanon
	23) .ma	Morocco
	24) .mh	Marshall Islands
	25) .mm	Myanmar
	26) .mp	Northern Mariana Islands
	27) .mv	Maldives
	28) .nc	New Caledonia
	29) .nf	Norfolk Island
	30) .np	Nepal
	31) .nr	Nauru
	32) .om	Oman
	33) .pf	French Polynesia
	34) .pk	Pakistan
	35) .pw	Palau
	36) .tc	Turks and Caicos Islands
	37) .tj	Tajikistan
	38) .tk	Tokelau
	39) .tm	Turkmenistan
	40) .to	Tonga
	41) .tv	Tuvalu
	42) .vu	Vanuatu
	43) .ws	Samoa
	44) .ye	Yemen
Europe (EUR)	1) .ax	Åland Islands
	2) .ba	Bosnia and Herzegovina
	3) .eu	European Union
	3) .fo	Faroe Islands
	4) .gi	Gibraltar
	5) .md	Moldova

	6) .sm	San Marino
North America (NA)	1) .gl	Greenland
	2) .pr	Puerto Rico
Latin America and Caribbean (LAC)	1) .ag	Antigua and Barbuda
	2) .ai	Anguilla
	3) .bb	Barbados
	4) .bo	Bolivia
	5) .bs	Bahamas
	6) .bz	Belize
	7) .cr	Costa Rica
	8) .cu	Cuba
	9) .ec	Ecuador
	10) .gf	French Guiana
	11) .gp	Guadeloupe
	12) .gs	S. Georgia & the S. Sandwich Islands
	13) .gy	Guyana
	14) .ht	Haiti
	15) .hn	Honduras
	16) .jm	Jamaica
	17) .kn	Saint Kitts and Nevis
	18) .ky	Cayman Islands
	19) .mq	Martinique
	20) .ms	Montserrat
	21) .mx	Mexico
	22) .pa	Panama
	23) .pe	Peru
	24) .sr	Suriname
	25) .sv	El Salvador
	26) .sx	Sint Maarten
	27) .tc	Turks and Caicos Islands
	28) .tt	Trinidad and Tobago
	29) .vc	Saint Vincent and the Grenadines

B Appendix: Similar Initiatives at Regional Organizations

Table 8 shows an overview of similar initiatives at regional organizations, which we include here with their approval.

Table 8. Initiatives similar to TLD-OPS at regional organizations.

Attribute	ccNSO	CENTR*	APTLD**	AfTLD	LACTLD
Status	Operational	Development	Non-existent	Unkown	Operational
List name	TLD-OPS	TRUSTED	N/A		TEC
Members	ccTLD Security and Stability Contacts only, including non-ccNSO	CENTR members and associates	N/A		Technical staff from registries, no outsiders
Members appointed/authenticated by	ccTLD's IANA Admin Contact (max 3/ccTLD)	CEO or by proxy (max 3/CENTR member)	N/A		ccTLD manager or technical director
Members obtain contact info through	Automated emails, requests on list, mailman who command	Regular emails from CENTR Secretariat, separate CENTR-wide Who-Is-Who (centr.org/users)	N/A		LACTLD
Members share Incident info through	External channel (TLD-OPS list not recommended)	Emails on the list	N/A		Mailing list itself, but hardly used for that purpose
List administrator	ccNSO Secretariat	CENTR Secretariat	N/A		LACTLD Secretariat
Host	DNS-OARC	CENTR	N/A		NIC.BR
Software	mailman	Unkown	N/A		mailman
*Tentative info as the CENTR list is currently being setup **APTLD: they considered an incident response list in 2007, but there was no interest at the time					

C Appendix: SECIR Deliverables

Table 9 shows the deliverables of the SECIR WG, as defined in the WG charter [9]. With this final report, all deliverables are ready.

Table 9. SECIR deliverables.

No.	Title	Type	Status	Reference
D1	Operational SECIR Mailing List	Service	Ready	tld-ops@lists.dns-oarc.net
D2	SECIR List Membership Management	Document	Ready	[8]
D3	SECIR Instruction Manuals	Document	Ready	[8], [13]
D4	SECIR Final Report	Report	Ready	This document

D Appendix: SECIR Outreach Results

Table 10 shows the outreach result of the SECIR WG.

Table 10. SECIR outreach.

Title	Venue
TLD-OPS Status Update	ccNSO Members Day #1, ICANN53, Buenos Aires, June 2015
TLD-OPS Business Cards	ICANN53, Buenos Aires, June 2015
Join the TLD-OPS Mailing List	TLD-OPS leaflet, April 2015, http://ccnso.icann.org/workinggroups/ccnso-tld-ops-mailing-list-en.pdf
TLD-OPS Secure Communication Email List	TLD-OPS Homepage, http://ccnso.icann.org/resources/tld-ops-secure-communication.htm
SECIR WG: Status Update	Tech Day, ICANN52, Singapore, February 2015
SECIR WG: Status Update	ccNSO Members Day #1, ICANN52, Singapore, February 2015
SECIR WG: Status Update	ccNSO Members Day #1, ICANN51, Los Angeles, October 2014