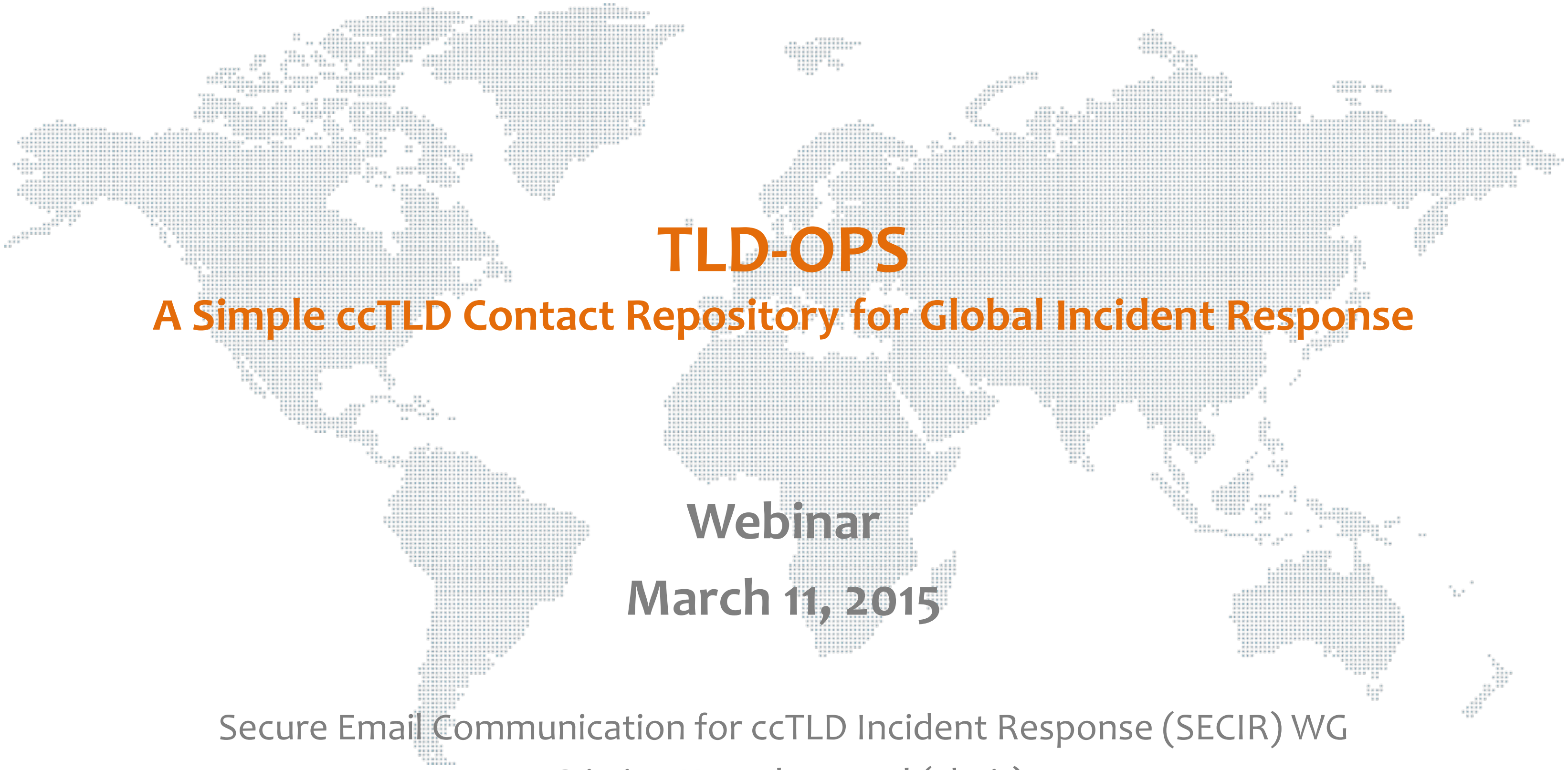


TLD-OPS

A Simple ccTLD Contact Repository for Global Incident Response

Webinar

March 11, 2015

Secure Email Communication for ccTLD Incident Response (SECIR) WG

Cristian Hesselman, .nl (chair)

TLD-OPS Mailing List

- ccTLD Contact Repository for global incident response
- Lookup of names, email addresses, telephone numbers
- May be used to exchange incident info, but not recommended
- Explicitly open to non-ccNSO members

Expected Impact

- Improved handling of incidents that require a coordinated response of ccTLDs at the global level

- Such as targeted attacks on or malfunctions of registration systems, the DNS, or the Internet at large

Why a Mailing List?

- Easy to use for everyone
- Globally accessible
- Near zero costs (CRI survey, Dec 2013)
- Maximizes chances of getting everyone on board

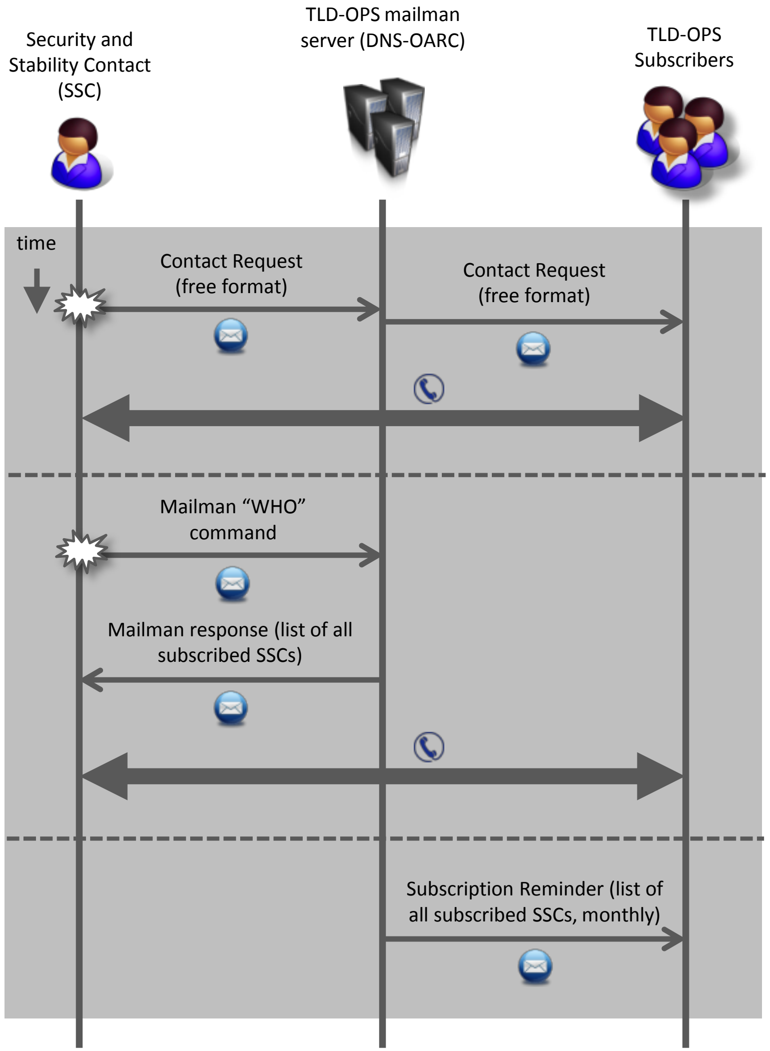
TLD-OPS Members

- Security and Stability Contacts (SSCs) only
- Responsible for overall security and stability of a ccTLD
- At most three SSCs per ccTLD on the TLD-OPS list
- On the list with personal info, not role-based
- List address: tld-ops@lists.dns-oarc.net

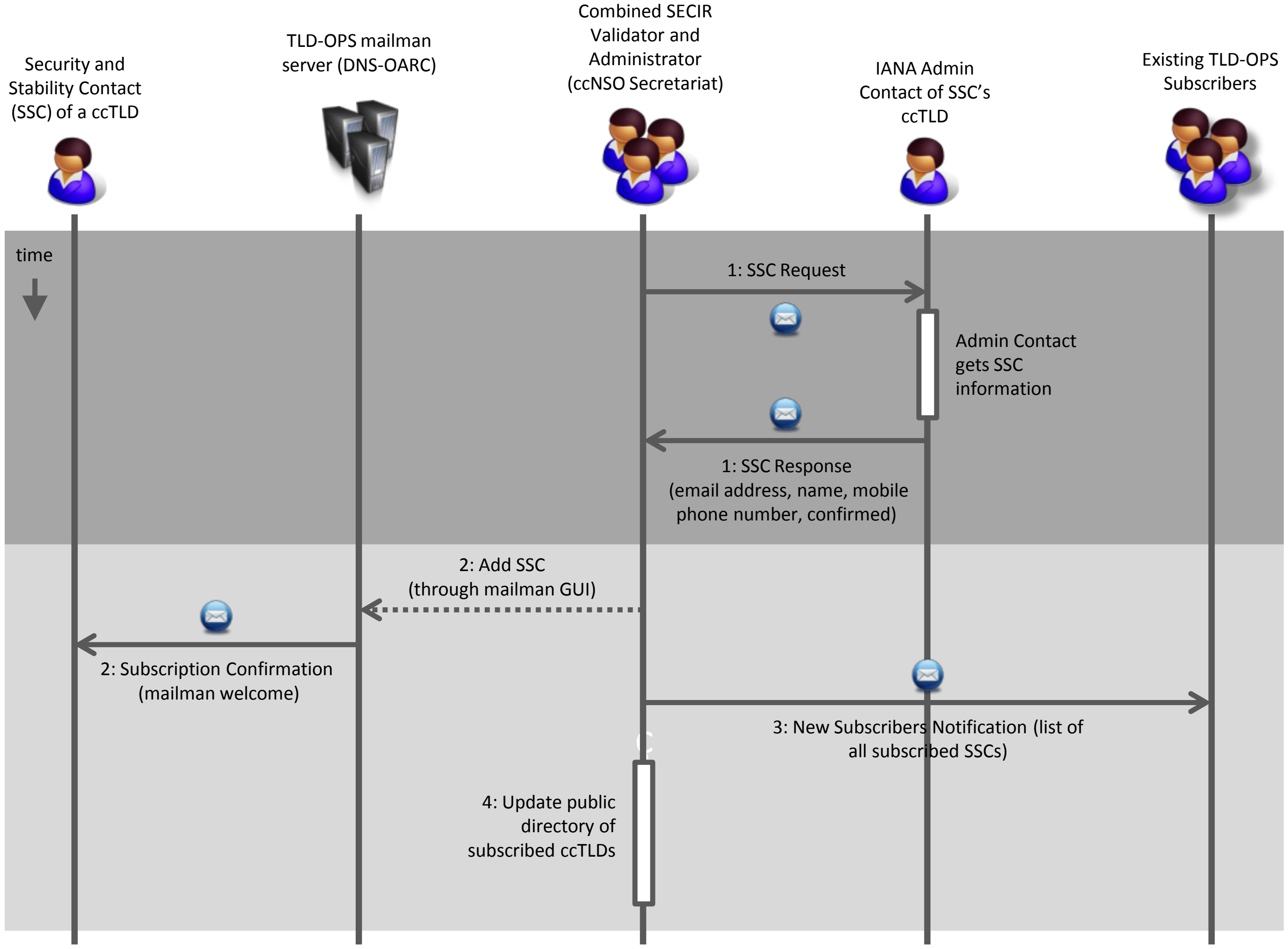
IANA Admin Contact

- Appoints/authenticates SSCs
- *Should preferably respond from Admin Inbox*
- *Or respond from personal address, CC’ing admin email address*
- ccNSO Secretariat invites ccTLDs through IANA Admin Contact

TLD-OPS Usage


Security and Stability Contact (SSC)
TLD-OPS mailman server (DNS-OARC)
TLD-OPS Subscribers
time
Contact Request (free format)
Contact Request (free format)
Mailman "WHO" command
Mailman response (list of all subscribed SSCs)
Subscription Reminder (list of all subscribed SSCs, monthly)

TLD-OPS Subscription Procedure



Security and Stability Contact (SSC) of a ccTLD
TLD-OPS mailman server (DNS-OARC)
Combined SECIR Validator and Administrator (ccNSO Secretariat)
IANA Admin Contact of SSC's ccTLD
Existing TLD-OPS Subscribers
time
1: SSC Request
Admin Contact gets SSC information
1: SSC Response (email address, name, mobile phone number, confirmed)
2: Add SSC (through mailman GUI)
2: Subscription Confirmation (mailman welcome)
3: New Subscribers Notification (list of all subscribed SSCs)
4: Update public directory of subscribed ccTLDs

Invitation Email ("SSC Request")

From: ccNSO Secretariat
To: ccTLD IANA Admin Contact
Subject: Invitation to join the TLD-OPS mailing list

Dear IANA Admin Contact,

We are sending you this email to invite your ccTLD to join the TLD-OPS mailing list.

The purpose of the TLD-OPS list is to enable ccTLD operators to easily and quickly contact each other, thus allowing them to better handle 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 who have been authenticated as such by their IANA Admin Contact. More details about the admission procedure are available at http://ccnso.icann.org/resources/tld-ops-secure-communication.htm

To subscribe your ccTLD to the TLD-OPS list, we kindly ask you to reply to this email within 5 working days and use the response template below to send us the contact information of the people who are responsible for your ccTLD's overall security and stability. Note that we currently admit at most three people per ccTLD to the TLD-OPS list.

IMPORTANT: Your reply should preferably come from the email address you have registered in the IANA database for your ccTLD's Administrative Contact. If this is not possible (e.g., because your IANA admin address is a forwarding address), then you MUST copy the IANA admin email address in your response.

The TLD-OPS list is an initiative of the ccNSO (country code Name Supporting Organization). It is however open to all ccTLDs and we therefore also encourage non-ccNSO members to sign up.

The TLD-OPS list is being maintained by the ccNSO Secretariat. The list server runs at DNS-OARC. More information is available at http://ccnso.icann.org/resources/tld-ops-secure-communication.htm.

Best regards,

ccNSO Secretariat

*** RESPONSE TEMPLATE ***

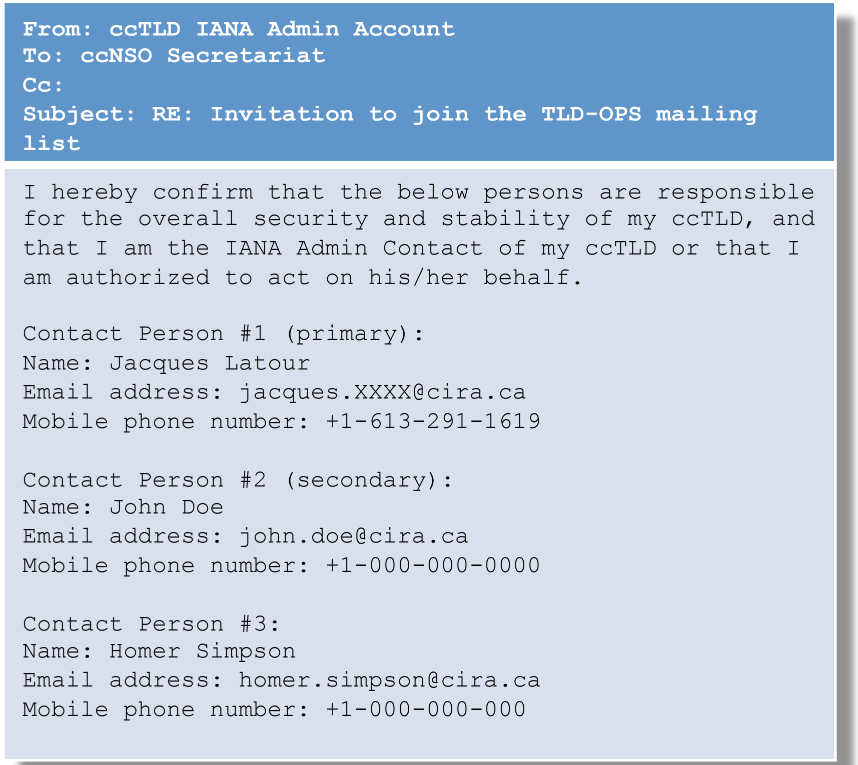
I hereby confirm that the below persons are responsible for the overall security and stability of my ccTLD, and that I am the IANA Admin Contact of my ccTLD or that I am authorized to act on his/her behalf.

Contact Person #1 (primary):
Name: <FirstName1> <LastName1>
Email address: <EmailAddress1>
Mobile phone number: +<country code> <number>

Contact Person #2 (secondary):
Name: <FirstName2> <LastName2>
Email address: <EmailAddress2>
Mobile phone number: +<country code> <number>

Contact Person #3:
Name: <FirstName3> <LastName3>
Email address: <EmailAddress3>
Mobile phone number: +<country code> <number>

Invitation Response Email ("SSC Response")



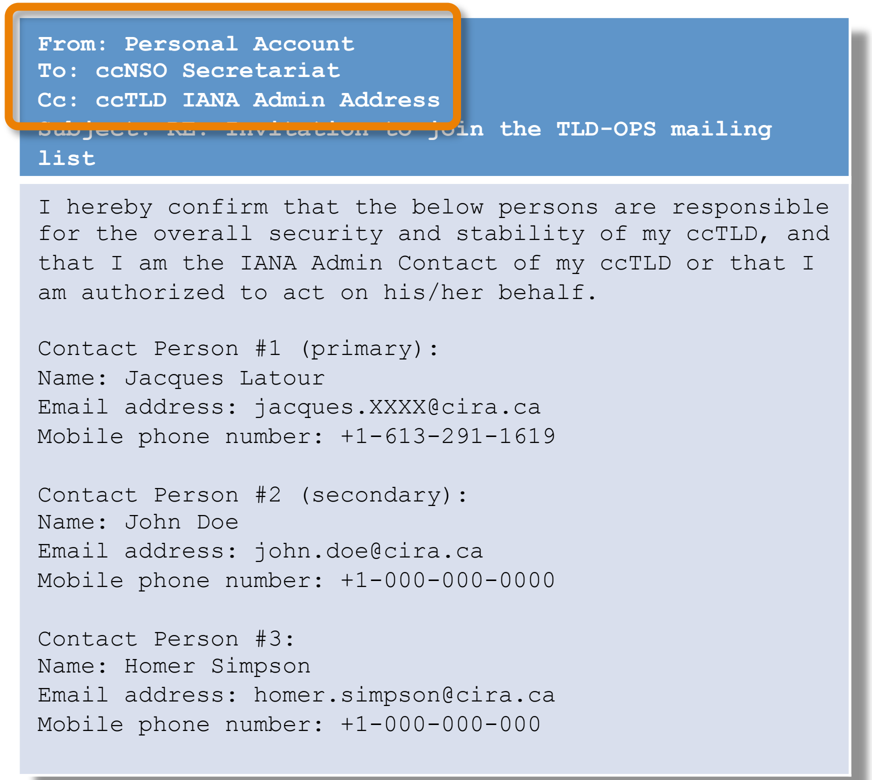
From: ccTLD IANA Admin Account
To: ccNSO Secretariat
Cc:
Subject: RE: Invitation to join the TLD-OPS mailing list

I hereby confirm that the below persons are responsible for the overall security and stability of my ccTLD, and that I am the IANA Admin Contact of my ccTLD or that I am authorized to act on his/her behalf.

Contact Person #1 (primary):
Name: Jacques Latour
Email address: jacques.XXXX@cira.ca
Mobile phone number: +1-613-291-1619

Contact Person #2 (secondary):
Name: John Doe
Email address: john.doe@cira.ca
Mobile phone number: +1-000-000-0000

Contact Person #3:
Name: Homer Simpson
Email address: homer.simpson@cira.ca
Mobile phone number: +1-000-000-000



From: Personal Account
To: ccNSO Secretariat
Cc: ccTLD IANA Admin Address
Subject: RE: Invitation to join the TLD-OPS mailing list

I hereby confirm that the below persons are responsible for the overall security and stability of my ccTLD, and that I am the IANA Admin Contact of my ccTLD or that I am authorized to act on his/her behalf.

Contact Person #1 (primary):
Name: Jacques Latour
Email address: jacques.XXXX@cira.ca
Mobile phone number: +1-613-291-1619

Contact Person #2 (secondary):
Name: John Doe
Email address: john.doe@cira.ca
Mobile phone number: +1-000-000-0000

Contact Person #3:
Name: Homer Simpson
Email address: homer.simpson@cira.ca
Mobile phone number: +1-000-000-000

Rules of Engagement (draft)

TLP Color*	TLD-OPS definition	Requesting Contact Information	Sharing of Actual Incident Information
WHITE: unlimited distribution	Info may be distributed freely, without restriction (equal to TLP definition).	N/A	SSCs explicitly flag message as WHITE.
GREEN: community-wide distribution	Info for use by subscribed SSCs and may be shared with larger incident response community.	N/A	SSCs explicitly flag message as GREEN.
AMBER: limited distribution	Info for use by all subscribed SSCs. No forwarding, no sharing of message content or sender identity (person or organization).	All messages exchanged on the list to obtain or share contact info. AMBER code is implicit.	SSCs explicitly flag message as AMBER. SSCs should carefully think about sending this type of information on the list as the list is unencrypted.
RED: for named recipients only	Info for use by a limited number of specific subscribed SSCs.	N/A	SSCs explicitly flag message as RED. SSCs should use a different communications channel and not use TLD-OPS as the list is unencrypted.

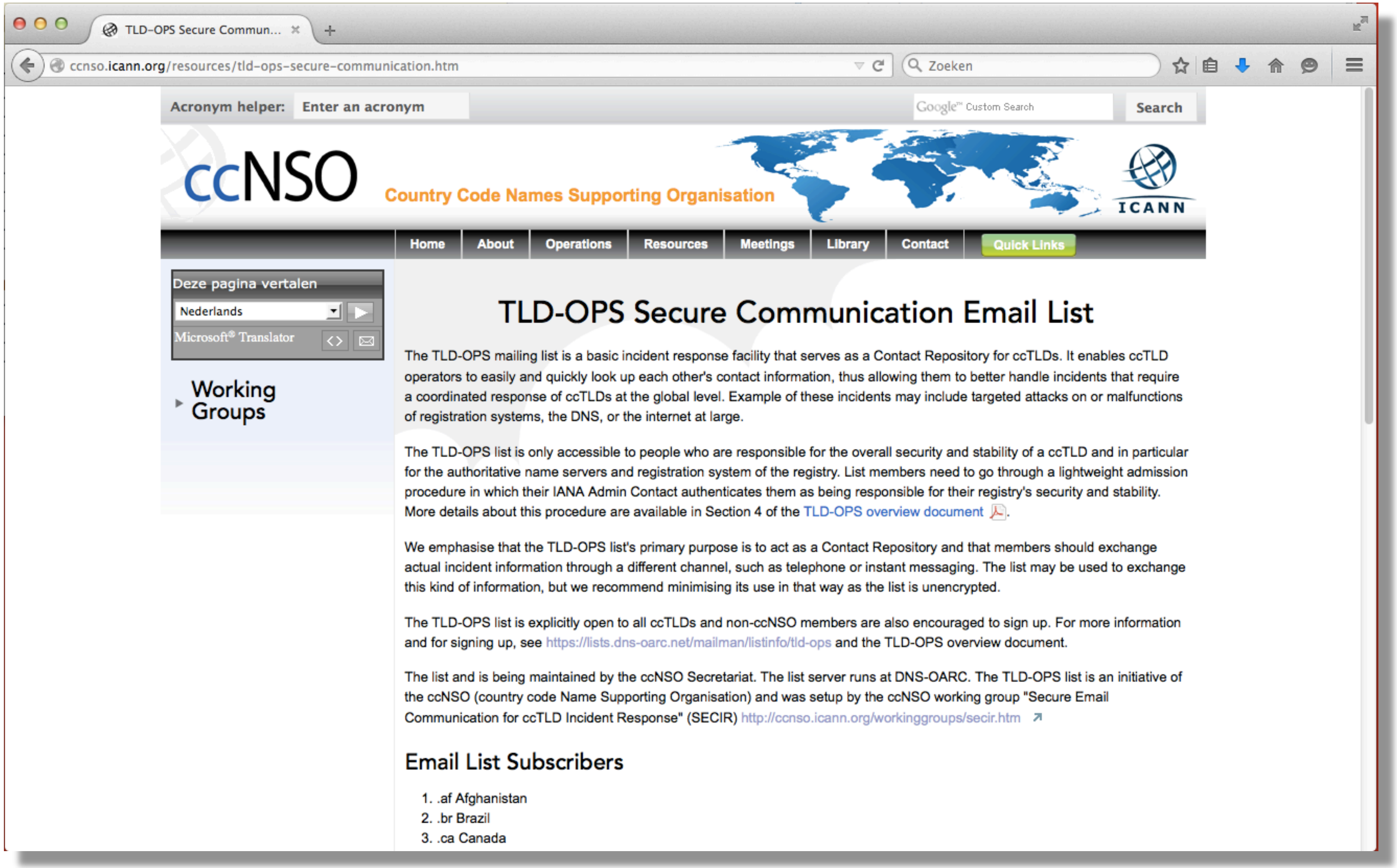
* Traffic Light Protocol: http://en.wikipedia.org/wiki/Traffic_Light_Protocol

Status and Next Steps

- 55 ccTLDs subscribed (Mar 11, 2015)
  - 107 SSCs
  - 3 IDNs

- Check your Admin Inbox!
  - ccNSO Secretariat will continue sending out invitations
  - Please follow instructions to ease the Secretariat’s work
  - Working in reverse alphabetical order

TLD-OPS Home



TLD-OPS Secure Communication Email List

The TLD-OPS mailing list is a basic incident response facility that serves as a Contact Repository for ccTLDs. It enables ccTLD operators to easily and quickly look up each other's contact information, thus allowing them to better handle incidents that require a coordinated response of ccTLDs at the global level. Example of these incidents may 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. List members need to go through a lightweight admission procedure in which their IANA Admin Contact authenticates them as being responsible for their registry's security and stability. More details about this procedure are available in Section 4 of the TLD-OPS overview document.

We emphasise that the TLD-OPS list's primary purpose is to act as a Contact Repository and that members should exchange actual incident information through a different channel, such as telephone or instant messaging. The list may be used to exchange this kind of information, but we recommend minimising its use in that way as the list is unencrypted.

The TLD-OPS list is explicitly open to all ccTLDs and non-ccNSO members are also encouraged to sign up. For more information and for signing up, see https://lists.dns-oarc.net/mailman/listinfo/tld-ops and the TLD-OPS overview document.

The list and is being maintained by the ccNSO Secretariat. The list server runs at DNS-OARC. The TLD-OPS list is an initiative of the ccNSO (country code Name Supporting Organisation) and was setup by the ccNSO working group "Secure Email Communication for ccTLD Incident Response" (SECIR) http://ccnso.icann.org/workinggroups/secir.htm

Email List Subscribers

1. .af Afghanistan
2. .br Brazil
3. .ca Canada

Q&A

SECIR WG Members
Frederico Neves, .br
Jacques Latour, .ca
Erwin Lansing, .dk
Cristian Hesselman, .nl (chair)
Geng-Da Tsai, .tw
Abibu Ntahigiye, .tz

ICANN Staff
Gabriella Schittek

TLD-OPS Home
http://ccnso.icann.org/resources/tld-ops-secure-communication.htm

SECIR Home
http://ccnso.icann.org/workinggroups/secir.htm

Cristian Hesselman
+31 6 25 07 87 33
cristian.hesselman@sidn.nl
@hesselma