ccNSO

ICANN

JOIN THE TLD-OPS MAILING 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 (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 explicitly open to both ccNSO members and non-ccNSO members. It is set up in such a way that every ccTLD will be able to join, thus maximizing the collective incident response capabilities of the ccTLD community.

HOW TO JOIN

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. To join the list, your IANA Admin Contact needs to send an email with the names, email addresses, and phone numbers of the security and stability contacts of your ccTLD to the ccNSO Secretariat. Please make sure that the email comes from the address you have registered in the IANA database for your ccTLD's Administrative Contact. If this is not possible, then you MUST copy the IANA admin email address in your email.

SUBSCRIPTION TEMPLATE

Please use the format below to subscribe your ccTLD to the TLD-OPS list. The template is also available from the TLD-OPS homepage for copying and pasting.

```
From: ccTLD IANA Admin Address
To: ccNSO Secretariat <ccnsosecretariat@icann.org>
Cc: ccTLD IANA Admin Address (if "From:" is not the IANA Admin Address)
Subject: Request to join the TLD-OPS mailing list


---

Dear ccNSO Secretariat,

I would like to subscribe the people below to the TLD-OPS list. I hereby
confirm that they 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.

Best regards,

IANA Admin Contact of <ccTLD>

== CONTACT INFORMATION ==

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>
```

ccNSO

PERSONAL TRUST

The TLD-OPS list is based on personal trust, which means that subscribers can only join with their personal email address and phone number. The underlying rationale is that a personal trust model will contribute to further increasing trust within the ccTLD community, for instance because people start recognizing each others names. The consequence is that role-based email addresses are not allowed on the list.

The vouching model that is typically used in the incident response community 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 this model.

RULES OF ENGAGEMENT

All information shared on the list to obtain the contact information of a ccTLD is confidential and must not be shared outside the TLD-OPS group. Subscribers should exchange actual incident information through a different channel, such a telephone call or secure instant messaging. If you nonetheless decide to exchange such type of information through the TLD-OPS list, then please use the color codes and guidelines in the table below.

TLP COLOR*	TLD-OPS DEFINITION**	SHARING OF INCIDENT INFORMATION
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

LIST ADDRESS: tld-ops@lists.dns-oarc.net

MORE INFORMATION

Please visit the TLD-OPS homepage at http://ccnso.icann.org/resources/tld-ops-secure-communication.htm for additional information and for the list of ccTLDs who have already joined TLD-OPS.

The TLD-OPS list was set up by the working group "Secure Email Communication for ccTLD Incident Response" (http://ccnso.icann.org/workinggroups/secir.htm), which is part of the country code Name Supporting Organization (http://ccnso.icann.org). The TLD-OPS list is being maintained by the ccNSO Secretariat. The list server runs at DNS-OARC.

This leaflet is for distribution within the ccTLD community only. April 19, 2015