prop-125: Implementation Update

George Odagi

Internet Resource Analyst / Policy Support

prop-125: Validation of “abuse-mailbox” and other IRT emails

Authors

Jordi Palet Martinez and Aftab Siddiqui

Status

Incident Response Team (IRT) objects in APNIC Whois

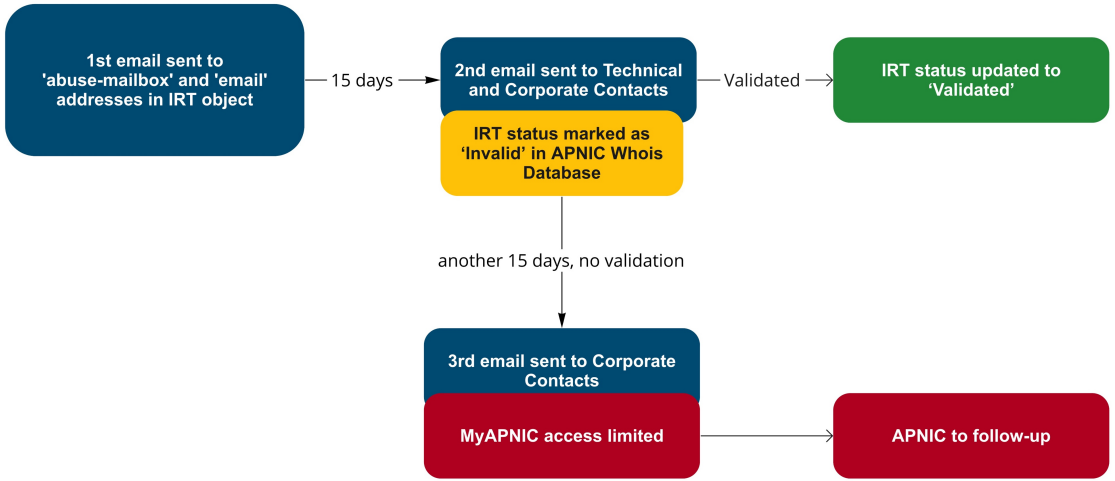
- Object in the APNIC whois containing contact information of network administrators responsible for receiving network abuse reports
- As a result of prop-079 at APNIC 29, APNIC implemented mandatory IRT references on 8 November 2010
- Aimed to provide a more accurate and efficient way for abuse reports to reach the correct contact

Incident Response Team (IRT) object

```
irt:            IRT-APNIC-AP
address:        Brisbane, Australia
e-mail:         helpdesk@apnic.net
abuse-mailbox:  helpdesk@apnic.net
admin-c:        HM20-AP
tech-c:         NO4-AP
auth:           # Filtered
remarks:        APNIC is a Regional Internet Registry.
remarks:        We do not operate the referring network and
remarks:        are unable to investigate complaints of network abuse.
remarks:        For information about IRT, see www.apnic.net/irt
remarks:        helpdesk@apnic.net was validated on 2020-02-03
mnt-by:         APNIC-HM
last-modified:  2020-02-03T02:04:33Z
source:         APNIC
```

Implementation details

- Implemented from 1 July 2019
  - All email addresses in IRT objects
  - Validation process by a human
- Frequency
  - Every time the object is updated
  - Validated at least every six months
- Demonstrate abuse mailbox
  - Is monitored by a human
  - Is responsive to legitimate reports
- Failure to validate
  - After 15 days object is marked invalid in whois
  - After 30 days restricted access to MyAPNIC



Step 1: Validation email

Dear Incident Response Team contact,

We are contacting you because you are listed as an Incident Response Team (IRT) contact in the APNIC Whois Database for the IRT(s) below:

IRT object name → IRT-APNIC-AP1

You can use the APNIC whois search to query IRTs:

https://www.apnic.net/whois

Important: validate IRT contact

As of 30 June 2019, APNIC policy requires all IRT contact(s) to be validated every 6 months, and the IRT contact to demonstrate the abuse mailbox is monitored and responsive to legitimate abuse reports. Failure to validate within 15 days will result in the IRT whois object being marked as 'Invalid' and further action by APNIC to follow-up.

To validate your email address, please click on the link below:

Unique validation link → https://validation.apnic.net/aa911de4-e3c6-4901-80d8-059a4596032a/confirm

If you have any questions, please refer to the IRT guide below:

https://www.apnic.net/irt

Step 2: Confirm validation

IRT Email Validation

APNIC Policy requires all contacts registered in IRT (Incident Response Team) whois objects to be validated every six months.

To complete this process, please click the Validate IRT button below and indicate that you understand the policy requirements to regularly monitor your abuse mailbox and promptly respond to abuse reports to resolve any complaints.

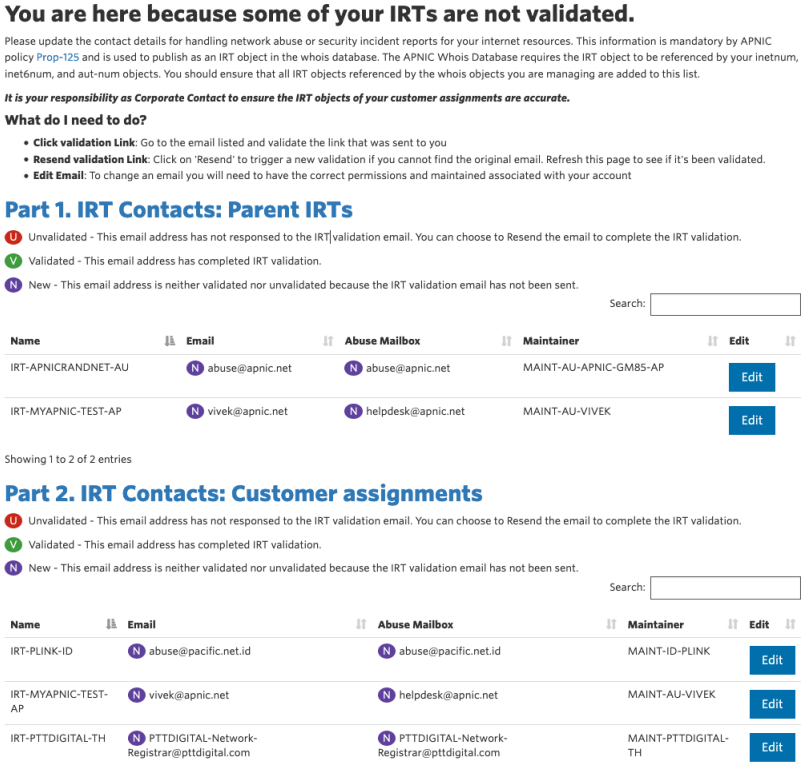
☑ I have read and understand APNIC Policy 5.3.4. Registering Contact Persons

Validate IRT

protected by reCAPTCHA
Privacy - Terms

If you prefer to use our phone validation service contact APNIC Helpdesk on +61 7 3858 3188.

Step 3: Review in MyAPNIC



You are here because some of your IRTs are not validated.

Please update the contact details for handling network abuse or security incident reports for your internet resources. This information is mandatory by APNIC policy Prop-125 and is used to publish as an IRT object in the whois database. The APNIC Whois Database requires the IRT object to be referenced by your inetnum, inet6num, and aut-num objects. You should ensure that all IRT objects referenced by the whois objects you are managing are added to this list.

It is your responsibility as Corporate Contact to ensure the IRT objects of your customer assignments are accurate.

What do I need to do?

- **Click validation Link**: Go to the email listed and validate the link that was sent to you
- **Resend validation Link**: Click on 'Resend' to trigger a new validation if you cannot find the original email. Refresh this page to see if it's been validated.
- **Edit Email**: To change an email you will need to have the correct permissions and maintained associated with your account

Part 1. IRT Contacts: Parent IRTs

U Unvalidated - This email address has not responsed to the IRT validation email. You can choose to Resend the email to complete the IRT validation.

V Validated - This email address has completed IRT validation.

N New - This email address is neither validated nor unvalidated because the IRT validation email has not been sent.

Search:

Name	Email	Abuse Mailbox	Maintainer	Edit
IRT-APNICRANDNET-AU	N abuse@apnic.net	N abuse@apnic.net	MAINT-AU-APNIC-GM85-AP	Edit
IRT-MYAPNIC-TEST-AP	N vivek@apnic.net	N helpdesk@apnic.net	MAINT-AU-VIVEK	Edit

Showing 1 to 2 of 2 entries

Part 2. IRT Contacts: Customer assignments

U Unvalidated - This email address has not responsed to the IRT validation email. You can choose to Resend the email to complete the IRT validation.

V Validated - This email address has completed IRT validation.

N New - This email address is neither validated nor unvalidated because the IRT validation email has not been sent.

Search:

Name	Email	Abuse Mailbox	Maintainer	Edit
IRT-PLINK-ID	N abuse@pacific.net.id	N abuse@pacific.net.id	MAINT-ID-PLINK	Edit
IRT-MYAPNIC-TEST-AP	N vivek@apnic.net	N helpdesk@apnic.net	MAINT-AU-VIVEK	Edit
IRT-PTTDIGITAL-TH	N PTTDIGITAL-Network-Registrar@pttdigital.com	N PTTDIGITAL-Network-Registrar@pttdigital.com	MAINT-PTTDIGITAL-TH	Edit

Implementation status

Phase One

- Includes validation of IRTs associated with parent resource records
- Created new escalation mailbox (escalation-abuse@apnic.net)

Phase Two

- Includes IRTs associated with customer assignments
- Resolved some issues encountered during phase one

Some stats

As of the last 6 months

- 15836 IRTs referenced in resources
- 9623 email validation requests issued
- 5995 email validation requests confirmed
- 62.3% validation rate

Road blocks

- Software bugs
  - Errors with updating IRT email addresses
  - Whois remarks not being updated
  - Validation status not updating in MyAPNIC
- UX/UI considerations
  - Difficult to navigate
  - Process is long and confusing

Final phase

- MyAPNIC restriction reinstated
- Add ‘abuse-c’ attribute to Whois records
- Resolve any other issues encountered
- Report back to community at APNIC 50

Feedback from members

University/CERT:

'These emails are not reports of abuse. They are a form of spam and waste resources that could be devoted to legitimate complaints to the abuse address.'

Feedback from members (cont'd)

Government department:

'This is not a good policy. We are a government department and are encouraged not to click on links containing potential phishing tactics.'

'We have multiple team members who are monitoring and would under real world situations, respond to a potential abuse situation (we have done so in the past). We deal with real people, not email links.'

Feedback from members (cont'd)

Large service provider:

'This is a distribution group that goes to a team of over 100 people and this list is changing. They have processes in place for intelligently handling emails and this is outside of their norm.

They do not have to do this for any other RIR. For all of the other RIR's, as the owner, I can go in and validate through the portal. I do not need to return or click on the link through email.'

Considerations

- Do you feel this policy should be amended?
- Is it too harsh to restrict MyAPNIC access after 30 days?
- Should the validation process occur every 6 or 12 months?

Questions or comments?


25 YEARS
2020
APRICOT
APNIC 49
MELBOURNE
AUSTRALIA
12 – 21 February 2020
#apricot2020