

Abuse Contact Policy Update

AFPUB-2018-GEN-001-DRAFT07



@JordiPalet

(jordi.palet@theipv6company.com)

Summary of the problem (1)

- The current policy **doesn't imply the obligation** to register an abuse contact and specifies a format for personal communication and for “automatic reporting”, which compared to other RIRs becomes confusing, as a single email will be more efficient, as at the end, reports get copied to both emails.
- As a result, **some LIRs may not have this contact information registered and up to date** for their resources. In fact, there are even cases of LIRs that use a non-existent mailbox or one that is not actively monitored.
- In practice, **this contact becomes ineffective** to report abuses and generally gives rise to security issues and costs for the victims. This is also contradictory with RSA, that states that information in databases must be accurate. This policy ensures that this can be automatically and periodically verified by AFRINIC, without entering in the operational details of how doing it. In fact there is an AFRINIC activity (<https://afrinic.net/stats/contact-update>) that aims for the verification of the contacts, however it has only reported for 2017. Again, this proposal, ensures that this activity is done in an automated fashion (as much as possible), saving cost to the membership and the community.

Summary of the problem (2)

- This proposal aims to solve this problem and ensure the existence of a proper abuse-c contact and the process for its utilization, which is more uniform across all the RIRs, in order to facilitate cross-region abuse reporting.
- Existing policy references to a **“Best Practice Paper”, which is not deemed as mandatory** and in fact, **is not being used by the community**. This proposal doesn't change the scope of that document, and in fact, a link between the few existing IRT objects and the new one, should be automatically established.
- At this way, AfriNIC abuse contact will be in line with other RIRs. APNIC, for example, is now using the IRT, but since an equivalent proposal has been accepted, an automated “link” (alias or pointer) to the pre-existing IRT will be created, so abuse-c and abuse-mailbox prevail.

Summary of the problem (3)

- There is no need to delete the other optional data today included in the IRT, it is an operational AFRINIC decision how to handle the transition. This policy just ensures that abuse-c and abuse-mailbox are available and verified periodically.

Addressing the problem

- The Internet community is based on **collaboration**. However, in many cases this is not enough and we all need to be able to contact those LIRs that may be experiencing a problem in their networks and are unaware of the situation.
- This proposal creates a new section in the Policy Manual to solve this problem by means of a simple, **periodic verification**, and establishes the basic rules for performing such verification and thus avoids unnecessary costs to third parties that need to contact the persons responsible for solving the abuses of a specific network.
- The proposal guarantees that the cost of processing the abuse falls on the LIR whose client is causing the abuse (and from whom they receive financial compensation for the service), instead of falling on the victim, as would be the case if they had to resort to the courts, thus avoiding costs (lawyers, solicitors, etc.) and saving time for both parties.
- For this, the **abuse-c attribute becomes mandatory** in the "aut-num", "inetnum" and "inet6num" objects, as well as in any others that may be used in the future. This attribute is an abuse contact, which must contain at least the "abuse-mailbox" attribute.
- The proposal is expected to be implemented in 90 days, to be confirmed by AFRINIC, a reasonable time frame to allow both the staff to develop the tool and the members to update their abuse-c contacts.

Proposed Changes (1)

8.1 Introduction

This policy specifies a dedicated object that shall be used as the preferred place to publish abuse public contact information within the AFRINIC service region.

The mentioned object can be referenced in the inetnum, inet6num and aut-num objects in the AFRINIC whois Database. It provides a more accurate and efficient way for abuse reports to reach the correct network contact

8.1 Introduction

This policy specifies a mandatory attribute (abuse-c) that must be used to publish abuse public contact information within the AFRINIC service region.

The mentioned attribute must be referenced in the inetnum, inet6num and aut-num objects in the AFRINIC whois Database. It provides a more accurate and efficient way for abuse reports to reach the correct contact..

Proposed Changes (2)

8.2 Policy details

(all replaced)

8.2 Description of “abuse-c” and “abuse-mailbox”

Resources allocated/assigned by AFRINIC must include a mandatory "abuse-c" contact attribute (abuse contact), pointing to a person or role, with at least one valid, monitored and actively managed email inbox (abuse-mailbox) intended for receiving reports regarding abusive behavior, security issues, and the like.

The "abuse-mailbox" attribute must be available in an unrestricted way via whois, APIs and future techniques.

Considering the hierarchical nature of IP address objects, child objects of those directly distributed by AFRINIC may be covered by parent objects or they may have their own "abuse-c" attribute.

Following usual practices, other "e-mail" attributes may be included for other purposes.

Proposed Changes (3)

8.3 Advantages and disadvantages of the policy

(all replaced)

8.3 About the "abuse-mailbox"

Emails sent to "abuse-mailbox":

- Require intervention by the recipient.
- Must not require the reporter to complete a form.
- Must guarantee that abuse reports and related logs, examples, or email headers are received.

Proposed Changes (4)

8.4 Objectives of "abuse-c"/"abuse-mailbox" validation

The procedure, which will be developed by AFRINIC, must meet the following objectives:

1. A simple process that guarantees the abuse contact is able to fulfil its intended purpose.
2. Confirms that the resource holder:
 - has read the procedure and the policy
 - regularly monitor the abuse-mailbox
 - measures are taken
 - abuse reports receive a response.
3. Initial validation period of no longer than 15 days.
4. If validation fails, escalate to other LIR contacts and set a new validation period not to exceed 15 days.

8.5 Validation of "abuse-c"/"abuse-mailbox"

AFRINIC will validate compliance with the items above, both when the "abuse-c" and/or "abuse-mailbox" attributes are created or updated, as well as periodically, not less than once every 6 months, and whenever AFRINIC sees fit.

Proposed Changes (5)

8.6 Escalation to AFRINIC

Fraudulent behavior (for example, an "abuse-mailbox" that only replies to AFRINIC's emails, or to messages with a specific subject or content), or failure to comply with the remaining aspects of this policy (incorrect or lack of response to cases of abuse) can be reported to AFRINIC for a re-validation (as per section 8.5 above).

8.7 Slow-start and progress follow-up

The initial/escalation periods and the validation periodicity set by this policy can be amended yearly by AFRINIC, considering internal procedures, staffing needs and actual data, considering both, a slow-start and follow-up of the accuracy of the data. The reasons for the amendments shall be properly communicated to the community.

Additional Information (1)

If this proposal reach consensus, to comply with it, AFRINIC must rename mnt-IRT to abuse-c. It is an operational AFRINIC decision if an alias (pointer, duplicated attribute, or any other alternative) to mnt-IRT is kept and for how much time (transition period), in order to facilitate the search in whois for the same information, regardless if looking for abuse-c or mnt-IRT. It is an operational AFRINIC decision to keep and for how much time, the IRT or delete it, as well as the rest of the actual information in the IRT. AFRINIC will also decide how to better update the actual guidelines (<https://www.afrinic.net/library/membership765-abuse-policy-bcp>) or if they aren't longer needed. This is done in order to assimilate the IRT to the majority of the RIRs where it is abuse-c.

Additional Information (2)

As a matter of clarification, the “initial” and “escalation” validation periods may be modified by AFRINIC, if deemed appropriate, provided it informs the community of its motivation for doing so. For example, in the implementation phase, the periods could be extended, and adjusted as a higher percentage of contacts become accurate.

Similarly, the frequency of the periodic validation can be modified if AFRINIC deems this appropriate and informs the community of its reasons for doing so.

For example, a single validation might be done in the first year to facilitate adherence to the policy. The number of annual validations could increase over time, perhaps becoming quarterly, with the aim of improving the quality of the contacts.

Additional Information (3)

This will facilitate AFRINIC for a “slow-start” to implement the policy and ensure that no additional staff is required in the initial implementation phases, as depending on the rate of failed contacts, they may need more time for the first passes thru all the membership. For example, could be expected that the first pass takes 12-24 months, and be done by different types of members (LIRs/end-users/others), with a batch each month or even holding the next batch in case of a very high failure rate, etc.

As in all the other policies, this one doesn't set specific different conditions for legacy holders. This is a generic AFRINIC issue that should be tackled in a uniform way for all the policy manual.

Similarly, the policy doesn't state the consequences of lack of compliance, as this is generically stated in the RSA.

Additional Information (4)

The policy doesn't define what is abuse, because that definition doesn't fall in any way in the actions from the AFRINIC perspective. Each Internet participant shall define what is an abuse for them, and if others don't respect that, they can use the abuse-c to contact them and in case of inaction to resolve the case, they should escalate the matter according to their own internal procedures, which in some cases, may also depend on their local regulations. All that is outside the scope of AFRINIC.

There is no additional GDPR impact by this policy, as this is already covered by all the existing AFRINIC regulations on that matter.

This proposal doesn't enforce any implementation timing, which is left to the operational practices, priorities and staffing needs of AFRINIC.

References

- An equivalent proposal has been accepted in APNIC and LACNIC, **both already implemented**.
 - <https://www.apnic.net/community/policy/proposals/prop-125>
 - <https://politiclas.lacnic.net/politiclas/detail/id/LAC-2018-5/language/en>
- A new version is being worked out for RIPE and ARIN.

Responses to Impact Analysis

- All looks like 100% clear and nothing against this proposal.