*Staff Note: The version of ARIN-prop-266 below represents the version considered and rejected due to scope by the Advisory Council during their 10 April 2019 meeting.*

**ARIN-prop-266: BGP Hijacking is an ARIN Policy Violation**

**Proposal Originator:** Carlos Friaças, Jordi Palet Martinez

**Problem Statement:**

This proposal aims to clarify that BGP hijacking is not accepted as normal practice within ARIN's service region, primarily because it negates the core purpose of running a (Regional Internet) Registry. The proposal is not concerned with simple operational mistakes – it is intended to address deliberate BGP hijacking events.

BGP hijacking is not acceptable behavior. A "BGP Hijack" is defined by announcing a prefix to another network without the resource holder's consent.

There must be consequences for hijacking for members or individuals/organizations that have a service agreement (either directly or indirectly) with ARIN. This proposal aims to clarify that an intentional hijack is indeed a policy violation.

A. Arguments Supporting the Proposal

- BGP hijacking completely negates the purpose of a (Regional Internet) Registry.
- This community needs to explicitly express that BGP hijacking violates ARIN policies.
- If nothing changes in this field, the reputation of the ARIN service region will continue to be affected from a cybersecurity perspective due to BGP hijacking events.

B. Arguments Opposing the Proposal

- Neither the ARIN community or ARIN itself are the "Routing Police".
- Mitigation/counter-argument: Nobody will try to dictate to anyone how their routing policy should be at any given moment. However, ARIN needs to be able to choose not to enter into (or maintain) a contractual relationship with people/companies that are performing BGP hijacks. There are already enough sources of historic and almost real-time routing data which function as a worldwide observatory. From these sources it is possible to accurately evaluate who is performing BGP Hijacks and harming (or trying to harm) third party networks by doing so. The external experts are mere evaluators, who can use available sets of routing data to determine whether BGP hijacking events have taken place, and whether were intentional.

**Policy Statement:**

**Proposed Text 1.0 Introduction**

BGP hijacks happen on an almost daily basis. Hijacks can be on a global scale (propagated to all networks) or restricted (only one or some networks). Through this document, the ARIN community clarifies that BGP hijacking is not an acceptable practice.

**2.0 BGP Hijacking is a Policy Violation**

A hijack is understood to be the announcement of routes through BGP to third parties without the consent of the resource holder. This is considered to be a violation of ARIN policy.

The location of the resource holder or hijacker in such cases is irrelevant. A hijack constitutes a policy violation even if both parties are located outside of the ARIN service region. The announcement of unallocated address space or autonomous system numbers to third parties is also considered a policy violation and is evaluated according to the same parameters.

**3.0 Scope: Accidental vs. Deliberate**

A distinction can be made between accidental or deliberate hijacks from available routing datasets, looking at parameters such as duration, recurrence, possible goals, and the size of hijacked blocks. Other parameters may also be considered in the future.

**4.0 Lines of Action**

ARIN is not able to monitor the occurrence of BGP hijacks or assess whether they are policy violations. It must therefore rely on external parties, both to report hijacks and determine whether they are deliberate.

Reports sent to ARIN need to include a minimum set of details, such as: “Networks Affected”, “Offender ASN”, “Hijacked Prefixes” and “Timespan” (this is not a definitive list and other details may also be required).

The ARIN will provide a public web-based form (or equivalent alternatives) to submit these reports, which will be made publicly available, so third parties could add information relevant to the case avoiding duplicated reports. The tool will have a section in case of sensible information that must not be published.

As soon as the involved parties are identified, they will be notified, so they can provide relevant information and mitigate the hijack, avoiding further damages and possibly false claims. The experts will only consider those cases which persist or had been reported as latest as six months since they ceased.

ARIN will select a pool of worldwide experts who can assess whether reported BGP hijacks constitute policy violations. Experts from this pool will provide a judgement regarding each reported case, no later than four weeks from the moment the report was received. The direct upstreams of the suspected hijacker, which facilitate the hijack through their networks, may receive a warning the first time. Nevertheless, in successive occasions they could be considered by the experts, if intentional cases are reproduced, as an involved party.

The expert's investigation, will be able to value relationships between LIRs/end users, of the same business groups. Accidental cases or those that can't be clearly classified as intentional, will receive a warning, which may be considered if repeated.

Any cases in which the alleged hijacker can demonstrate that his infrastructure was improperly manipulated by third parties (for example, compromised routers) can't be considered intentional.

**5.0 Expert's Pool**

The selection procedure of the expert's pool should be open and managed by ARIN, possibly in collaboration with other RIRs.

1. A call will be made, every two years, to the global community including the requirements of experience and knowledge. Additional calls will be made if it is needed to expand the group of experts.
2. The same number of experts must participate in each case and phase (initial and appeal if any), to avoid discrimination between cases. It should be defined when implementing the process.
3. The minimum number of experts per case and phase will be three. If a larger number is necessary, it must be odd, and the community will be informed of the reasons for the change.
4. The expert's must sign a document that confirms their impartiality and, therefore, that have no direct or indirect relationship with the involved parties, before accepting each case.
5. The cases in progress must be completed by the experts initially assigned, even if they are replaced in the biannual selection process. Only in case of justified cause and communicated to the community, one expert may be replaced by another.

**6.0 Procedure**

The procedure must incorporate, at least, the following steps:

1. ARIN will verify that the report contains sufficient information before assigning it to the group of experts.
2. The assigned experts will verify the reported information regarding historical BGP data.

3. The experts will exclude those cases that are clearly accidental, although they must indicate this in their report, so that ARIN transmits it to the suspected hijacker to avoid its repetition.
4. If the event is ruled to be intentional, they will write a report with their conclusions, or with the confirmation or not of the same, if it is the appeal phase.
5. ARIN staff can't be part of the expert's group, however they can provide assistance.
6. Neither ARIN nor the claimant(s) can appeal the decision of the experts. 7.0 Retroactivity Only hijacking events that occur after this policy has been implemented are eligible to be considered.

**8.0 Possible Objections**

A report containing an expert judgement on the case will be sent to the suspected hijacker. This party will then have a maximum of four weeks to object to any conclusions contained in the report. Any objections are then assessed and ruled as admissible/non-admissible by the experts, during a maximum two-weeks review period. Following this, the report is finalized and published.

**9.0 Appeals**

Following the publication of the final expert's report, the suspected hijacker has a maximum of two weeks in which they can file an appeal. If an appeal is filed, an alternative set of experts will review this for a maximum of four weeks. The results of this review are final and cannot be further appealed.

**10.0 Ratification**

Once the report has been published, any policy violation will be ratified by ARIN Board of Trustees. Otherwise, the complaint/report will be archived. The ratification will be delayed in case of an appeal, until the second expert's group has published their review.

**11.0 Transition Period**

As soon as the policy implementation is completed, a transition period of 6 months will be established, so that organizations that announce unassigned address space or autonomous systems numbers, due to operational errors or other non-malicious reasons, receive only a warning.

**Timetable for Implementation**: Immediate, to be confirmed by ARIN

**Anything Else:**

Situation in other regions: The policy has already been submitted to RIPE and LACNIC, and we are working in order to submit ASAP to APNIC and AFRINIC.