Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	**)**	
	)	PS Docket No. 22-90,
Secure Internet Routing	**)**	FCC 22-18; FRS 75229
	)	

Response of
The American Registry for Internet Numbers, Ltd.

April 8, 2022

Attn: Ms. Marlene H. Dortch,
Secretary, Office of the Secretary, FCC

The American Registry for Internet Numbers, Ltd. (ARIN) respectfully submits the following comments and responses to the Federal Communications Commission (the "Commission") Request for Comments published in the Federal Register, Vol. 87, No. 48 of 11 March 2022.

Introduction

ARIN recognizes the Commission's attention on the important topic of secure Internet routing. As one of five Regional Internet Registries (RIRs) that administer Internet number resources globally (and the RIR which handles the United States, Canada, and many islands of the Caribbean[1]), ARIN wishes to make the Commission aware of several items relevant to this subject.

1) One of the services provided by ARIN is its Resource Public Key Infrastructure (RPKI) service. RPKI is an opt-in service that aids in securing Internet routing that uses cryptographically verifiable statements to ensure that representations about Internet number resources are certifiably linked to the stated holder of the rights to said resources. At present, the RPKI service is stable, technically sound, and ready for production use.

2) ARIN's RPKI service allows organizations with Internet number resources and a Registration Services Agreement (RSA) with ARIN to obtain a resource certificate which in turn allows them to make authoritative, signed statements about Internet number resource as well as which autonomous systems are authorized to originate the prefix into the routing table (BGP). These statements are called Route Origin Authorizations (ROAs). Organizations globally may utilize the published ROAs to make more informed decisions about the validity of routing information that they receive.

3) ARIN has deployed and invested significant resources in its RPKI service and believes that it is suitable for improving security of Internet routing. ARIN calls to the attention of the

---

[1] American Registry for Internet Numbers, "Our Region", https://www.arin.net/about/welcome/region/, retrieved 25 March 2022

Commission several significant considerations regarding ARIN's deployment of RPKI services that are worth noting –

    a. While the RPKI service is intended to enhance routing security, it also is a goal in the deployment of RPKI to not make the Internet routing system more brittle. To that end, currently accepted best practices for validation of routing information via RPKI require that network operators continue to route as they do today under circumstances where route validity cannot be determined[2]. Adherence to this best practice avoids an inappropriate dependency on RPKI such that an issue with the RPKI service would result in significant detrimental effect to routing. ARIN therefore conducts periodic testing and scheduled outages to help ensure users of RPKI have configured their networks, and their use of RPKI, without inappropriate dependency on the service and reduction in the robustness of Internet routing overall.

    b. ARIN's RPKI services are available to all parties holding resources in the ARIN registry that have entered into an RSA with ARIN. ARIN notes that utilizing our RPKI services may require some organizations that do not presently have such an agreement to enter into an RSA with ARIN, as ARIN provides a more limited set of registry services to a subset of the organizations in its service region that were receiving registry service in the region prior to ARIN's establishment. As the USG-approved, self-regulating successor Internet number registry for the region[3], ARIN has continued to provide these existing "legacy resource holders" basic registry services without fee or executed contract, but ARIN does require entry into ARIN's RSA and payment of fees (just as all other ARIN customers) for those who wish to utilize more advanced registry services whose development has been funded by our community over the years.

    c. ARIN charges fees for its services which are reasonable and based on an overall cost recovery model. ARIN has a member-elected Board of Trustees that establishes the fee schedule, and changes to our fees or standard RSA are done in consultation with our community.

4) With regard to any rulemaking by the Commission on utilization of RPKI for securing Internet routing, ARIN notes that it has not brought the question of regulatory involvement in this area to its community, and therefore it would not be appropriate for ARIN to represent a particular position. ARIN respectfully recommends that the Commission duly weigh any input received from those organization that would be most directly affected by any such rulemaking, that is, Internet Service Providers and Network Operators.

5) Aside from rulemaking, the Commission may wish to consider the Internet security requirements included in the variety of Internet services that the FCC specifies or purchases to the extent that the security of their Internet routing is a concern.

---

[2] "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", IETF RFC 7115 / BCP 185, https://www.rfc-editor.org/rfc/rfc7115.txt

[3] "Internet Moves Toward Privatization", National Science Foundation, News Release 97-046, https://www.nsf.gov/news/news_summ.jsp?cntn_id=102819, retrieved 25 March 2022.

<u>Discussion</u>

ARIN observes there are a series of questions in the Commission's Request for Comments published in the Federal Register in paragraphs 8-19. Below we provide comments in response to the questions in the order they appear by paragraph in the Request for Comments.

Paragraph 8

The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN does not provide responses to those requests for comments; however, ARIN provides the following with respect to parties participating in RPKI and resulting BGP security implications:

> ARIN notes that the nature of RPKI services for securing Internet routing involves two essential roles: publication of ROAs (which is done by network operators to communicate their authorized routing partners) and validation of BGP routing information received using the published ROAs.   The task of ROA publication is a prerequisite that network operators need to perform first so that there are ROAs available for all to use globally. The task of route origin validation is utilization of those published ROAs by network operators (and significant organizations with multiple connections to the Internet) to deprioritize or discard BGP routing information received based on its validity.

> There is no inherent linkage between two tasks: one may have a network operator publishing ROAs so that those who are receiving their routing announcements will validate them, but that same operator does not validate the routing it receives; similarly, one may have a network which helps secure its routing by performing route validation but does not yet publish ROAs with its own routing validation information.

> It is also worth noting that there are multiple types of RPKI deployment options available to network operators, the two most common being Hosted RPKI and Delegated RPKI.

> Hosted RPKI is a solution that gives organizations the opportunity to take advantage of the enhanced routing security features of the RPKI service by creating ROAs for their IP address and ASN resources, without the requirement of running the components of RPKI publication that include a certificate authority (CA) system, a repository (database), or publication services. The network organization creates ROAs, but their RIR runs all the cryptographic operations of the CA, stores their ROAs in a hosted repository (database), and responds to network queries for this RPKI information. This solution is the most common method selected by network operators today due to its ease of use and limited responsibility.

> The Delegated solution is when an organization chooses to run their own CA, their own repository to store their ROAs, and associated publication services. The uptime requirement of running a repository is a requirement that many network organizations do not want to undertake, often making the Delegated RPKI a less desirable deployment option. Few Delegated

deployments of RPKI exist today – of ARINs 2537 RPKI customers, only 41 are utilizing the delegated model.

Paragraph 9

The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN does not play a direct role in measuring BGP security, nor does it write any tools that provide this type of service. Therefore, ARIN respectfully provides no further comment with regard to Paragraph 9.

Paragraph 10

The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN does not provide responses to those requests for comments; however, ARIN provides the following:

ARIN has invested extensive time development resources at significant cost in building and maintaining these RPKI services for ARIN customers. These services are built to the IETF standards and best current practices that define the infrastructure and performance criteria for the RPKI as they apply to the roles defined for the RIRs to perform. ARIN monitors the activity in the standards-setting bodies for new requirements that necessitate changes in our services to remain consistent with accepted standards and best current practices. ARIN has been running RPKI services since 2012.

With regard to obstacles preventing network operators from deploying certain security measures, including RPKI, that is best answered by those network operators. However, ARIN would like to address a particular hurdle that has been raised by some legacy resource holders in their decision to deploy RPKI; that being the requirement to enter into an RSA with ARIN to be able to utilize ARIN's RPKI services. ARIN notes that hundreds of legacy resource holders have entered into an RSA with ARIN, including major agencies and departments of the US Government, commercial organizations, and educational institutions of all types. ARIN welcomes feedback on the RSA and has updated it several times to address concerns raised by our community. ARIN believes that the reasonable requirement to enter into an RSA with ARIN does not constitute a material impediment to the deployment of RPKI. ARIN recognizes that some organizations may not have reviewed our current agreement and/or have concerns based on past impressions.

Additionally, concerns have been raised about the terms under which ARIN's RPKI is made available to users. ARIN has responded by clarifying and incorporating changes to address such concerns. For example, one concern was that developers of RPKI validation software were previously not able to integrate acceptance of certain RPKI terms of service such as the Relying Party Agreement (RPA) into their software. While ARIN recognizes this is something best considered by developers, ARIN has made this possible and welcomes such integration.

While there are reasonable limitations on the use of RPKI information, developers are able to use RPKI information for research, educational, analysis, and reporting purposes as well as distribution in machine-readable format for real-time network routing purposes. This allows for development of more sophisticated services that engages with and utilizes RPKI.

ARIN also engages in outreach efforts to make the community aware of its RPKI service and the terms of engaging in ARIN's RPKI service. Through its website, as well as direct engagement with representatives of governmental entities, ARIN regularly works with governmental entities to address any issues that may prohibit them from agreeing to such terms, including limited modifications to the terms where there is a legal barrier to those governmental entities entering into such terms.

Finally, with regard to legacy IP address holders, ARIN engages with such holders to inform them of the benefits of entering into an RSA with ARIN and to dispel any misconceptions that doing so upsets any property and transferability rights. Entrance into an RSA with ARIN clarifies the relationship of legacy IP address holders with ARIN and provides the benefit of express contractual rights in a writing signed by both parties.

Paragraph 11

The Commission seeks comment in this paragraph including certain topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN does not provide responses to those topics for which there are requests for comments; however, ARIN provides the following:

As previously stated, the unavailability of the RPKI service by DDOS attacks or for other reasons should not have an impact on routing when operators follow best current practices. ARIN's RPKI service deploys multiple instances in geographically disperse locations to provide redundancy in defense of coordinated denial of service attacks. Additionally, the use of multiple connectivity providers at each location adds another layer of redundancy to defend the ARIN RPKI installations. The performance of this design has been tested by intentionally disabling components of the infrastructure resulting in the loss of reachability, while having no impact to users of RPKI services. By design, should a complete loss of connectivity to the RPKI service occur, adherence to the RPKI best current practices by network operators will result in falling back to traditional BGP routing on the Internet.

Regarding preventing conflicts among the trust anchors, ARIN extensively coordinates with the other RIRs and uses automated tools. The Number Resource Organization (NRO) is the coordinating body for the world's RIRs. The RIRs use this forum to facilitate communications in subject matter-specific working groups, including Engineering-focused subjects like RPKI. ARIN uses automated tools for monitoring the current performance and operations of the RPKI service. Additionally, ARIN's engineering team regularly interacts with its RIR counterparts, keeping apprised of actions in the standards-setting organizations which drive RPKI development.

Paragraph 12

The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN does not have input into the decision-making process of network operators in this regard and does not opine on those decisions or any basis of those decisions. Therefore, ARIN respectfully provides no further comment with regard to Paragraph 12.

Paragraph 13

   The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN does not have input into the decision-making process of network operators in this regard and does not opine on those decisions or any basis of those decisions. Therefore, ARIN respectfully provides no further comment with regard to Paragraph 13.

Paragraph 14

   The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. With regard to any rulemaking contemplated by the Commission on use of RPKI for securing Internet routing, ARIN reiterates that it has not brought the question of regulatory involvement in this area to its community, and therefore it would not be appropriate for ARIN to represent a particular position. ARIN respectfully recommends that the Commission duly weigh any input received from those organization that would be most directly affected by any such rulemaking, that is, Internet Service Providers and Network Operators.

Paragraph 15

   The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators that operate on a global basis. ARIN respectfully provides no further comment with regard to Paragraph 15.

Paragraph 16

   The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. As with any service offered by ARIN, there was a significant one-time expenditure of capital and human effort to develop and deploy RPKI. As ARIN continues to offer RPKI as discussed and expected by the community, there are substantial ongoing maintenance costs for continued development and updates to software as well as upgrades and routine replacement of equipment used to provide RPKI.   ARIN considers these costs to be inherent to the registry and incorporated into our overall cost model and hence to be recovered through the standard registry services fees paid by all contracted ARIN customers. The associated costs and resource requirements for parties to utilize RPKI are best known by those parties; and thus, ARIN provides no further comment with regard to paragraph 16.

Paragraph 17

   The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators. ARIN's costs do not substantially change with respect to a phased-deployment model.   ARIN notes that aside from its rulemaking role, the Commission is also a purchaser or specifier of Internet services and may consider the role BGP security requirements of such services.

Paragraph 18

      The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators as well as general members of the community that rely on secure Internet routing. However, ARIN states that the benefits of more secure Internet routing are varied and wide reaching. More secure Internet routing contributes to a more robust and reliable system of managing Internet traffic that benefits all users of the Internet. There is also the benefit of combating nefarious activities and mitigating risks that include but are not limited to fraud, hacking, denial of service attacks, hijacking, cyber attacks, data privacy breaches, theft, etc.

Paragraph 19

      The Commission seeks comment in this paragraph on several topics that would best be addressed to other parties such as Internet Service Providers and network operators and those members of the community that would most benefit from increased diversity and inclusion. ARIN states that the measures discussed in, and that are the subject of, the Commission's Request for Comments are deployed and implemented objectively with no regard to race, disability, income level, etc. More secure Internet routing, while not directly related to the principles of digital equity and inclusion, carries with it the potential of increasing robustness and availability of Internet services.

<div align="center">Conclusion</div>

      ARIN expresses its sincere gratitude for the opportunity to comment on this discussion around secure Internet routing. The ongoing work in this area is of utmost importance and is essential in maintaining a robust, stable, reliable, and secure Internet for all users of the Internet both domestically in the United States and worldwide. We appreciate the Commission's efforts in this regard and remain available to respond to any further questions or comments the Commission may have.

                                  Respectfully submitted,

                                  John Curran, President/CEO
                                  American Registry for Internet Numbers, Ltd.
                                  P.O. Box 232290
                                  Centreville, VA 20120
                                  (703) 287-9840
                                  jcurran@arin.net