



Federal Resource Public Key Infrastructure (RPKI) Playbook

May 2024
(Version 1.3)

Table of Contents

| | |
|--|-----------|
| Summary Overview | 2 |
| Step 1: Identify Netblocks and Autonomous System Numbers (ASNs) | 2 |
| Step 2: Ensure Netblocks are Under Appropriate ARIN Org IDs | 3 |
| - Transferring a Netblock to a Different ARIN Org | 3 |
| - Listing a Designated Routing POC to Manage RPKI | 6 |
| Step 3: Ensure ARIN Orgs Have Updated Contact Information | 8 |
| Step 4: Ensure Resources are Covered by a Valid RSA | 10 |
| Step 5: Enable RPKI and Add RSAs | 11 |
| New Developments | 16 |
| Closing Statement | 16 |

A special thank you is extended to the following for their time and contributions in the development of this document:

- **Robert (Bob) Cannon**, Senior Telecommunications Policy Analyst, Office of Policy Analysis and Development, National Telecommunications and Information Administration (NTIA)
- **Eric Estes**, N-Wave IT Security Program Manager and Information System Security Officer, Office of the Chief Information Office, National Oceanic and Atmospheric Administration (NOAA)
- **Doug Montgomery**, Manager of Internet Technologies Research, National Institute of Standards and Technology (NIST)
- **Brian Scott**, Deputy Assistant National Cyber Director for Cyber Policy and Programs, Office of the National Cyber Director, The White House
- **Steve Wallace**, Director of Routing Integrity, Internet2



This Federal Resource Public Key Infrastructure (RPKI) Playbook is a step-by-step guide for leveraging the [American Registry of Internet Numbers \(ARIN\) hosted RPKI service](#) to help protect U.S. Federal Government networks from route hijacking.

Summary Overview

- Route hijacks are a [legitimate threat](#).
- Any organization owning or managing logical network resources should protect its stakeholders from the impacts of route hijacks with [Resource Public Key Infrastructure \(RPKI\)](#).
- RPKI allows a network resource owner to make a digitally signed and verifiable assertion a.k.a. Route Origin Authorization (ROA), proving that a specific Autonomous System (AS) has the authority to originate a route prefix.
- Over time, more and more upstream network providers will make routing decisions based on the validity of ROAs.
- Implementation of routing security and RPKI is a priority recognized in the [National Cybersecurity Strategy](#), and will become increasingly important over time.



STEP 1: Identify Netblocks and Autonomous System Numbers (ASNs)

The first step in this process is to identify which netblocks belong to your organization and need protection from RPKI, as well as which ASNs should be allowed to originate those netblocks. For some smaller or centrally-managed organizations this is easy, perhaps only having a single or small number of well-known prefixes under their control. For some larger or more historically decentralized organizations, this can be challenging and will require investigation and outreach.

- A.** Perform outreach / datacalls to Federal Information Security Management Act (FISMA) systems and legacy programs to provide a complete list of network resources
- B.** Search [ARIN](#) for known prefixes and ASNs to understand status
- C.** Use tools to determine/verify RPKI status
 - [Routinator](#)
 - [IRR Explorer](#)
 - [RIPEstat](#)
- D.** Generate a list of netblocks and ASNs requiring action

STEP 2: Ensure Netblocks are Under Appropriate ARIN Org IDs

Organizational restructures happen over time, and the individuals responsible for managing the logical network resources may have changed. Step 2 is to ensure any netblocks identified in Step 1 are under the appropriate ARIN Org IDs corresponding to the individuals who will be managing them.

In some cases, netblocks may need to be transferred to another ARIN Org. Before initiating a transfer, ensure the recipient Org has a legal and justifiable claim to manage the resources as ARIN will attempt to verify legitimacy of the claim and may deny the transfer if not sufficiently justified. Also, it's important to be fully aware of any potential implications to your annual fee before initiating a transfer.



To Transfer a Netblock to a Different ARIN Org:

A. Identify Recipient ARIN Org ID

Work with contacts from the recipient Org who will be managing the resources to ensure the correct Org ID is identified for the transfer. Many Organizations will have both a legacy Org ID (corresponding to any legacy resources held before the establishment of ARIN in 1997), and a 'current' Org ID (corresponding to newer resources). Org IDs can be viewed under the **ARIN Account Manager Dashboard**: click "*Your Records*" and then "*Organization Identifiers*":

ACCOUNT MANAGER

- Dashboard
- Tickets
- Your Records
 - Point of Contact Records
Manage POCs linked to your account
 - Organization Identifiers**
Manage Org IDs and Org POCs
 - Associations Report
Records connected to your account
- IP Addresses
- ASNs
- Routing Security
- Transfer Resources
- Payments & Billing
- Downloads & Services
- Ask ARIN
Create a help desk ticket

Organization Identifiers

If your only responsibility is to manage the billing information for an organization, please go to [Payments & Billing](#) to request billing authorization for your Org ID.

If your Org ID does not have a valid Admin or Tech POC, you can [recover it](#).

Org Actions

- [Create Org ID](#)
- [Recover Org ID](#)

Organizations Associated with Your User Account

Organizations are associated with your account if you are linked to any Point of Contact (POC) for the Org ID, or if you are the Voting Contact.

| Org Handle | Org Name |
|------------|---|
| | National Oceanic and Atmospheric Administration |
| | National Oceanic and Atmospheric Administration |
| | National Weather Service |
| | U.S. Dept. of Commerce |

What is an Org ID?

An Organization Identifier (Org ID) is a record that represents a business, non-profit corporation, or government entity in the [ARIN database](#).

You must have an Org ID to request IP addresses or ASNs (number resources).

B. Initiate Transfer

Either the source or recipient Org can initiate the transfer via the **ARIN Account Manager Dashboard**. Click *“Transfer Resources”* and then answer the questions to determine the correct type of transfer. Ensure your transfer type accurately reflects your organizational structure and consult with ARIN if in doubt.

The screenshot shows the ARIN Account Manager Dashboard. On the left is a navigation menu with items: Dashboard, Tickets, Your Records, IP Addresses, ASNs, Routing Security, Transfer Resources (highlighted), Payments & Billing, Downloads & Services, and Ask ARIN. The main content area is titled "Transfer Resources" and includes a link to "Transfer Resources" and a list of transfer types: NRPM 8.2 (Mergers and Acquisitions Transfers), NRPM 8.3 (Transfers to Specified Recipients within the ARIN Region), NRPM 8.4 (Transfers between Regional Internet Registries (RIRs)), and Transfer Pre-approval requests. A note mentions Reassign Addresses and contacting the upstream organization. Below this is a form titled "About Your Transfer" with questions: "Are both the source and recipient organizations within the ARIN Region?" (Yes selected), "Will you be receiving or supplying resources?" (Receiving selected), "Have you identified the other party involved in this transfer?" (Yes selected), and "Is this transfer a result of a corporate restructure or reorganization?" (Yes selected). A section for "Mergers and Acquisitions Transfers (NRPM 8.2) - Recipient" provides criteria and a "Continue" button.

Once the transfer is initiated, a ticket is created and ARIN staff will guide you through the rest of the process, including:

C. Pay necessary fees

- Note that each transfer requires a one-time non-refundable fee (currently \$500) for ARIN to process the transfer. Multiple resources can be transferred in a single request for one fee.
- In some cases you must also pay delinquent annual fees from the source organization.

D. Obtain required documentation and notarized affidavits

- ARIN staff may ask for documentation supporting the transfer.
- One item which is almost always required is a notarized affidavit from a *‘duly authorized officer’* of the source organization, attesting to the approval of the transfer. ARIN will provide the exact language required for the affidavit.
- A *‘duly authorized officer’* can be a FISMA System Owner, Lab/Program Director, or other person holding a Federal leadership position within the source organization.

The undersigned, _____, hereby affirms and declares
under penalty of perjury that:

(a) I am a duly authorized officer of _____

(b) I acknowledge and authorize the transfer of AS: _____ and AS _____ from _____
to _____

(c) There are no known disputes over AS: _____ and AS _____ issued to _____
, and _____

(d) I acknowledge and understand that ARIN cooperates with law enforcement agencies in instances of suspected fraud.

Signature

Date

North Carolina

County of _____

_____, appearing before the undersigned
Name of principal

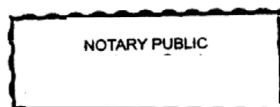
notary and being duly sworn, says that:

1. I am signing an Affidavit to
transfer AS _____ and AS _____
2. from _____ to _____

Principal's Signature

Sworn to (or affirmed) and subscribed before me this the 30th day of Sept.
2023.

(Official Seal)



Official Signature of Notary

_____, Notary Public

Notary's printed or typed name

My commission expires: _____

In most cases, RPKI is managed by the Tech or Admin contacts for the Org. However, it is also possible to designate a 'Routing POC', in cases where the resources should remain with the current Org but RPKI should be managed by a service provider or other network specialist not holding one of the main roles for the Org.

To list a Designated Routing POC to Manage RPKI:

A. In the ARIN Account Manager Dashboard, select "Your Records", then "Organization

The screenshot shows the ARIN Account Manager dashboard. The left sidebar contains a navigation menu with items like Dashboard, Tickets, Your Records, Point of Contact Records, Organization Identifiers (highlighted), Associations Report, IP Addresses, ASNs, Routing Security, Transfer Resources, and Payments & Billing. The main content area is titled 'Organization Identifiers' and includes a yellow warning box about billing, a link to 'recover it', and a table of organizations associated with the user account.

| Org Handle | Org Name |
|------------|---|
| | National Oceanic and Atmospheric Administration |
| | National Oceanic and Atmospheric Administration |
| | National Weather Service |
| | U.S. Dept. of Commerce |

B. Under Organization Points of Contact, click "Manage":

The screenshot shows the ARIN Account Manager dashboard with the 'Organization Record' page selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Organization Record' and includes an 'Org Info' section with details for the National Oceanic and Atmospheric Administration, and an 'Organization Points of Contact' section with expand/collapse controls and a 'Manage' button circled in red.

Org Info

Org ID: |
Org Name: National Oceanic and Atmospheric Administration
Address: 325 Broadway
Boulder, CO 80305
United States
Membership: Service Member ⓘ
Registered Date: |
Last Modified Date: |

Organization Points of Contact

Only the Admin and Tech POCs associated with an organization can modify the organization record. If the Admin and Tech POCs are not valid, you can submit a request to [recover your Org ID](#).

Expand All Collapse All

- Admin POC:
Admin POC:
Name:
Phone Number:
Email:
- Tech POC:
Tech POC:
Name:
Phone Number:
Email:
- Abuse POC:

Manage

C. Under Routing POCs, click "Add Routing POC":

NOC POCs: A NOC POC is responsible for network operation issues. (Optional)

Routing POCs: The Routing POC is responsible for routing registry and certification issues. (Optional)

DNS POCs: The DNS POC is responsible for reverse DNS and secure DNS issues. (Optional)

D. To search for the handle of the contact which will manage RPKI, click "Find POCs". In the case of NOAA N-Wave, the handle is NAT41-ARIN. For other organizations, they will need to provide the appropriate handle to list as a Routing POC.

E. Once these steps are completed, the newly added Routing POC will be able to manage RPKI and add ROAs directly.

NOTE: this does not remove the ability for account managers within the Org to manage RPKI; both internal contacts and Routing POCs may do so.

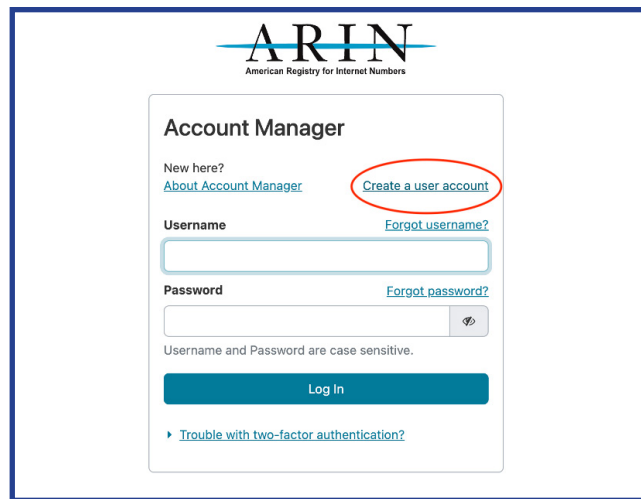


STEP 3: Ensure ARIN Orgs have Updated Contact Information

Organizations change, and people come and go. As a result, many ARIN Org contacts are outdated. Accurate contact information is important for communication regarding the network resources (e.g. security incidents, abuse complaints, legal/policy violations, technical issues, and administrative/billing issues), as well as having the appropriate personnel linked to the roles/POCs which will be performing tasks within the ARIN account.

Ensure all individuals who will be working with logical network resources via ARIN have user accounts with updated contact information.

A. To establish a user account, click *“Log In”* in the upper right of the ARIN home page, and then select *“Create a User Account”*:



An ARIN Org should have Points of Contact (POC) records representing the types of roles performed within the ARIN Org (Admin, Tech, Abuse, NOC, Routing or DNS POC).

Role-based POCs should ideally be generic and have generic contact info (phone numbers and email lists), which will persist as individuals come and go from the organization.



ROAdmin@xxx.gov

John.Doe@xxx.gov

Individual user accounts can then be linked to the role-based POCs, so the individuals may perform their required tasks.

B. To view POCs linked to your ARIN Org, access the **Account Manager Dashboard** and select **“Records”,** then **“Point of Contact Records”**:

The screenshot displays the ARIN Account Manager interface. On the left is a navigation sidebar with categories like Dashboard, Tickets, Your Records, Organization Identifiers, Associations Report, IP Addresses, ASNs, Routing Security, Transfer Resources, Payments & Billing, Downloads & Services, and Ask ARIN. The main content area is titled 'Point of Contact Records'. It features a yellow informational box, a 'POC Actions' panel with links for 'Create POC', 'Link POC', and 'Recover POC', and a 'Your Linked POCs' table. The table has columns for 'POC Handle', 'POC Name', and 'Last Modified', and currently shows no data. Below the table is a 'What is a POC?' section with explanatory text and a bulleted list of when a user account should be linked to a POC.

ACCOUNT MANAGER

Dashboard

Tickets

Your Records

Point of Contact Records
Manage POCs linked to your account

Organization Identifiers
Manage Org IDs and Org POCs

Associations Report
Records connected to your account

IP Addresses

ASNs

Routing Security

Transfer Resources

Payments & Billing

Downloads & Services

Ask ARIN
Create a help desk ticket

Point of Contact Records

If your only responsibility is to manage the billing information for an organization, you do not need a POC record. Go to [Payments & Billing](#) to request billing authorization for your Org ID.

To add, remove, or change POCs on an Org ID, go to [Organization Identifiers](#).

POC Actions

- [Create POC](#)
- [Link POC](#)
- [Recover POC](#)

Your Linked POCs

Your user account is linked to the listed Points of Contact.

| POC Handle | POC Name | Last Modified |
|------------|----------|---------------|
| | | |
| | | |
| | | |
| | | |

What is a POC?

A Point of Contact (POC) represents a specific person or role in [ARIN's Whois](#). A POC can be specified as an Admin, Tech, Abuse, NOC, Routing, or DNS POC for an organization.

Your user account should be linked to a POC if you:

- Need to create or manage **organization records** (Org IDs)
- Need to request or manage **IP Addresses** and/or **ASNs**
- Will serve as a contact for **network operation** or **abuse issues**, or be responsible for records pertaining to **routing** or **resource security**

C. To create a POC for a role such as 'Abuse', 'Admin', ' or Tech', click **“Create POC”**.

Again, list generic contact info such as email lists which will serve as persistent POCs to which individual users can then be linked.

D. To link a user account to a role-based POC, click **“Link POC”** and search for the handle corresponding to the user account.

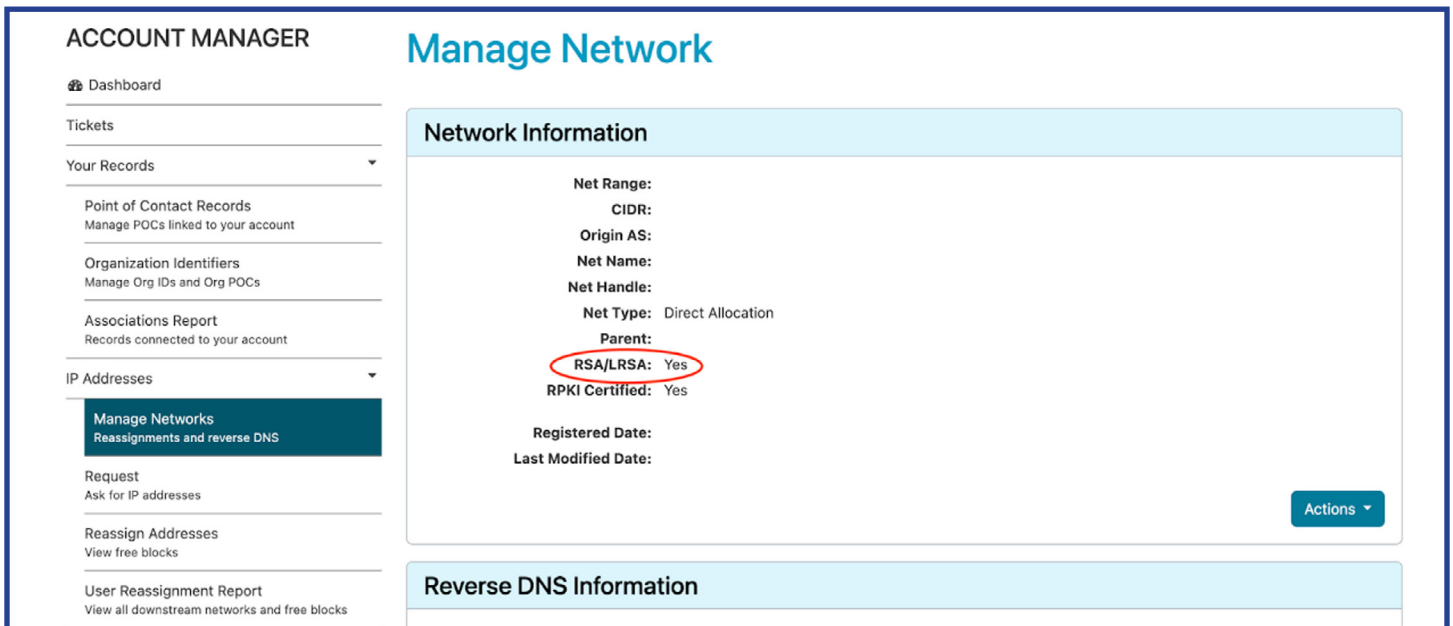
Role-based POCs and user accounts should be reviewed and updated periodically to ensure accuracy. ARIN will initiate contact to the POCs annually to verify contact information, but this function should also be performed by the account manager(s) for the Org IDs.

STEP 4: Ensure Resources are Covered by a Valid RSA

ARIN was established in 1997, after many organizations already owned and managed logical network resources. Such resources are known as 'legacy resources' and were not historically covered by an ARIN Registration Services Agreement (RSA). Resources must be covered by an RSA before they can be protected by ARIN's hosted RPKI service.

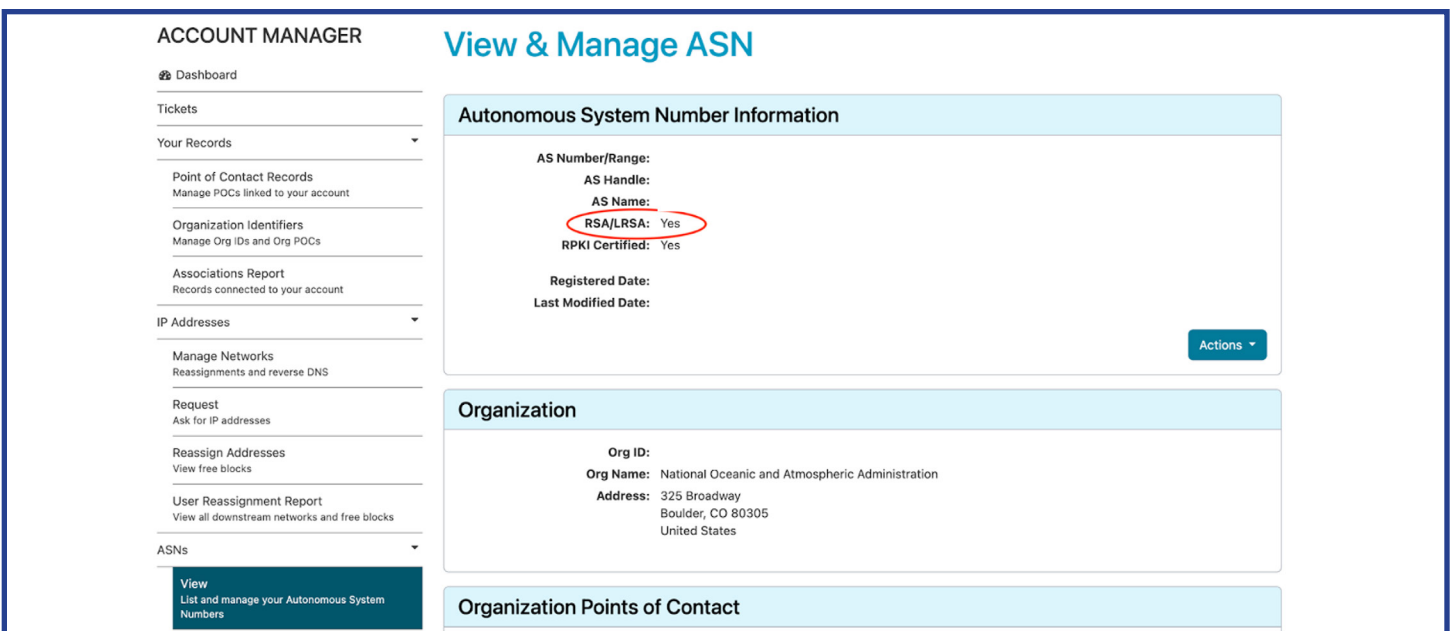
To see the RSA status of a given resource, simply drill down into its details from the main **Account Manager Dashboard**.

A. For Netblocks - click "*IP Addresses*", then "*Manage Networks*", and select the Net Handle for the netblock in question and view the "*RSA/LRSA*" status:



The screenshot shows the 'ACCOUNT MANAGER' interface with a sidebar on the left and a main content area. The sidebar includes sections for 'Dashboard', 'Tickets', 'Your Records' (with sub-items like 'Point of Contact Records', 'Organization Identifiers', 'Associations Report', and 'IP Addresses'), and 'Request' (with sub-items like 'Ask for IP addresses', 'Reassign Addresses', and 'User Reassignment Report'). The 'IP Addresses' section is expanded, showing 'Manage Networks' and 'Reassignments and reverse DNS'. The main content area is titled 'Manage Network' and contains a 'Network Information' section with the following details: Net Range, CIDR, Origin AS, Net Name, Net Handle, Net Type: Direct Allocation, Parent, RSA/LRSA: Yes (circled in red), RPKI Certified: Yes, Registered Date, and Last Modified Date. An 'Actions' button is visible in the bottom right of the 'Network Information' section. Below this is a 'Reverse DNS Information' section.

B. For ASNs - click "*ASNs*", then "*View*", select the AS Handle for the **ASN Information** in question and view the "*RSA/LRSA*" status:



The screenshot shows the 'ACCOUNT MANAGER' interface with a sidebar on the left and a main content area. The sidebar includes sections for 'Dashboard', 'Tickets', 'Your Records' (with sub-items like 'Point of Contact Records', 'Organization Identifiers', 'Associations Report', and 'IP Addresses'), and 'ASNs' (with sub-items like 'Manage Networks', 'Request', 'Reassign Addresses', and 'User Reassignment Report'). The 'ASNs' section is expanded, showing 'View' and 'List and manage your Autonomous System Numbers'. The main content area is titled 'View & Manage ASN' and contains an 'Autonomous System Number Information' section with the following details: AS Number/Range, AS Handle, AS Name, RSA/LRSA: Yes (circled in red), RPKI Certified: Yes, Registered Date, and Last Modified Date. An 'Actions' button is visible in the bottom right of the 'Autonomous System Number Information' section. Below this is an 'Organization' section with details: Org ID, Org Name: National Oceanic and Atmospheric Administration, and Address: 325 Broadway, Boulder, CO 80305, United States. At the bottom is an 'Organization Points of Contact' section.

There is an initiative under way to bring all government resources under a single RSA template with legal terms that have been approved by appropriate government legal offices. If resources under your Org are not covered by an RSA, reach out to your IT management to see if they can be brought under the government-wide RSA or if this is already in motion.

Alternatively, you can engage ARIN directly to bring your resources under your own version of the RSA, but beware of legal implications, as the standard RSA has some terms which are not appropriate for government use. Additionally, there are **fees** associated with bringing resources under an RSA which may be avoided or reduced by consolidating with the wider government initiative.



STEP 5: Enable RPKI and Add ROAs

Once resources are covered by an RSA, they can be protected by ARIN's hosted RPKI service.

A. To enable RPKI - access the **Account Manager Dashboard**, then click *"Routing Security"*:

The screenshot displays the ARIN Account Manager Dashboard. The left sidebar contains a menu with the following items: Dashboard (selected), Tickets, Your Records, IP Addresses, ASNs, **Routing Security** (circled in red), Transfer Resources, Payments & Billing, Downloads & Services, and Ask ARIN (with a sub-link 'Create a help desk ticket').

The main content area is titled 'Dashboard' and includes an 'Alerts' section with a yellow warning box: 'Two-Factor Authentication is not set. [Configure it now.](#)'

The 'Account Snapshot' section features four metrics:

- 2 Point of Contact records (POCs)
- 2 Organization Identifiers (Org IDs)
- 3 Networks (NETs)
- 2 Autonomous System Numbers (ASNs)

At the bottom, there is a 'What's New With ARIN Online' section with a link to 'ARIN Online Functionality' for an overview of all the functionality currently available within ARIN Online.

B. On the **Routing Security Dashboard** page, under *"Your Organizations"*, select *"Sign Up for RPKI"* for the organization for which you want to configure Hosted RPKI:

The screenshot shows the ARIN Routing Security Dashboard. On the left is the 'ACCOUNT MANAGER' sidebar with 'Routing Security' selected. The main content area is titled 'Routing Security Dashboard'. Below the header, there is a section for 'Your Organizations' which contains a table of organizations associated with the user account. The table has columns for Org ID, IRR Eligibility, IRR Action, RPKI Eligibility, and RPKI Action. The row for 'ARINL' has a green checkmark for IRR Eligibility and a red 'X' for RPKI Eligibility. The 'Sign Up for RPKI' link in the RPKI Action column for ARINL is circled in red. Below the table is a section for 'ARIN's RPKI Trust Anchor Locator (TAL)' with a link to 'Access RPKI TAL'.

| Org ID | IRR | | RPKI | |
|--------|-------------|--------------------------|-------------|----------------------------------|
| | Eligibility | Action | Eligibility | Action |
| ARIN-2 | ✓ | View IRR | ✗ | Ask ARIN |
| ARINL | ✓ | | ✗ | Sign Up for RPKI |

C. On the **Manage RPKI** page, under **Choose Between Two Models of RPKI**, select *"Sign Up for Hosted"* to make your resource certificate request:

The screenshot shows the ARIN Manage RPKI page. The page is titled 'Manage RPKI' and shows the 'Org ID: ARINL'. Below the header, there is a section for 'Choose Between Two Models of RPKI'. This section contains two columns: 'Hosted RPKI' and 'Delegated RPKI'. The 'Hosted RPKI' column describes using ARIN's infrastructure to create and manage ROAs, listing benefits like using ARIN's CA and repository, starting right away, and automatic renewal. A red arrow points to the 'Sign up for Hosted' button. The 'Delegated RPKI' column describes running your own Certificate Authority (CA) to create and manage ROAs, listing requirements like using your own CA and software. Below the columns is a note stating that on sign-up, ARIN generates a Resource Certificate for the number resources that are both directly assigned to the Org ID and covered under a signed Services Agreement (RSA/LRSA) with ARIN. At the bottom, there is a link for more information about RPKI, 'Resource Certification'.

D. To begin your certificate request, select "Hosted Certificate" In the top bar of the Manage RPKI page.

E. If prompted, read and agree to the [RPKI Terms of Service](#). (NOTE: Not required for resources covered by an RSA version 12 or greater). ARIN will create a resource certificate covering the resources allocated to your Org.

F. After submitting your request, you will be returned to the Routing Security Dashboard page. You can then select "Manage RPKI":

ACCOUNT MANAGER

Dashboard

Tickets

Your Records

IP Addresses

ASNs

Routing Security

Transfer Resources

Payments & Billing

Downloads & Services

Ask ARIN
Create a help desk ticket

Routing Security Dashboard

ARIN supports routing security with two services: [Internet Routing Registry \(IRR\)](#) and [Resource Public Key Infrastructure \(RPKI\)](#). Registrants can use these services to help secure Internet routing for their eligible resources.

Your Organizations

Organizations associated with your user account are listed alphabetically by Org ID.

| Org ID | IRR | | RPKI | |
|--------|-------------|----------------------------|-------------|-----------------------------|
| | Eligibility | Action | Eligibility | Action |
| ARIN-2 | ✓ | View IRR | ✗ | Ask ARIN |
| ARINL | ✓ | Manage IRR | ✓ | Manage RPKI |

ARIN's RPKI Trust Anchor Locator (TAL)

Relying party software (validator) must incorporate the ARIN TAL to fetch data from ARIN's RPKI repository.

[Access RPKI TAL](#)

G. To begin creating ROAs, access the RPKI: ROAs page and you can begin creating ROAs for your resources by selecting "Create ROA":

ACCOUNT MANAGER

Dashboard

Tickets

Your Records

IP Addresses

ASNs

Routing Security

Transfer Resources

Payments & Billing

Downloads & Services

Ask ARIN
Create a help desk ticket

RPKI: ROAs

Org ID: ARINL Hosted RPKI: Overview **ROAs** Certified Resources

The Org ID has the following Route Origin Authorizations (ROAs) in ARIN's RPKI Repository.

Route Origin Authorizations

Filter ROAs by Origin AS or Prefix.

Resource: Search ROAs

Example: AS64496 or 64496, 2001:DB8::/48 or 192.0.0.0/24

[Create ROA](#)

| Origin AS | Prefixes | ROA Name |
|------------|----------|----------|
| None found | | |

i A Route Origin Authorization (ROA) is a cryptographically signed object, made by the authenticated resource holder, that states the authorized Origin ASN for a prefix or set of prefixes.

ARIN auto-renews ROAs created using the Hosted RPKI service so that they persist until manually deleted.

H. After entering the required information, select "Next Step". Verify the information in your ROA is correct and select "Submit":

The screenshot shows the ARIN Account Manager interface for creating a Route Origin Authorization (ROA). The page title is "RPKI: Create ROA". On the left is a navigation menu with "Routing Security" selected. The main content area has a sub-header "Create a Route Origin Authorization (ROA)" and a description: "Create route origin authorizations (ROAs) for the IP resources covered by your RPKI certificate." The form includes fields for: *Origin AS (required), *Prefixes (with a "Prefix ?" tooltip), Max Length (with a "Max Length ?" tooltip and a value of 24), and ROA Name (with a tooltip: "Optional: Provide a helpful nickname, such as DDOS_Mitigation"). A red arrow points to the "Next Step" button. Below the form is an informational box: "A Route Origin Authorization (ROA) is a cryptographically signed object that states which Autonomous System (AS) is authorized to originate a particular prefix or set of prefixes. For more information, visit ARIN's Route Origin Authorizations documentation."

The screenshot shows the ARIN Account Manager interface for reviewing a Route Origin Authorization (ROA). The page title is "RPKI: Create ROA". On the left is a navigation menu with "Routing Security" selected. The main content area has a sub-header "Review ROA" and a summary of the ROA details: Origin AS, Prefixes, Max Length 24, and Auto-renewing: Yes. A red arrow points to the "Submit" button. A "Previous Step" button is also visible.

I. **Finally**, you will then be returned to the **RPKI: ROAs** page, where you will receive confirmation that your ROA has been created. Your ROA will be listed in the **Route Origin Authorizations** table.

The screenshot displays the ARIN ACCOUNT MANAGER interface. On the left is a navigation menu with options like Dashboard, Tickets, Your Records, IP Addresses, ASNs, Routing Security (highlighted), Transfer Resources, Payments & Billing, Downloads & Services, and Ask ARIN. The main header shows 'ACCOUNT MANAGER' and 'RPKI: ROAs'. A green success message states: 'ROA for "AS38870 149.112.152.0/24 Max Length 24" was saved successfully.' Below this, the 'Hosted RPKI' section includes tabs for Overview, ROAs (selected), and Certified Resources. A message indicates that the Org ID (ARINL) has the following Route Origin Authorizations (ROAs) in ARIN's RPKI Repository. The 'Route Origin Authorizations' section features a search bar with the label 'Resource:' and a 'Search ROAs' button. Below the search bar is an example: 'Example: AS64496 or 64496, 2001:DB8::/48 or 192.0.0.0/24'. A 'Create ROA' button is also present. A table with the following structure is shown:

| Origin AS | Prefixes | ROA Name |
|-----------|----------------|------------|
| | Max Length: 24 | Manage ROA |

At the bottom, an information box explains: 'A Route Origin Authorization (ROA) is a cryptographically signed object, made by the authenticated resource holder, that states the authorized Origin ASN for a prefix or set of prefixes. ARIN auto-renews ROAs created using the Hosted RPKI service so that they persist until manually deleted.'

A Note on “Max Length”

Specifying a “Max Length” can provide some flexibility, allowing more specific prefixes underneath to be advertised out of the same ASN without needing separate ROAs. One such use case is to allow an upstream provider to perform Distributed Denial of Service (DDOS) scrubbing, originating more specific prefixes out of their own ASN to divert traffic through the scrubbing service. However, the “Max Length” parameter has been shown to theoretically introduce additional risks, such as forged origin AS attacks described [here](#). Best practice dictates that “Strict ROAs” should be published, for the exact prefixes as advertised. This requires careful coordination with all stakeholders to ensure that all prefixes are covered by valid ROAs.

Verifying ROA Status of Routes Seen on the Internet

When managing ROAs, it can be useful to verify the status of prefixes via internet facing tools which query the global route tables. Popular examples include:

- [Routinator](#)
- [IRR Explorer](#)
- [RIPEstat](#)

New Developments



Routing day speakers in attendance at the Department of Commerce (DOC) press conference held on May 13th, including multiple federal agency representatives and ARIN's CEO

U.S. Department of Commerce Implements Internet Routing Security

On May 13, 2024, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) alongside several other bureaus within Commerce including the Bureau of Economic Analysis (BEA), the Bureau of Industry and Security (BIS), the National Oceanic and Atmospheric Administration (NOAA) and the International Trade Administration (ITA), began implementing an important Internet routing security measure, enhancing cybersecurity throughout the Department and completing a key priority from the National Cybersecurity Strategy. Per the press release, "NTIA created Route Origin Authorizations (ROAs) that authenticate NTIA's addresses as destinations found on the Department of Commerce's network. The partnership with NTIA and NOAA N-Wave allows for all DOC bureau creation of ROAs, and federal wide guidance on routing security through an available "RPKI" playbook. ROAs protect against address hijacks – falsely announcing addresses as destinations on the wrong network. Address hijacks can result in loss of service or interception of data."

To read the press release entitled "*U.S. Department of Commerce Implements Internet Routing Security*", click [here](#).

Closing Statement

In completing the steps outlined in this "*Federal RPKI Playbook*", you will have helped to protect your network resources from route hijacks and misconfigurations which could divert legitimate traffic from its intended destination. Additionally, you will have helped support the National Cybersecurity Strategy in securing the technical foundation of the internet.

For additional questions about the content in this playbook, contact nwave-security@noaa.gov.



Website: nwave.noaa.gov
Email: nwave-security@noaa.gov