ARIN, Law Enforcement, & Public Safety

FREQUENTLY ASKED QUESTIONS



What do Regional Internet Registries (RIRs) do?

The core function of an RIR is to manage and distribute Internet number resources (IPv4 and IPv6 addresses and Autonomous System Numbers [ASNs]) within their defined geographical regions of the world, as well as maintain a unique registry of those number resources and their associated contact information (commonly referred to as "Whois"). Additionally, each RIR provides a wide variety of associated supporting services, tools, and public awareness and capacity building programs, typically in collaboration with industry partners from across the world.

LEARN MORE ABOUT ARIN SERVICES

LEARN MORE ABOUT THE RIR SYSTEM

Why is the work of the RIRs valuable to law enforcement and cybersecurity organizations?

Online criminal activity requires the use of a computer and an IP address. All IP addresses can be traced through one of the five RIRs and their registry database, commonly referred to as Whois. This registration data can be a valuable tool for law enforcement in their investigative process. Additionally, Whois can assist law enforcement in determining which Internet service provider(s) (ISP) may be connected to a particular end user to be able to identify appropriate recipients on whom to serve legal process such as a subpoena.

Do all of the other RIRs work with law enforcement and public safey organizations, and if so, how would one contact them for information?

Yes. Each RIR has dedicated staff that works with and supports law enforcement in a variety of ways. Additionally, the five RIRs are members of the Public Safety Coordination Group, which was created for the explicit purpose of global coordination of law enforcement and public safety engagement. Visit each RIR's homepage to learn more.



ARIN, Law Enforcement, & Public Safety

FREQUENTLY ASKED QUESTIONS

How does ARIN support law enforcement and other public safety organizations with their investigations?

- **Publicly accessible Internet number resource registry information (Whois):** ARIN's public registry of Internet number resources and their associated contact information can be used as a first step in a criminal investigation.
- **Case support:** ARIN's compliance with law enforcement often begins with an email or phone call to answer basic questions before a subpoena or court order is issued. ARIN responds promptly to law enforcement inquiries, subpoenas, and court orders, and ARIN can assist in the preparation of these requests in order to facilitate the process.
- **Capacity building programs:** ARIN provides training, outreach, webinars, and dedicated information sharing sessions on a variety of topics including security, technical matters, and governance.
- **Global trust community access:** ARIN supports an international community of law enforcement and related participants.
- **Data accuracy initiatives:** LEAs work to improve the integrity and accuracy of registration data via participation in the formal community policy development processes of the ARIN community as well as the communities of the other RIRs.
- **Public Policy and Members Meetings:** LEAs can attend ARIN's free Public Policy and Members Meetings, which provide valuable opportunities to become familiar with, and participate in, Internet number resource governance and policy making processes.

LEARN MORE ABOUT TRAINING AT ARIN

LEARN MORE ABOUT ARIN MEETINGS

What measures does ARIN take to provide accurate Whois data?

- **Contractual Requirements (stipulated in the Registration Services Agreement):** Registrants must comply with all policies, and provide and maintain accurate registration information in Whois for themselves and their customers. This contract may be terminated if the holder violates any applicable laws, statutes, rules, or regulations.
- **Policy Requirements:** All but the smallest assignments to customers must be publicly registered in Whois. Annual Point of Contact validation is required for any organization who has received Internet number resources from ARIN or its predecessor registry, or any organization that has a reallocation from an upstream ISP. Contact types that must be validated include Admin, Tech, NOC, and Abuse. Reallocations and certain types of reassignments will not be processed by ARIN unless the recipient organization is already registered in Whois and has at least one validated Point of Contact associated with it. ARIN may audit a resource registrant at any time.
- **Business Practices:** All organizations requesting resources directly from ARIN must have a registered legal presence in region and be in good standing. All new organization registration requests are vetted during the initial application and will be re-vetted again every 12 months if/when they return to ARIN to request additional services.



ARIN, Law Enforcement, & Public Safety

FREQUENTLY ASKED QUESTIONS

Does ARIN restrict certain data fields in its Whois to address concerns with GDPR?

All registration information placed in ARIN's Whois as part of the registration process is publicly displayed and available to query. As a public registry, ARIN's mission and obligations include distributing information about who administers number resources – most obviously, the Whois database, which provides technical troubleshooters, law enforcement, and the interested public with information about which network providers administer specific number resources. Distributing this information is very much in the public interest of proper functioning of the Internet, as ARIN details in its privacy practices.

What types of fraudulent activity does ARIN typically see?

Much of the fraudulent activity detected by ARIN (and the other RIRs) centers around attempted hijackings of IPv4 address space in Whois. As a result of the depletion of the IPv4 address space, the demand for IPv4 resources continues to be strong while the supply remains constrained, which has created an incentive for malicious actors to attempt to manipulate and falsify registration data. There are also reports of route hijackings, buying and selling of IPv4 addresses outside of the registry system, and the leasing of address space through the use of falsified Letters of Authority.



ARIN, Law Enforcement, & Public Safety

Information Not Publicly Available in Whois

- Domain names and any associated information
- Authoritative information for subdelegations by ISPs using RWhois, resources registered in other RIRs' Whois, customer reassignments smaller than /29 (per ARIN policy), and some privatized residential customers (per ARIN policy)
- Routing information
- Accurate geographic location of the network

Why doesn't ARIN have the geographic location of the IP address?
The main purpose of Whois is to record authorized users or assignees of an Internet resource. ARIN cannot guarantee that the address associated with an Internet resource record is the actual physical location of the network.

Other Information ARIN May Be Able to Provide

- Upstream ISP or end user contact information
- Customer reassignment information smaller than /29
- Previous address holders subsequent to a transfer of the resources to another organization
- Financial transaction records and billing Points of Contact
- Other miscellaneous information provided by customers when seeking ARIN services

ARIN may be able to provide this information with a properly issued subpoena, which should include the name of the organization, the individual's name(s), the IP address or ASN in question, and the specific date range for alleged activity or for information requested. Subpoenas should not include extraneous material that is not related to ARIN's services or business model.

Useful Tools and Resources

Using ARIN's Whois
arin.net/resources/registry/whois/

ARIN's Bulk Whois Data (downloadable)
arin.net/reference/research/bulkwhois/

ARIN's Historical Whois Data (Whowas)
arin.net/reference/research/whowas/

Routing History
stat.ripe.net/

RIR Statistics
nro.net/about/rirs/statistics/

Number and Name Lookup Services (Root zone database for TLDs)
iana.org/domains/root/db

↑ SCAN FOR FREQUENTLY ASKED QUESTIONS