REPORT ON

ARIN'S

DESCRIPTION OF ITS RPKI PLATFORM AND ON THE SUITABILITY OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD

DECEMBER 1, 2022 TO SEPTEMBER 30, 2023

ARIN– SOC 3 TABLE OF CONTENTS

Acronym Table

AFRINIC	African Network Information Centre
AICPA	American Institute of Certified Public Accountants
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers, Ltd
BGP	Border Gateway Protocol
CA	California
CEO	Chief Executive Officer
FL	Florida
GCP	Google Cloud Platform
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
LACNIC	Latin America and Caribbean Internet Centre
LLP	Limited Liability Partnership
RIPE	Regional Internet Registry for Europe
RPKI	Routing Public Key Infrastructure
SOC	Service Organization Controls
TSP	Trust Services Principles
VA	Virginia
WA	Washington

Section 1: Assertion of the Management of ARIN

Assertion of the Management of ARIN

We are responsible for designing, implementing, operating, and maintaining effective controls within ARIN's RPKI Platform throughout the period December 1, 2022 to September 30, 2023, to provide reasonable assurance that ARIN's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity*, *Confidentiality, and Privacy*, (*With Revised Points of Focus-2022*), in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2022 to September 30, 2023, to provide reasonable assurance that ARIN's service commitments and system requirements were achieved based on the applicable trust services criteria. ARIN's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2022 to September 30, 2023, to provide reasonable assurance that ARIN's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Christian Johnson
Chief Information Security Officer
ARIN
November 8, 2023

Section 2: Independent Service Auditors' Report

MARCUM
ACCOUNTANTS ▲ ADVISORS

Independent Service Auditor's Report

To: ARIN

Scope

We have examined ARIN's accompanying assertion titled "Assertion of ARIN Management" (assertion) that the controls within ARIN's RPKI Platform (system) were effective throughout the period December 1, 2022 to September 30, 2023, to provide reasonable assurance that ARIN's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022)*, in AICPA *Trust Services Criteria*.

Service Organization's Responsibilities

ARIN is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ARIN's service commitments and system requirements were achieved. ARIN has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ARIN is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve ARIN's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ARIN's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within ARIN's RPKI Platform were effective throughout the period December 1, 2022 to September 30, 2023, to provide reasonable assurance that ARIN's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Marcum LLP

Marcum LLP

Tampa, FL
November 8, 2023

Attachment A: ARIN's Description of the Boundaries of its RPKI Platform

Company Overview and Services Provided

Company Overview

ARIN is a nonprofit, member-based organization that supports the operation and growth of the Internet. ARIN accomplishes this by carrying out its core service, which is the management and distribution of Internet number resources such as IPv4 and v6 addresses and ASNs. ARIN manages these resources within its service region, which is comprised of Canada, the United States, and many Caribbean and North Atlantic islands. ARIN also coordinates policy development by the community and advances the Internet through informational outreach. ARIN's Headquarters facility is located in Chantilly, Virginia. ARIN is one of five RIRs along with AFRINIC (Africa), APNIC (Asian Pacific), LACNIC (Latin America), and RIPE (Europe).

ARIN was incorporated April 18, 1997 and began operations December 22, 1997 to "provide IP registration services as an independent, nonprofit corporation." Until this time, IP address registration for the ARIN region was done in accordance with policies set by the IETF by Network Solutions corporation as part of the InterNIC project. The National Science Foundation approved the plan for the creation of a not-for-profit organization to "give the users of IP numbers (mostly Internet service providers, corporations and other large institutions) a voice in the policies by which they are managed and allocated within the North American region." Network Solutions transitioned these tasks, as well as initial staff and computer infrastructure to ARIN.

ARIN is structured to operate as a service organization that is responsive to the needs of the public it serves. It is organized and driven by the users in the community and is thus able to keep in step with their requirements. The ARIN Board of Trustees and Advisory Council oversee and direct the President & CEO as well as the ARIN staff.

Services Provided

ARIN's RPKI Platform, also known as Resource Certification, is a specialized public key infrastructure framework supporting improved security for the Internet's BGP routing infrastructure. RPKI is an important component of resource certification based on the Internet resources management hierarchy.

RPKI aims to add a verifiable form of a holder's current right to specific resources over the Internet by using cryptographically verifiable statements to verify the association between Internet number resources (IP addresses and ASNs) and their rightful holders. This enables resource holders to attest which ASNs should originate their prefixes (i.e. blocks of IP addresses). Network operators can compare BGP announcements from the global Internet routing table with RPKI validity data to make informed decisions to enhance their routing security.

ARIN offers 3 configurations of RPKI: Hosted, Delegated, and Hybrid. Each type is designed to meet different customer needs and make use of a central RPKI design layout. A customer reviews the RPKI configuration descriptions to determine which configuration is right for their environment, then follows the appropriate implementation instructions.

Infrastructure

The RPKI infrastructure consists of both provisioning and public facing services. Provisioning is available from Chantilly and Ashburn, VA locations and makes available the core RPKI services to the public facing service nodes, which are accessible from Equinix facilities in Ashburn, VA and San Jose, CA and from the Wowrack facility in Seattle, WA.

ARIN's RPKI infrastructure is made up of virtualized nodes for publication of RPKI services in its Hosted, Delegated, and Hybrid configurations. ARIN also uses GCP to provide the resources to host a small segment of RPKI. ARIN uses IBM's HSM to securely manage, process, and store cryptographic keys inside a tamper-resistant hardware device. RPKI services are available and backed up at each of the offsite locations, providing parallel availability and redundancy.

Software

The following is a summary of software systems used to deliver ARIN's RPKI:

- Hypervisor and server operating systems
- Virtual machine management
- Server metric visualization
- Configuration management
- Monitoring
- Firewalls
- Packet capture, storage, and indexing
- Intrusion detection system

People

ARIN's organizational structure defines specific roles, responsibilities, and appropriate lines of reporting required to support RPKI. It is comprised of, and supported by the following teams who are responsible for the delivery and management of the system:

- Executive Management Team – Responsible for providing the overall direction, strategic vision, and management for ARIN and RPKI.
- Office of the Chief Customer Officer – Oversees all aspects of customer excellence and develops and maintains key client relationships with appropriate senior-level points of contact with ARIN customers and key Internet number resource stakeholders. The Communications and Registration Services Departments report to the Chief Customer Officer.
- Engineering – Responsible for development, implementation, and support of ARIN internal systems and technical community services. Engineering also works with the other RIRs on various projects and provides systems-related support for community-based policy implementations.
- Information Security – Provides the overall definition, guidance, and direction of information security strategies to support ARIN's corporate objectives and protect the company's assets.
- Human Resources and Administration – Responsible for providing overall strategic direction for all activities related to acquiring personnel, managing employee compensation, internal

company policies, administering payroll and staff benefits, employee training, office management and security, and travel administration.

Processes and Procedures

Management has developed and communicated to employees a set of policies, processes, and procedures in several operational areas which supports the company's security, availability and confidentiality objectives. As part of the wider Information Security Management Program, ARIN has developed and organized the following policies and procedural documents that are used to support the RPKI.

- Access Control
- Backup and Restoration
- Business Continuity and Disaster Recovery
- Change Management
- Corporate Ethics
- Crisis Communications
- Customer Support
- Data Retention and Disposal
- Incident Management
- Information Classification
- Information Security
- Information Security Risk Assessments
- IT Acceptable Use
- Key Management and Cryptography
- Network Security
- Personnel Security
- Physical and Environmental Security
- Security and Phishing Defense Training
- Server Security
- Software Development
- Technology Equipment Handling and Disposal
- Vendor Risk Management
- Vulnerability and Penetration Testing
- Workstation and Mobile Devices

Control activities are in place to ensure that actions are carried out properly and efficiently to achieve compliance with policies and procedures. ARIN applies a risk management approach to select and develop control activities. After relevant risks are identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable TSCs and the overall objective of the organization.

Data

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the potential impact to ARIN if that data is disclosed, altered, or destroyed without authorization. The classification of data helps determine appropriate security controls for safeguarding that data.

ARIN maintains the data it collects in accordance with the classification assigned to the data and uses classifications of low, moderate, and high for sensitivity and impact. Information systems and resources are protected at the level they inherit from the data stored or passing through the system. Periodic reviews of data classification are conducted by ARIN to ensure that data remain classified correctly and are sufficiently protected. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

ARIN uses secure methods and protocols for the transmission of confidential information over public networks and databases housing sensitive customer data are encrypted at rest. Specific data destruction periods are determined based on data classification, media type, industry compliance, and operational necessity.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Risk Assessment

ARIN management performs an annual risk assessment, which requires management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. ARIN's management reevaluates the risk assessment annually or when otherwise necessary to both update the previous results and to identify new areas of concern.

The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence.
- Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and applicable regulations.
- Monitoring – The monitoring phase includes ARIN management performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

Subservice Organizations

ARIN uses Equinix and Wowrack as subservice organizations for data center colocation services. Equinix and Wowrack are responsible for the uptime, management, physical and logical security of the infrastructure that supports the delivery of internet, and environmental conditions that provide power and cooling to their devices. Equinix and Wowrack are also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

ARIN also uses GCP for IaaS to host a portion of RPKI infrastructure. GCP is responsible for the uptime, management, physical and logical security of the infrastructure that supports the delivery of internet, and environmental conditions that provide power and cooling to their devices. GCP is also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

Communication

Internal Communications

ARIN has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events were communicated. These methods include orientation for new employees and ongoing trainings for employees. Job descriptions are provided to employees and evaluations are completed against those job descriptions annually.

External Communications

ARIN has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in communication of significant events. These methods include the use of e-mail messages and a customer contact option on the ARIN website.

Attachment B: Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

ARIN designs its processes and procedures related to its RPKI Platform to meet its objectives. Those objectives are based on the service commitments that ARIN makes to user entities, the laws and regulations that govern service providers, and the financial, operational, and compliance requirements that ARIN has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of ARIN's RPKI Platform are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Access and authentication standards.
- Intrusion detection and incident handling standards.
- Use of encryption protocols to protect customer data at rest and in transit.
- Use of firewalls to limit unnecessary ports, protocols, and services.

Availability commitments to user entities are documented in customer agreements. Availability commitments are standardized and include, but are not limited to, the following:

- Processing capacity is maintained, monitored, and evaluated.
- Backup and recovery capabilities are in place.
- Business continuity and disaster recovery plans are in place and tested.

Confidentiality commitments to user entities are documented in customer agreements. Confidentiality commitments are standardized and include, but are not limited to, the following:

- Information is defined and classified into categories with associated periods.
- Data retention and disposal policies and procedures are documented and in place.
- Equipment with data storage capabilities are wiped as a component of the disposal process.

ARIN establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ARIN's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the

system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the RPKI Platform.

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

- Marcum LLP
  www.marcumllp.com
- Marcum Bernstein & Pinchuk
  www.marcumbp.com
- Marcum Insurance Services
  www.marcumis.com
- Marcum RBK Ireland
  www.marcumrbk.com
- Marcum Search
  www.marcumsearch.com
- Marcum Strategic Marketing
  marketing.marcumllp.com
- Marcum Technology
  www.marcumtechnology.com
- Marcum Wealth
  www.marcumwealth.com

MARCUM
ACCOUNTANTS ▲ ADVISORS

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com