BUSINESS CONSTITUENCY

The ICANN GNSO Business Constituency
Newsletter, March 2024

Welcome to San Juan and **ICANN79**

Greetings from the BC Chair and welcome to ICANN79!

We gather this time in San Juan, Puerto Rico, where our community will conduct the 2024 Community Forum. It promises to be a full week of consultations and collaboration. As always, there is much work to be done as we work on the myriad issues in front of our governance body.

2023 was a very eventful year, when we emphasized the need for redoubling our efforts to underline the efficacy of the multistakeholder model, urged the community to continue the battle against domain name system abuse, and made preliminary preparations for a new gTLD round, among other important business.

In San Juan, the BC, and the business users of the internet which it represents, anticipate robust discussion of the important and varied issues before us.

Whether you're new to the BC or a veteran of our work, your knowledge, advocacy and opinions are important. You are very much encouraged to join discussions, ask questions, and make your input known. The BC needs thoughtful contributions from you and others who carry forward the needs of online businesses.

The Community Forum is a longer ICANN meeting, with time built in for extensive consultations and collaborative work. This includes expanded times for our BC and Commercial Stakeholder Group (CSG) meetings, both scheduled for later in

continued over page >>

>> continued from front page

the week, where we will discuss matters of immediate importance. I encourage you to make time for all these sessions.

ICANN Org has done its usual outstanding job of organizing a meeting schedule and venue that is sure to be as welcoming as possible, and the BC will seize upon the opportunity to collaborate with our community colleagues toward ICANN's mission of providing a stable, secure and resilient domain name system. When you get a moment, take the opportunity to say thanks to ICANN staff for the significant effort that goes into planning an inclusive set of proceedings.

The BC very much needs your support and input. Our group represents the interests of businesses ranging from the small to multinational, and our responsibilities to our constituency have only grown over time. As challenges arise in ICANN policy work, we rely on the input of our membership to be most impactful.

As we embark on our work, don't hesitate to join and contribute. You'll find that your BC colleagues are open and welcoming to your input and will help you advance your interests within the ICANN sphere.

Again, on behalf of your colleagues in the BC, welcome to ICANN79. All the best for a productive time in San Juan.

Sincerely,

Mason Cole,
BC Chair

ICANN79 At a Glance

Throughout the week of ICANN79, numerous sessions will cover issues of importance to BC members. Make sure to fully review the conference agenda for the times and topics that interest you. Here is a summary of the sessions specific to BC and CSG

Saturday, March 2 • 09:00 – 10:00
ICANN79 PSWG and CSG Meeting

Sunday, March 3 • 15:00 - 16:00
Joint Session: CPH and CSG Memberships

Sunday, March 3 • 16:15 - 17:30
CPH DNS Abuse Community Outreach

Tuesday, March 5 • 09:00 - 10:00
CSG Working Session:
Share Your Stories – RDS Requestor Experiences

Tuesday, March 5 • 10:30 - 12:00
NCPH Work Session

Tuesday, March 5 • 13:15 - 14:30
BC Membership Work Session

Tuesday, March 5 • 16:15 - 17:30
ICANN Board and CSG Membership

Wednesday, March 6 • 10:30 - 12:00
ICANN Board and Community
FY26-30 Strategic Plan Development Community Consultation

Thursday, March 7 • 10:30 - 12:00
ICANN Public Forum

The 2024 Nominating Committee Will Fill Seven Open Leadership Positions

Many BC members are noted for their expertise and called upon to provide input to important issues in their communities. Here is one example.

Tanzania Launches Initiative to Protect Children Online

Dorothy Gwajima, Tanzania's Minister of Community Development, Women, and Special Groups

Today's children are growing up in an increasingly digital world and more young children in the region are spending time online.

Tanzania has established a national advisory council and launched a Child Online Protection (COP) campaign to promote awareness about the forms of criminality that children face online. The campaign will focus on teaching children, parents, and teachers about their roles in protecting children online.

Dorothy Gwajima, Tanzania's Minister of Community Development, Women, and Special Groups, announced that the COP will run for one year in electronic, print, outdoor, and online media to raise awareness and review child-related laws and regulations. The Minister notes findings in a 2022 ECPAT International/UNICEF study that revealed 4% of children have been subjected to various forms of violence online.

Yusuph Kileo, a cybersecurity and digital forensics expert, stresses that, Digital access exposes children to a wealth of benefits and opportunities, but also to a host of risks including access to harmful content, sexual exploitation and abuse, cyber bullying, and misuse of their private information. He urged everyone to know the risks and how to protect themselves against those risks.

"As the first ICANN Public Meeting of 2024, ICANN79 is our first opportunity this year to come together as a community to solve problems and work together to ensure an inclusive, interoperable Internet for all. Whether you are attending this Community Forum in person or joining us online, your participation underscores the strength of our shared commitment to the future of ICANN and to a secure, stable, and unified global Internet."

Tripti Sinha
ICANN Board Chair

Follow ICANN on Social Media

@icann

facebook.com/icannorg

linkedin.com/company/icann

youtube.com/ICANNnews

flickr.com/icann

soundcloud.com/icann

slideshare.net/icannpresentations

The impact of **Artificial Intelligence** (AI) and **Internet of Things** (IoT) on cybersecurity

By Yusuph Kileo – A cybersecurity and digital forensics expert.

2023 was filled with countless cyberattacks across many countries due to massive increase of IoT in many sectors. Some of these attacks targeted critical infrastructure, financial institutions, governments and other companies.

Internet of things (IoT) – There is an increase use of connected devices with ability to exchange data over the internet. According to Statistita, 805 billion U.S. dollars were spent on the Internet of Things (IoT) technology worldwide last year (2023).

Thermostats, cars, lights, refrigerators, and more appliances can all be connected to the IoT. Moreover, most critical infrastructures have adopted the IoT to facilitate real-time asset/resource visibility and real-time, predictive and prescriptive insights.

With that the IoT brought many benefits which includes, improved operational efficiency, improved end-customer experience, reduced costs, end-to-end remote monitoring and management of assets/resources, and Data-driven insights for quick decision-making.

Artificial intelligence (AI) – can be described as the simulation of human intelligence processes by machines, especially computer systems. Specific applications of AI include expert systems, natural language processing, speech recognition and machine vision.

Since the release of ChatGPT in December 2022, we've seen products and services built with AI integrations for both internal and customer use. Organisations across all sectors report they are building integrations with Larger Language Models LLMs into their services or businesses. This has heightened interest in other applications of AI across a wide audience.

Many organisations such as financial and healthcare sectors have started using AI. Weak AI tends to be simple and single-task oriented, while Strong AI carries on tasks that are more complex and human-like. Some critics fear that the extensive use of advanced AI can have a negative effect on society.

IoT, AI and other cyber threat landscape

The Omdia 2023 report on IoT cybersecurity brings to the forefront the evolving nature of cyber threats targeting IoT infrastructure. The activities of cybercrime syndicates such as Bigpanzi, along with the discovery of a novel variant of the P2PInfect botnet, underscore the sophistication and dynamism of modern cyber threats.

These developments are not just a wake-up call but a clarion call for the adoption of comprehensive and advanced cybersecurity measures. Sectrio's advanced scanning and testing tools, along with its decoy and

deception solutions, represent a leap forward in building resilience against such threats.

The year 2023 was filled with countless cyberattacks across many countries due to massive increase of IoT in many sectors – Some of these attacks targeted critical infrastructure, financial institutions, governments and other companies. As African countries are now pushing for digital transformation and experiencing rapid economic development, cybersecurity remains a pressing concern for businesses across Africa.

Unfortunately, some of the African countries indicate inadequate security measures to fight off cybercrime, leaving them highly susceptible to cyberattacks – They have weak prevention mechanisms to combat cyber threats and poor intrusion detection systems, thereby placing sensitive transactions at significant risk.

There is an increase in the volume and sophistication of cyberattacks in financial institutions. According to the 2023 Africa Financial Industry Barometer, 97% of surveyed leaders of financial institutions in Africa rank cybercrime and regulatory constraints on cybersecurity as the leading threat to the financial services industry alongside worsening economic conditions.

These massive cyberattacks in the region threaten the security of the growing economy and critical infrastructure. MTN Nigeria lost $53 million from its mobile money service, forcing them to sue several banks in Nigeria. Financial institutions and e-citizen portals were halted by distributed denial of service (DDoS) attacks in Kenya. In South Africa there is an increase in backdoor and spyware attacks with an alarming 106,000 recorded attempts.

There are many similar cybersecurity incidents in other African countries and there is a need for urgent action to strengthen protection measures. Failure to counter cyberthreats can have

The most targeted organizations with cyberattacks last year were those in the financial sector (18%), followed by telecommunications companies (13%), government agencies (12%), and organizations from the trade (12%) and industrial (10%) sectors.

serious consequences for individuals, businesses and the socio-economic development of the continent.

Africa is not alone in this. In just September 2023 other parts of the world experienced massive cyberattacks. A few notable incidents include: on September 6, travel booking company Sabre experienced a serious ransomware attack where 1.3 terabytes of data were stolen by Dunghill. On September 11 a ransomware attack on Save The Children lead to the loss of 6.8 terabyte of data and entertainment company MGM Resorts suffered a cyberattack made public on X saying that the security incident severely impacted its business operations. The following day Hong Kong-based cryptocurrency exchange platform, CoinEx, saw the loss of US$70 million in cryptocurrency following a cyberattack launched against it.

In 2023, the most common cyberthreats in Africa includes Insider threats, Social Engineering, Software update supply chain attacks, Phishing attacks, Mobile malware, online shopping fraud, Ransomware, Man-in-the-middle (MitM) attacks, Cryptojacking attacks, IoT botnet DDoS attacks and Malware attacks among others.

According to the year 2023 Positive technology report, the most targeted organizations with cyberattacks were those in the financial sector (18%), followed by telecommunications companies (13%), government agencies (12%), and organizations from the trade (12%) and industrial (10%) sectors.

The impact brought by these growing cyberattacks includes, Loss of customer/business, Loss of organisation critical data, Threat to organisation/National Security, Damage of Goodwill and Reputation, Loss of Revenue – Economic Losses, Temporary or permanent closure, Lawsuits and arbitrations, Danger of terrorism, Time wastage and System down time – reduced productivity.

Data poisoning attacks occur when an attacker tampers with the data that an AI model is trained on to produce undesirable outcomes (both in terms of security and bias).

The UK's National CyberSecurity Center (NCSC) wants everyone to benefit from the full potential of AI. However, for the opportunities of AI to be fully realised, it must be developed, deployed and operated in a secure and responsible way. Cybersecurity is a necessary precondition for the safety, resilience, privacy, fairness, efficacy and reliability of AI systems.

However, AI systems are subject to novel security vulnerabilities (described briefly below) that need to be considered alongside standard cybersecurity threats. When the pace of development is high – as is the case with AI – security can often be a secondary consideration. Security must be a core requirement, not just in the development phase of an AI system, but throughout its lifecycle.

It is therefore crucial for those responsible for the design and use of AI systems – including senior managers – to keep abreast of new developments. For this reason, the NCSC has published AI guidelines designed to help data scientists, developers, decision-makers and risk owners build AI products that function as intended, are available when needed, and work without revealing sensitive data to unauthorised parties.

Generative AI (and LLMs in particular) is undoubtedly impressive in its ability to generate a huge range of convincing content in different situations. However, the content produced by these tools is only as good as the data they are trained on; and the technology contains some serious flaws, including AI hallucination, data poisoning, creating toxic content, and is prone to 'prompt

injection attacks'. AI can be biased and is often gullible when responding to leading questions.

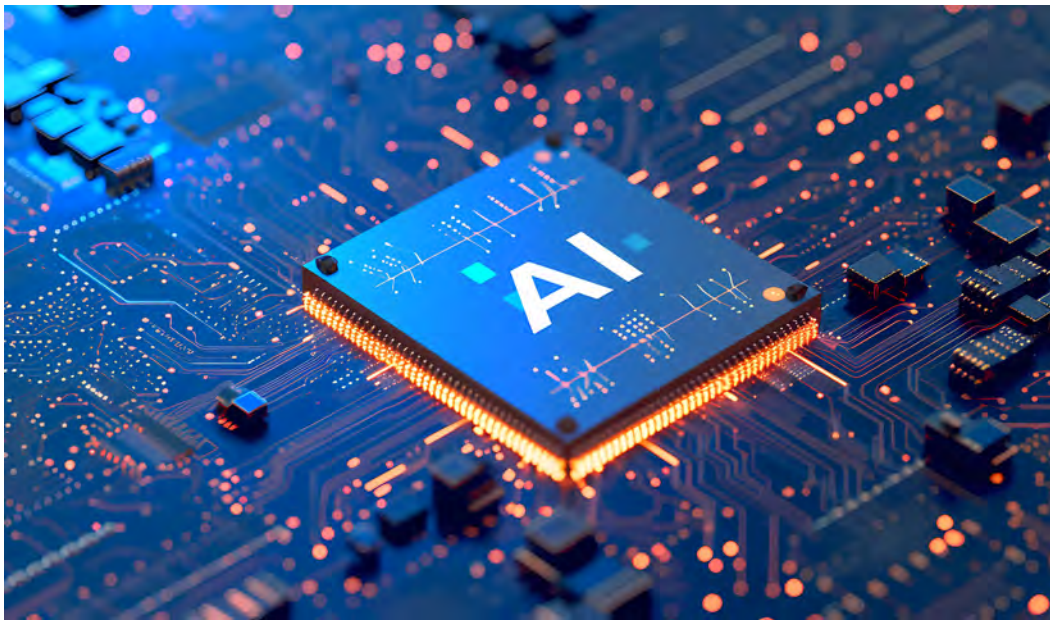
Prompt injection attacks are one of the most widely reported weaknesses in LLMs. This is when an attacker creates an input designed to make the model behave in an unintended way. This could involve causing it to generate offensive content, or reveal confidential information, or trigger unintended consequences in a system that accepts unchecked input.

Data poisoning attacks occur when an attacker tampers with the data that an AI model is trained on to produce undesirable outcomes (both in terms of security and bias). As LLMs in particular are increasingly used to pass data to third-party applications and services, the risks from these attacks will grow, as we describe in the NCSC blog 'Thinking about the security of AI systems'.

IoT Proactive Measures and Best Practices

Ensuring the security integrity of IoT devices before their deployment is not just a matter of best practice but a critical necessity. From vulnerability scanning and penetration testing to the implementation of stringent security protocols such as regular updates, authentication, network segmentation, and encryption, the layers of defense are manifold.

Additionally, incident response planning stands out as a pivotal strategy in mitigating the impact of any potential breach. The industry-wide endorsement of Global Platform's Security Evaluation Standard for IoT Platforms, highlighted in the report, underscores the growing consensus on standardized security benchmarks.



Securing the AI

Organisations need to develop AI which will deliver secure outcomes, rather than providing a static list of steps for developers to apply. By thinking about the overall security of systems containing AI components, stakeholders at all levels of an organisation can prepare to respond to system failure, and appropriately limit the impact on users and systems that rely on them.

Crucially, keeping AI systems secure is as much about organisational culture, process, and communication as it is about technical measures. Security should be integrated into all AI projects and workflows in your organisation from inception. This is known as a 'secure by design' approach, and it requires strong leadership that ensures security is a business priority, and not just a technical consideration.

Leaders need to understand the consequences to the organisation if the integrity, availability or confidentiality of an AI-system were to be compromised. There may be operational and reputational consequences, and your organisation should have an appropriate

Crucially, keeping AI systems secure is as much about organisational culture, process, and communication as it is about technical measures. Security should be integrated into all AI projects and workflows in your organisation from inception.

response plan in place. As a manager you should also be particularly aware of AI-specific concerns around data security. You should understand whether your organisation is legally compliant and adhering to established best practice when handling data related to these systems.

It's also important to note that the burden of using AI safely should not fall on the individual users of the AI products; customers typically won't have the expertise to fully understand or address AI-related risks. Developers of AI models and systems should take responsibility for the security outcomes of their customers.

Key recommendations to secure our digital world in general

The widespread use of technology, combined with insufficient cybersecurity measures, lack of right skillset, inadequate legislation in the field of information security, and a low level of public awareness concerning information security creates favorable conditions for cybercriminals. Moreover, many African countries are facing economic constraints, making it difficult to allocate sufficient funds for cybersecurity.

African governments must develop, implement and regularly update national cybersecurity policies and strategies, involving a wide range of stakeholders in the process.

Establishing a dedicated national institution (Cybersecurity authority) to coordinate cybersecurity activities, respond to cyber incidents, monitor threats and help organizations recover from major cyberattacks should be a top priority for governments.

Governments should work on creating and implementing legislation for the protection of personal data. This legislation should combat cybercrime, guarantee the protection of personal data, and maintain the digital security of citizens and organizations.

Regular cybersecurity awareness should be conducted. People should be educated on potential privacy risks when working in virtual environments.

Governments should identify critical information infrastructure, disruption of which could cause non-tolerable events at the level of industries and countries.

Collaboration between governments and industry peers is also recommended to enhance collective defense against cyberattacks and exchange best practices and thoughts.

Organisations should implement best practices in safeguarding personal and corporate data.

Organizations should have an up to date incident response plan that will help in case of cyberattack. The plan should contain steps to take, as well as a list of people and services to reach in case of emergency. This plan should be regularly tested by conducting attack simulations.

Network segmentation might limit an attacker's exploration of compromised networks. Critical systems in particular should be totally isolated from the rest of the corporate network.

Establishing continuous vulnerability assessment and triage as a basement for effective vulnerability management process

Implementing strict access controls is highly recommended. The principle of least privilege should always be in use for any resource. Multifactor authentication should be deployed wherever possible.

All systems and devices must be up to date and patched to avoid being compromised by a common vulnerability.

Questions to ask about the security of your organisation's AI systems

Managers, board members and senior executives can use the following questions in discussions with technical and security staff, to help you understand how your organization is dealing with the Artificial Intelligence/Machine Learning (AI/ML) threat.

- Do you understand where accountability and responsibility for AI/ML security sit in your organisation?
- Does everyone involved in ML deployment, including board members and/or senior executives, know enough about AI systems to consider the risks and benefits of using them?
- Does security factor into decisions about whether to use ML products?
- How do the risks of using ML products integrate into your existing governance processes?
- What are your organisation's critical assets in terms of ML and how are they protected?
- What is the worst case (operationally or reputationally) if an ML tool your organisation uses fails?
- How would you respond to a serious security incident involving an ML tool?
- Do you understand your data, model and ML software supply chains and can you ask suppliers the right questions on their own security?
- Do you understand where your organisation may have skills or knowledge gaps related to ML security? Is a plan in place to address this?

ICANN Multistakeholder Organizational Chart

ICANN Board of Directors

From Left to Right:

Bottom row:

Edmon Chung, Sally Costerton, Tripti Sinha, Danko Jevtovic, Sarah Deutsch, León Sánchez;

2nd row:

Maarten Botterman, Nico Caballero, Christian Kaufmann, Katrina Sataki, Patricio Poblete, Catherine Adeya, Becky Burr;

3rd row:

James Galvin, Wes Hardaker, Harald Alvestrand, Sajid Rahman, Chris Buckridge; Chris Chapman.

For more information on the ICANN Board visit here.

Country Code Names Supporting Organization (ccNSO)

Alejandra Reynoso (Chair)
Adebiyi Oladipo (V. Chair)
Jordan Carter (V. Chair)

Address Supporting Organization (ASO)

Oscar Robles (Chair)
John Curran (V. Chair)

Empowered Community Administration

Jonathan Zuck (ALAC)
German Valdez (ASO)
Alejandra Reynoso (ccNSO)
Nicolas Caballero (GAC)
Tomslin Samme-Nlar (GNSO)

Government Advisory Committee (GAC)

Nicolas Caballero (Chair)
Vice Chairs: Zeina Bou Harb, Francis Olivier Cubahiro, Nigel Hickson, Ola Bergström, Wang Lang

Security & Stability Advisory Committee (SSAC)

Ram Mohan (Chair)
Tara Whalen (V. Chair)

Root Server System Advisory Committee (RSSAC)

Jeff Osborn (Chair)
Ken Renard (V. Chair)

At-Large Advisory Committee (ALAC)

Jonathan Zuck (Chair)
Claire Craig (V. Chair)
Justine Chew (V. Chair)

Root Zone Evolution Review Committee (RZERC)

Tim April (Chair)

Technical Liaison Group (TLG)

Christian Toche (ETSI)
Howard Benn (ETSI)
Reinhard Scholl (ITU-T)
Jie Zhang (ITU-T)
Wendy Seltzer (W3C)
Shadi Abou-Zahara (W3C)
Warren Kumari (IAB)
Tim Wicinski (IAB)

Nominating Committee 2024

Amir Qayyum (Chair)
Paul Diaz (Chair-Elect)
Vanda Scartezini (Associate Chair)

Ombuds

Krista Papac,
Interim Ombuds

Customer Standing Committee (CSC)

Brett Carr (Chair)

GNSO Stakeholder Groups, Constituencies & Council

GNSO Council Leadership

- **Nacho Amadoz** – Vice-Chair, CPH – EU (AGM 2024)
- **Gregory DiBiase** – Chair – NA (AGM 2024)
- **Tomslin Samme-Nlar** – Vice-Chair, NCPH – AAPAC (AGM 2024)

Contracted Party House Councilors

Registries Stakeholder Group
Kurt Pritz (NA)
Jennifer Chung (AAPAC)
Nacho Amadoz (EU)

Registrar Stakeholder Group
Antonia Chu (AAPAC)
Greg DiBiase (NA)
Prudence Malinki (EU)

Nominating Committee Appointees (NCAs)
Desiree Miloshevic (EU)
Anne Aikman Scalese (NA)
Paul McGrady (NA)

Liaison and Observers
Everton T. Rodrigues ccNSO (LAC)
Justine Chew ALAC (AAPAC)
Jeff Neuman GAC (NA)

Non-Contracted Party House Councilors

Commercial Stakeholder Group
Commercial and Business Users
Lawrence Olawale Roberts (AF)
Mark Datysgeld (LAC
Intellectual Property
Damon Ashcraft (NA)
Susan Payne (EU)
Internet Service and Connection Providers
Osvaldo Novoa (LAC)
Thomas Rickert (EU)

Noncommercial Stakeholder Group
Wisdom Donkor (AF)
Stephanie Perrin (NA)
Manju Chen (AAPAC)
Bruna Martins dos Santos (LAC)
Taiwo Peter Akinremi (AF)
Tomslin Samme-Nlar (AAPAC)

Contracted Party House

Registries Stakeholder Group Executive Committee
Samantha Demetriou (Chair)
Beth Bacon (V. Chair, Policy)
V. Chair, Administration (currently vacant)
Karen Day (Treasurer)
Sue Schuler (Secretariat)

Registrar Stakeholders Group
Ashley Heineman (Chair)
Jothan Frakes (V. Chair)
Owen Smigelski (V. Chair)
Benny Samuelsen (Treasurer)
Eric Rokobauer (Secretary)
Zoe Bonython (Secretariat)

Non-Contracted Party House

Intellectual Property Constituency
Lori Schulman (Chair)
John McElwaine (V. Chair)
Michael Graham (Treasurer)
Jan Janssen (Secretary)
Patrick Flaherty (Participation Coordinator)

Commercial Stakeholders Group*

Business Constituency
Mason Cole (Chair)
Steve DelBianco (V. Chair, Policy Coordination)
Tim Smith (V. Chair, Finance & Operations)
Marie Pattullo (CSG Representative)

Internet Service Providers & Connectivity Providers Constituency
Philippe Fouquart (Chair & CSG Rep)
Susan Mohr (V. Chair)
Lars Steffen (ExComm)

* The groups' officers are omitted here

Noncommercial Stakeholders Group*

Noncommercial Users Constituency
Benjamin Akinmoyeje (AF) (Chair)
Ines Hfaiedh (AF)
Amin Hacha (EU)
Pedro de Perdigão Lana (LAC)
Ken Herman (NA)
Mili Semlani (AP)

Not-for-Profit Operational Concerns Constituency
Juan Rojas (Chair)
Glenn McNight (V. Chair)
Bolutife Adisa (Secretary)
Caleb Ogundele (Membership Committee Chair)
Emmanuel Vitus (Policy Committee Chair)
Jean Quéralt (Communications Committee Chair)

The Benefits of BC Membership

The Business Constituency (BC) is the voice of commercial Internet users within ICANN – the Internet Corporation for Assigned Names and Numbers.

Business users rely on a stable and secure Internet and e-commerce experience, one that serves their users and customers on a global basis. Through your participation in ICANN, and in the Business Constituency, your company will make a difference on behalf of business.

BC members contribute as:

- participants on the BC e-mail list to learn about and debate issues
- participants on telephone conferences to reach consensus on key issues
- participants at physical meetings coincident with ICANN global meetings
- issue managers on specific topics
- bridges for information flow between other GNSO constituencies

The mission of the BC

The Constituency fully represents the views of the Internet business user community.

ICANN policy positions are consistent with the development of business via an Internet that is stable, secure and reliable while promoting consumer confidence.

ICANN policy positions derive from broad stakeholder participation in a common forum for suppliers and users.

BC Executive Committee

Chair
Mason Cole

Vice Chair, Policy Coordination
Steve DelBianco

Vice Chair, Finance & Operations
Tim Smith

CSG Representative
Marie Pattullo

GNSO Councilor
Lawrence Olawale-Roberts

GNSO Councilor
Mark Datysgeld

2024 Nominating Committee Members

Large Business Seat
Mia Brickhouse

Small Business Seat
Vivek Goyal

BC Finance Sub Committee:
Tim Smith (Chair), Jimson Olufuye, Chris Chaplow, Jay Sudowski, Yusuph Kileo, Lawrence Olawale-Roberts

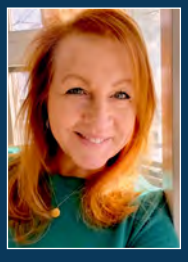
BC Credentials Committee:
Zak Muscovitch (Chair), Vivek Goyal, Roger Baah, John Berard, Kate Buckley

BC Communications Committee:
Vivek Goyal (Chair), Yusuph Kileo, Joseph Ambali

BC Onboarding Committee:
Roger Baah (Chair), Mark Datysgeld, Samuel Dada

Join the conversation on X:
https://twitter.com/icannbc

BC Secretariats



Brenda Brewer

Andrea Glandon

If you would like to become a member of the BC, please contact the BC Secretariat at:

info@icannbc.org

or simply visit our website and register online:

www.icannbc.org