INTERNET SERVICE PROVIDERS AND CONNECTIVITY PROVIDERS CONSTITUENCY (ISPCP)

Public Comment on Guidelines for Advancing Universal Acceptance (UA) Adoption

Submitted to: UA Expert Working Group (UA EWG) / ICANN Public Comment Process

Submitted by: Internet Service Providers and Connectivity Providers Constituency (ISPCP)

Date: April 2026

Reference: Guidelines for Advancing Universal Acceptance (UA) Adoption — Draft for Public Comment, 20 February 2026

1. Introductory Statement

The Internet Service Providers and Connectivity Providers Constituency (ISPCP) welcomes the opportunity to comment on the UA Expert Working Group's draft guidelines for advancing Universal Acceptance adoption.

ISPCP members operate the infrastructure through which the vast majority of internet users experience the DNS and email ecosystem — including recursive DNS resolvers, email, hosting infrastructure, and broadband and mobile connectivity services. We are therefore simultaneously a key stakeholder in UA adoption and a critical enabler of UA-readiness for the wider ecosystem.

ISPCP broadly endorses the UA EWG's guidelines as a constructive and comprehensive framework. We commend the EWG for the breadth of its stakeholder coverage and for grounding the guidelines in a realistic understanding of organizational complexity and incentive structures. However, our review identifies several significant gaps and areas requiring strengthening, which we detail below. In particular, ISPCP draws the EWG's attention to three overarching concerns:

- The guidelines do not adequately address the role of Artificial Intelligence (AI) systems including large language models, AI-powered email filtering, AI assistants, and AI-driven application development tools as both potential barriers to and enablers of UA adoption. This is a critical omission given the pace at which AI is reshaping the internet application landscape. AI Systems increasingly parse, generate and process domain names and email addresses as a part of their core functionality.Systems that are not designed to handle IDNs and EAI will systematically fail in multilingual contexts thereby reinforcing existing UA gaps at scale.
- The guidelines for hosting providers and ISPs (Charter Question 7) are comparatively underdeveloped relative to the detailed guidance provided for

other stakeholder groups. ISPCP offers substantive additions from an operational perspective.

- The guidelines underestimate the structural complexity of the 'chicken-and-egg' problem in UA adoption and do not offer sufficiently concrete mechanisms for breaking the impasse.

ISPCP will participate actively in ongoing ICANN processes related to UA and looks forward to contributing operationally grounded perspectives through its representatives and through continued public engagement.

2. General Observations on the Guidelines

2.1 Strengths of the Draft Guidelines

ISPCP considers the following aspects of the draft guidelines to be well-conceived and important:

- The technology stack framing (Guideline 1 and Figure 1) is technically accurate and helpful. UA cannot be achieved through superficial front-end changes; the vertical dependency on internationalization at the platform and library level is real and is appropriately emphasized.
- The recognition of organizational complexity in large tech organizations (Guideline 6) and the recommendation for multi-level engagement rather than top-down approaches reflect hard-won practical wisdom and are likely to produce better outcomes than uniform engagement strategies.
- The indicators framework (Guidelines 42–45) covering awareness, policy support, implementation, and capacity development is a sound structure. The emphasis on self-reporting with standardized templates and incentives is pragmatic.
- The recommendation to consider developing an issues report for UA adoption by registries and registrars (Guideline 24) is strongly supported by ISPCP. A policy-grounded analysis of gaps at the DNS industry level is a necessary precursor to meaningful incentive-based reform.

- ISPCP further notes that several components of UA-readiness — particularly in the email and messaging ecosystem — are already commercially implementable, with solutions available in the market. The guidelines may benefit from recognizing and leveraging such existing implementations to accelerate adoption, rather than assuming a purely future-state readiness model.

- ISPCP further notes that while the indicators framework is well structured, the guidelines would benefit from the inclusion of clearly defined Universal Acceptance (UA) adoption goals, implementation procedures, and measurable success criteria. Establishing baseline targets and a structured methodology for tracking UA awareness and readiness across stakeholder categories will significantly enhance accountability and outcome-driven execution.

2.2 Cross-Cutting Concern: Absence of AI as a Stakeholder Category

The draft guidelines were presumably scoped prior to the widespread deployment of generative AI systems. However, given the February 2026 publication date of this draft, ISPCP considers it essential that the guidelines explicitly address the AI ecosystem before finalization. The omission is significant for the following reasons:

- Large language models and AI assistants frequently parse, generate, and process domain names and email addresses as part of their core function. Systems that are not trained on or designed to handle IDNs and EAI will systematically fail or mishandle multilingual identifiers — perpetuating UA gaps at massive scale as AI adoption accelerates.
- AI-powered spam filters and email security systems operated by ISPs and email providers are trained predominantly on ASCII-script email data. This creates a systemic risk that internationalized email addresses and IDN-linked communications will be incorrectly classified as suspicious or spam — a bias embedded at the infrastructure level that actively undermines UA adoption even where front-end systems are nominally UA-ready.
- AI-driven code generation tools (such as GitHub Copilot, Cursor, and similar) are widely used by software developers. If these tools suggest or generate code that does not handle IDNs and EAI correctly — for example, by generating ASCII-only email validation regex patterns — they will propagate UA non-readiness at scale across the developer ecosystem. This is arguably a more systemic risk than individual developer knowledge gaps.
- Voice-based AI assistants and natural language interfaces are increasingly used to navigate the internet. If these systems cannot correctly recognize, process, and resolve IDN domain names or internationalized email addresses spoken in non-Latin scripts, they represent an additional UA barrier for the populations UA is most intended to serve.
- AI training data pipelines, data labeling systems, and model evaluation frameworks need to be UA-ready if AI systems are to be capable of correctly handling multilingual identifiers.

- Specific AI-based diagnosis tools/libraries for UA readiness based on the compendium of available UA recommendations may be developed and integrated in mainstream code validation softwares

ISPCP recommends that the UA EWG add a dedicated stakeholder category for AI systems and AI platform providers, parallel to the existing categories for big tech, open-source, and the DNS industry. The guidelines for this category should cover at minimum: AI model training practices, AI-powered email and spam filtering systems, AI code generation tools, and voice/conversational AI interfaces.

In parallel, the guidelines should include a structured approach for documenting and disseminating best practices across stakeholder groups. A centralized repository of real-world UA implementation examples — including deployment models, technical configurations, challenges encountered, and mitigation approaches — will accelerate adoption by reducing duplication of effort and improving confidence among implementers.

2.3 Need for Time-Bound Targets and Phased Implementation

ISPCP observes that while prioritization tiers have been defined, the guidelines do not establish measurable, time-bound targets for UA adoption. To drive meaningful progress, ICANN should define year-wise and milestone-based targets across key UA dimensions, including:

- UA-ready systems (applications, platforms, and services)
- UA-ready email infrastructure (EAI adoption rates)
- UA-compatible browsers and user agents
- UA-compliant DNS and resolver infrastructure

These targets should, where feasible, include indicative benchmarks (e.g., percentage-based adoption goals across key sectors) to enable measurable progress tracking and accountability.

In addition, UA adoption should be structured as a phased implementation model with clearly defined stages (e.g., Awareness → Readiness → Deployment → Optimization), each supported by measurable indicators, timelines, and stakeholder responsibilities. This will help align stakeholders, reduce ambiguity, and enable coordinated global progress.

3. Feedback on Specific Charter Questions and Guidelines

Charter Question 1 — Big Tech Organizations (Guidelines 3–7)

The guidelines would benefit from a clear definition and classification of “big tech organizations,” including criteria such as scale, market influence, and infrastructure dependency. This will enable a more focused and prioritized engagement strategy.

ISPCP supports the economic, social, and technical value messaging framework (Guidelines 3–5) and the tailored engagement approach (Guideline 6). We offer the following additions:

- The guidelines should explicitly address cloud platform providers — including hyperscalers such as AWS, Microsoft Azure, and Google Cloud — as a distinct sub-category of big tech. These providers supply the foundational infrastructure (DNS services, email APIs, identity management, CDN) on which millions of downstream applications depend. UA-readiness at the hyperscaler level would propagate upstream benefit across an enormous portion of the application ecosystem. Their absence from the stakeholder taxonomy is a notable gap.
- Content Delivery Networks (CDNs) are similarly absent from the guidelines. CDNs mediate a large proportion of global web traffic and must correctly handle IDN hostnames in TLS certificates, HTTP headers, and caching keys. ISPCP recommends CDN providers be explicitly included in the big tech engagement strategy.
- On prioritization (Guideline 7), ISPCP endorses the tech-stack dependency model but recommends it be operationalized as a publicly available, maintained taxonomy map — not merely a conceptual framework, so that ICANN org can demonstrate progress on dependencies in a transparent and measurable way.

Charter Question 2 — Open-Source Communities (Guidelines 8–12)

ISPCP supports the functional and application-based prioritization framework (Guidelines 8–9). We add:

- Email validator libraries deserve special emphasis as a priority target. Incorrect email validation — for example, rejection of valid EAI addresses by widely-used open-source validator libraries — is one of the most pervasive and user-visible UA failures. Fixing a small number of widely-used validator libraries would have an inordinately positive impact across the entire application ecosystem.
- The guidelines should address the particular challenge of open-source projects with sparse or inactive maintainers. Many foundational libraries used across the internet are maintained by one or two volunteers, often without institutional backing. A dedicated funding or grant mechanism — possibly coordinated by

ICANN in partnership with foundations such as the Open Technology Fund or Sovereign Tech Fund — could enable contracted fixes to high-impact, under-resourced libraries.

- Package manager ecosystems (npm, PyPI, Maven, Composer) should be identified as a strategic leverage point. Ensuring that popular packages available through these repositories are UA-ready, and flagging non-UA-ready packages in package registries, could accelerate remediation across the developer community.

- In parallel, the guidelines may also encourage alignment between open-source libraries and commercially deployed validation engines to ensure consistency between developer environments and production-grade email systems.

Charter Question 3 — Standards (Guidelines 13–15)

ISPCP recommends that the guidelines explicitly define “standards organizations” and categorize key entities (e.g., IETF, Unicode Consortium, CA/Browser Forum) to ensure structured and consistent engagement.

ISPCP supports the baseline standards list (Guideline 13) and interaction with standards organizations (Guideline 14). We add:

- The guidelines should specifically address DMARC, DKIM, and SPF — the email authentication standards that are critical to email deliverability for ISPs and email providers. These standards need to be reviewed and, where necessary, updated to ensure they fully support EAI. ISPs that implement these standards without EAI compatibility will inadvertently create a security-enforcement barrier to UA adoption.
- The TLS and X.509 certificate standards should be explicitly referenced in the context of IDN support. While RFC 5280 and related standards provide a framework for IDN in certificates, implementation inconsistencies across certificate authorities remain a practical barrier for hosting providers and ISPs seeking to offer IDN hosting services. ICANN should engage with the CA/Browser Forum on this issue.
- ISPCP recommends that ICANN advocate for UA-relevant test suites and conformance testing frameworks to be developed alongside standards. Standards adoption is significantly accelerated when implementers can verify compliance through automated tests — a dimension currently missing from the guidelines.

Charter Question 4 — Software Development Professionals (Guidelines 16–19)

ISPCP supports the outreach strategy and capacity development materials framework. We add:

- The guidelines should explicitly call out AI code generation tools as a target for UA capacity building. This means engaging with the teams responsible for AI coding assistants to ensure that the code they suggest for email validation, domain handling, and URL processing is UA-compliant. A specific workstream with providers of AI development tools could have multiplier effects across the entire developer population.
- Developer certification programs — such as those offered by cloud providers, the Linux Foundation, and professional societies — should be identified as a vehicle for embedding UA competency into recognized professional credentials. This is a more durable mechanism for reaching developers than event-based outreach.
- The recommendation to use CI/CD pipeline integration (Guideline 17e) is well-placed and ISPCP specifically endorses it. Automated UA testing integrated into standard development workflows is likely to be the most scalable and sustainable mechanism for ensuring ongoing UA compliance in software products.

Charter Question 5 — System Administrators (Guidelines 20–21)

ISPCP notes that the guidelines for system administrators, while adequate, underestimate the operational risk concerns that are the primary barrier to EAI adoption among email system administrators. We recommend:

- The guidelines should include a dedicated operational risk assessment guide for email system administrators, documenting the specific risks of enabling EAI support (e.g., interaction with legacy MTAs, spam filter behavior, authentication protocol compatibility) and providing evidence-based mitigation approaches. Without this, administrator caution will persist regardless of awareness campaigns.
- NOG (Network Operators Group) engagement (Guideline 20c) is well-targeted. ISPCP can support outreach through its member networks to NOG communities and recommends that ICANN develop NOG-specific presentation materials that address the operational realities of ISP email infrastructure.

Charter Question 6 — DNS Industry (Guidelines 22–26)

ISPCP strongly endorses the recommendation to develop an issues report on UA adoption gaps in registries and registrars (Guideline 24) and the suggestion of incentive-based policy approaches. We add:

- The guidelines should address the role of domain resellers and Web Host Manager Complete Solutionstyle registrar management platforms more explicitly. Many registrants interact with the DNS industry not through accredited registrars directly, but through resellers using third-party management software. UA gaps in these platforms — particularly in how they handle registrant contact data including email addresses — are a significant and under-addressed barrier.
- RDAP implementation by registrars should be explicitly highlighted as a UA compliance requirement. Many registrars continue to operate WHOIS-only outputs that do not support IDN or EAI in structured data fields. Guideline 22b references EPP and RDAP but does not sufficiently emphasize the compliance gap that exists in practice.
- ISPCP supports the self-assessment recommendation (Guideline 22d) and suggests that ICANN develop a publicly accessible UA-readiness scorecard for registrars and registries, similar to the approach used in other technical compliance contexts. Public visibility of scores creates market incentives without requiring mandatory enforcement.

4. ISPCP Detailed Input on Charter Question 7 — Hosting Providers & ISPs

Charter Question 7 is the section most directly relevant to ISPCP's membership. We consider the three guidelines provided (Guidelines 27–30) to be a reasonable starting point but significantly underdeveloped relative to the operational complexity and strategic importance of this stakeholder group. ISPCP offers the following detailed additions.

4.1 Understanding the ISP-Specific Barrier Landscape

ISPCP's operational experience suggests that the barriers to UA adoption among ISPs and hosting providers are more varied and entrenched than the draft guidelines imply. A simple survey (Guideline 27) will not capture the full picture. Key barriers include:

- Legacy infrastructure lock-in: ISPs and hosting providers frequently operate email and DNS infrastructure built over decades, with deeply embedded ASCII assumptions at multiple layers. Upgrading these systems requires coordinated changes across MTAs, IMAP/POP servers, webmail interfaces, billing systems, support ticketing systems, and customer-facing control panels. The interdependency of these systems makes piecemeal upgrades operationally risky.

- AI-driven spam filter bias: As noted in Section 2.2, ML-based spam and abuse detection systems operated by ISPs are trained on predominantly ASCII email data. These systems may systematically penalize EAI-formatted email, reducing deliverability for internationalized addresses even when the sending infrastructure is technically UA-ready. This is a documented operational concern that the guidelines do not address.
- Regulatory and data sovereignty constraints: ISPs in some jurisdictions operate under data localization requirements that affect how internationalized registrant data can be stored, processed, and transmitted. The guidelines do not address the interaction between UA adoption and applicable regulatory frameworks.
- Customer support complexity: Enabling UA support creates new customer support scenarios — for example, customers with IDN email addresses who experience deliverability issues due to non-UA-ready third-party services. ISPs must be prepared to diagnose and explain these issues, requiring additional staff training and documentation.
- Contractual and SLA constraints: Hosting providers operating under enterprise service agreements may face contractual barriers to unilateral infrastructure changes, even where the technical willingness to support UA exists.In many cases, ISPs and hosting providers may prefer to adopt proven, externally validated UA-ready components rather than undertaking full in-house redevelopment, particularly for email handling and validation layers.

4.2 Recommended Additional Guidelines for Charter Question 7

ISPCP recommends the following additional guidelines for Charter Question 7:

Develop a UA Readiness Reference Architecture for ISPs

ICANN should develop and publish a reference architecture for UA-ready ISP and hosting provider infrastructure, covering: recursive DNS resolver configuration for IDN support; SMTP/MTA configuration for EAI; IMAP and POP3 server configuration; webmail platform requirements; customer control panel (cPanel, Plesk, DirectAdmin) UA compatibility; and certificate management for IDN hostnames. This reference architecture should be maintained and version-controlled as standards evolve.Wherever possible, such reference architectures should incorporate real-world deployment models and interoperable components that have already demonstrated UA compliance in production environments.

Address AI-Powered Spam Filter Bias Directly

ICANN should work with major email security vendors — including those providing spam filtering services to ISPs — to ensure that machine-learning models used for

email classification are trained on sufficiently diverse multilingual data and are validated to not systematically disadvantage EAI-formatted email. This requires engagement with the email security industry (including vendors such as Proofpoint, Mimecast, and Cisco) as a specific workstream, separate from general big tech engagement.The ecosystem may also benefit from the emergence of specialized deliverability assurance layers or services that validate and certify EAI-compliant email handling across sending and receiving systems.

Establish an ISP UA Pilot Program

Rather than relying on messaging and awareness campaigns, ICANN should establish a structured pilot program in which a small number of ISPs commit to enabling UA support across a defined set of systems within a defined timeframe, with ICANN providing technical assistance, documentation, and post-implementation case study support. Pilot participants should span different regions and infrastructure scales. The outcomes should be documented and published to provide evidence for the broader market.

Engage with Hosting Control Panel Vendors

The UA-readiness of cPanel, Plesk, DirectAdmin, and similar hosting control panel software is a critical and largely unaddressed leverage point. These platforms are used by millions of hosting providers globally. UA gaps in these platforms — particularly in how they handle email address fields, domain name inputs, and DNS management — propagate non-readiness across their entire installed base. ICANN should engage directly with control panel vendors as a priority.

Address the Recursive Resolver Layer

ISPs operate recursive DNS resolvers for hundreds of millions of end users. The UA-readiness of these resolvers — including correct handling of IDN labels, DNSSEC validation of IDN zones, and appropriate error handling for non-ASCII queries from legacy applications — is a foundational enabler of the user-facing UA experience. ICANN should develop specific technical guidance for ISP resolver operators, and should coordinate with resolver software maintainers (BIND, Unbound, PowerDNS) to ensure default configurations are UA-ready.

4.3 Breaking the Chicken-and-Egg Impasse

The draft guidelines acknowledge the chicken-and-egg problem between foundational platform providers and higher-level applications (Guideline 7a) but do not resolve it for the ISP/hosting context. ISPCP recommends the following specific mechanisms:

- A coordinated simultaneous commitment program: ICANN should facilitate a structured commitment exercise in which ISPs, hosting providers, email client

developers, and webmail providers simultaneously announce phased commitments to EAI support, with defined timelines. The simultaneous nature of the commitment removes the incentive problem of waiting for others to move first.

- Conditional demand signaling: ICANN should work with major enterprises and public sector organizations to issue explicit statements of intent to use EAI addresses once hosting infrastructure supports them — creating visible demand that justifies ISP investment.
- A minimum viable UA deployment specification: Develop a minimal UA deployment specification that ISPs can implement without full infrastructure overhaul — for example, enabling EAI acceptance on inbound SMTP while deferring webmail display support — to allow incremental progress with limited risk.

4.4 Ecosystem Development and Capacity Building

ISPCP highlights a critical gap in the current ecosystem: the limited availability of organizations and solution providers capable of enabling UA readiness. To address this, ICANN should:

- Encourage the development of a global ecosystem of UA-ready service providers
- Provide technical enablement frameworks, certification programs, and toolkits
- Consider financial and capacity-building support mechanisms, particularly for developing regions

Strengthening the ecosystem will ensure that organizations seeking UA adoption have access to reliable implementation partners, standardized solutions, and scalable support mechanisms, thereby reducing barriers to entry and accelerating global UA readiness.

5. Input on Charter Question 8 — Public Sector and IGOs

ISPCP supports the public sector engagement framework (Guidelines 31–35) and particularly endorses engagement through GAC (Guideline 34) and IGO platforms. We add:

- National broadband and telecommunications regulators should be explicitly identified as a target audience. In many jurisdictions, the same regulatory body that oversees ISPs also manages or influences the ccTLD and sets technical requirements for electronic communications infrastructure. Engaging telecom regulators on UA creates a pathway to requiring UA-readiness as part of licensed ISP obligations or as a condition of public subsidy programs.

- E-government procurement requirements are among the most powerful levers for driving UA adoption. ISPCP strongly endorses Guideline 31b(iii) and recommends that ICANN develop a model UA procurement clause that governments can adopt directly — reducing the drafting burden and increasing consistency of requirements across jurisdictions.
- The guidelines should address the specific role of national CERT and cybersecurity agencies in UA adoption. These agencies influence the security posture of national digital infrastructure and can be allies in communicating that UA-readiness improves security outcomes (for example, by reducing the ambiguity that enables IDN homograph phishing attacks).
- Procurement frameworks may also consider recognizing vendors that demonstrate proven UA-compliant implementations in production environments, thereby accelerating adoption through trusted solution providers.

ISPCP further recommends strengthening the guidelines to explicitly address the social and public impact of UA adoption. Large-scale awareness campaigns, public outreach initiatives, and government-led digital inclusion programs should be leveraged to promote UA as a foundational requirement for a multilingual and inclusive internet.

6. Proposed New Stakeholder Category: AI Systems and AI Platform Providers

ISPCP recommends that the UA EWG add a new charter question and set of guidelines addressing the AI ecosystem. The following is ISPCP's proposed framework for this addition.

6.1 Why AI Requires a Dedicated Stakeholder Category

Artificial intelligence systems have become a primary interface layer between users and the internet across many contexts — including web search, email composition, domain name lookup, application development, and customer service. The UA-readiness of AI systems is therefore not a peripheral concern but a central enabler or barrier to UA adoption at scale. Specifically:

- AI language models are trained on large corpora of internet text that are disproportionately composed of ASCII-script content. This creates a systematic bias toward ASCII domain names and email addresses in model outputs and behavior.
- AI-powered email clients (such as those now integrated with major productivity suites) that compose or process email on behalf of users must handle EAI

correctly — including in address book matching, auto-complete, and email routing logic.

- AI-powered customer service and chatbot systems used by ISPs, registrars, and e-commerce platforms routinely collect and validate email addresses and domain names. Non-UA-ready AI systems in these roles create invisible barriers to UA adoption for end users.

6.2 Proposed Guidelines for the AI Stakeholder Category

AI-G1: Engage with AI Platform Providers on Training Data Diversity

ICANN should engage with leading AI foundation model providers (including OpenAI, Google DeepMind, Anthropic, Meta AI, Mistral, and regional providers) to advocate for training data diversity requirements that include multilingual domain names and email addresses across diverse scripts. This could be pursued through existing AI governance frameworks and voluntary commitments.

AI-G2: Address AI Code Generation Tools as a UA Vector

ICANN should engage directly with providers of AI-assisted development tools to ensure that code suggested for email validation, domain name handling, URL parsing, and user authentication correctly implements IDN and EAI standards. This may include contributing UA-compliant code examples and test cases to the training or fine-tuning datasets used by these tools, and advocating for UA-specific evaluation benchmarks.

AI-G3: Work with Email Security Vendors to Address ML Filter Bias

ICANN should establish a dedicated workstream with email security and spam filtering vendors to document the extent of ML bias against EAI-formatted email, develop testing methodologies for detecting such bias, and advocate for training data and model evaluation practices that ensure non-discriminatory treatment of internationalized email addresses.

AI-G4: Develop UA Benchmarks for AI Systems

ICANN, in collaboration with the Unicode Consortium and IETF, should develop a publicly available UA benchmark test suite for AI systems — covering correct handling of IDN domain names, EAI email addresses, bidirectional text in URLs, and multilingual input validation. This benchmark should be designed for integration into AI model evaluation frameworks and published under an open license.

AI-G5: Include AI in UA Measurement Framework

The indicators framework (Guideline 43) should be extended to include AI-specific UA metrics, including: the percentage of major AI assistants that correctly resolve and handle IDN domain names; the false positive rate of AI-powered spam filters for

EAI-formatted email; and the UA compliance rate of email validation code generated by widely used AI coding tools.

7. Input on Charter Question 10 — Measurement and Indicators

ISPCP supports the measurement framework (Guidelines 42–45) and particularly endorses the emphasis on practical, cost-effective indicators. Over time, these indicators could support the development of a UA compliance certification ecosystem, enabling organizations to identify and adopt verified UA-ready platforms and services. We offer the following additions:

7.1 ISP-Specific Indicators

The current indicator framework does not include ISP-specific metrics. ISPCP recommends the following additions to Guideline 43:

- Percentage of major ISP recursive resolvers correctly handling IDN queries — measurable through standardized probing from multiple geographic locations.
- Percentage of ISP SMTP servers accepting EAI-formatted email addresses in the MAIL FROM and RCPT TO fields — measurable through standardized test probes.
- Percentage of ISP webmail platforms displaying IDN domain names and EAI email addresses without encoding errors — assessable through automated testing frameworks.
- EAI deliverability rate: the ratio of EAI-formatted email successfully delivered end-to-end compared to equivalent ASCII email, measured across participating ISP pairs.

7.2 AI-Specific Indicators

As noted in Section 6, the measurement framework should include AI-specific indicators. ISPCP additionally recommends:

- UA compliance rate of email validation code generated by top AI coding tools — measured through standardized prompt-and-test methodology.
- False positive rate of AI-powered spam filters for EAI email — measurable through controlled delivery testing with EAI-formatted test addresses.
- IDN resolution accuracy of major AI assistants — measured through standardized queries for IDN domain names in multiple scripts.

7.3 Prioritization of the Measurement Framework

ISPCP recommends that ICANN prioritize development of the measurement framework (Guidelines 42–45) as an early implementation task, before broader stakeholder engagement scales up. Without baseline measurements, it is not possible to demonstrate the impact of ICANN's investments or to make evidence-based prioritization decisions. The UA reporting dashboard (Guideline 42b) should be publicly accessible and updated at least annually.

8. Prioritization Recommendations

ICANN has specifically requested community input on how the guidelines should be prioritized for implementation. ISPCP recommends the following prioritization framework, organized into three tiers:

Tier 1 — Immediate Priority (Year 1)

These actions have the highest leverage, address foundational enablers, or fill critical gaps:

- Establish baseline measurements and launch the UA reporting dashboard (Guidelines 42–43). Without measurement, prioritization cannot be evidence-based.
- Commission the issues report on UA adoption by registries and registrars (Guideline 24). This is a prerequisite for meaningful DNS industry reform.
- Engage with AI code generation tool providers on UA compliance in generated code (proposed AI-G2). The scale and speed of AI-assisted development makes this an urgent leverage point.
- Engage with email security vendors on ML spam filter bias against EAI (proposed AI-G3). This is an existing barrier that actively undermines UA adoption infrastructure being built elsewhere.
- Develop the ISP UA reference architecture and EAI email server configuration guidance (ISPCP-proposed). These are high-value, low-cost resources that directly enable ISP action.
- Fix widely-used open-source email validator libraries (supporting Guidelines 8–9). A small number of targeted fixes would have immediate and widespread impact.
- Establish a centralized UA Support and Assistance Center, including helpdesk services, technical advisory support, implementation toolkits, and multilingual knowledge resources. Such a center should provide practical guidance to

organizations at different stages of UA readiness, including troubleshooting support, best practice documentation, and training modules to accelerate adoption across diverse regions.

Tier 2 — Near-Term Priority (Years 1–2)

These actions build on Tier 1 foundations and address the primary stakeholder engagement priorities:

- Develop stakeholder-specific webpages with clear UA-readiness criteria and checklists (Guideline 2).
- Develop and publish the UA procurement model clause for government adoption (supporting Guideline 31b).
- Launch the ISP UA pilot program (ISPCP-proposed). Structured pilots with published outcomes build the evidence base for broader market adoption.
- Engage hyperscalers and CDN providers on UA-readiness (ISPCP addition to Charter Question 1).
- Develop UA benchmark test suite for AI systems (proposed AI-G4).
- Engage with hosting control panel vendors (cPanel, Plesk) on UA-readiness (ISPCP-proposed).

Tier 3 — Medium-Term Priority (Years 2–5)

These actions require foundational work in Tiers 1–2 to be effective:

- Academic curriculum integration (Guidelines 36–41). This is inherently a multi-year effort and is most effective once the professional ecosystem is already developing UA momentum.
- IGO engagement and international platform outreach (Guidelines 32–33, 41). Important but dependent on having a strong, evidence-backed narrative derived from Tier 1 measurement.
- Broad public sector outreach (Guidelines 31–35). Most effective once case studies and pilot outcomes (from Tier 2) are available to demonstrate impact.

9. Global Public Interest and Human Rights Considerations

ISPCP endorses the UA EWG's framing in Appendix B that UA adoption promotes the global public interest by enabling a diverse, multilingual, and inclusive internet. From an ISP and connectivity provider perspective, we add the following considerations:

- UA adoption directly advances the right to access information in one's own language — a human rights principle recognized in multiple UN frameworks. ISPs and hosting providers are a critical enabler of this right, as their infrastructure determines whether multilingual domain names and email addresses are practically usable by end users, regardless of what is technically registered or resolved at the registry level.
- The guidelines correctly identify that UA adoption supports digital inclusion. ISPCP notes that the populations most likely to benefit from UA — speakers of non-Latin-script languages in developing regions — are also disproportionately represented among the customer bases of regional ISPs and hosting providers. ICANN's engagement with these providers is therefore not merely a technical exercise but a direct contribution to digital equity.
- AI systems that are not UA-ready may perpetuate or amplify existing digital divides by providing lower-quality service to users whose language or script is underrepresented in training data. The human rights dimension of AI-related UA gaps deserves explicit attention in the EWG's final guidelines.

10. Implementation, Governance, and Accountability Framework

ISPCP recommends that ICANN complement the guidelines with a clear implementation and governance framework to ensure effective execution and accountability.

Implementation Approach:

ICANN should operationalize these guidelines through a structured program model, aligned with defined priorities, timelines, and measurable outcomes. This may include dedicated workstreams for key areas such as AI, ISP enablement, measurement, and public sector engagement.

Organizational Responsibility:

ICANN should designate clear internal ownership for UA implementation across relevant functions, including policy, technical, and stakeholder engagement teams. A coordinated cross-functional approach will be essential to ensure alignment between policy recommendations and operational execution.

Role of the UA Expert Working Group (UA EWG):

The UA EWG should continue to play a central role as a subject matter expert and coordination body, working in close collaboration with ICANN org and the broader community, and with appropriate visibility and support within ICANN, to advance UA adoption through:

- Providing technical guidance and best practices

- Contributing to the development of measurement frameworks and benchmarks
- Reviewing progress and identifying emerging gaps
- Advising on evolving stakeholder engagement strategies

In addition, the UA EWG can serve as a coordination and facilitation platform across Supporting Organizations (SOs) and Advisory Committees (ACs) by:

- Supporting existing UA-related working groups within SOs and ACs through knowledge sharing, guidance, and alignment of efforts
- Assisting SOs and ACs that are planning to establish UA-focused working groups by providing templates, frameworks, and initial guidance
- Promoting cross-community collaboration and consistency in UA adoption approaches while fully respecting the autonomy of each SO and AC

This approach will help create a more cohesive, scalable, and sustainable UA ecosystem across the ICANN community.

Monitoring and Reporting:

ICANN should establish a transparent monitoring and reporting mechanism, including periodic progress reports and publicly accessible dashboards, to track UA adoption across stakeholder groups and ensure accountability.

A clearly defined governance model will be critical to translating these guidelines into measurable, real-world impact.

Conclusion

ISPCP commends the UA EWG for producing a comprehensive and well-structured set of guidelines. The framework addresses a genuinely complex multi-stakeholder challenge with appropriate nuance regarding organizational diversity, incentive structures, and measurement requirements.

Our primary recommendations for strengthening the guidelines before finalization are:

- Add a dedicated AI stakeholder category covering AI platform providers, AI code generation tools, AI-powered email security systems, and voice AI interfaces, with specific guidelines and measurement indicators for each.
- Substantially strengthen the Charter Question 7 guidelines for hosting providers and ISPs, incorporating ISPCP's proposed additions on reference architecture, spam filter bias, pilot programs, control panel vendor engagement, and recursive resolver guidance.

- Add ISP-specific indicators to the measurement framework, including recursive resolver IDN handling, SMTP EAI acceptance rates, and webmail display compliance.
- Adopt ISPCP's tiered prioritization framework, beginning with measurement and high-leverage technical interventions, and supported by clear implementation and governance mechanisms, before scaling stakeholder engagement programs.

ISPCP will participate actively in ICANN's ongoing work on UA adoption through its representatives and through continued engagement with the ISP and connectivity provider community. We welcome further dialogue with the UA EWG and ICANN org on any of the issues raised in this submission.

Internet Service Providers and Connectivity Providers Constituency (ISPCP)

GNSO Constituency | ICANN

Public Comment submitted via ICANN's Public Comment Process

For inquiries, please contact the ISPCP Chair or designated GNSO representative.